Data. Protection. Adding Value.

Data Protection Laws - Brazil

Legislation

The Brazilian General Data Protection Law ("LGPD") was enacted in 2018 and came into force in September 2020. The LGPD was heavily inspired by the European GDPR, with many of the same obligations, requirements and rights for data subjects, and is dedicated to protecting the personal data of those to whom the law applies.

Risk Level: High

Scope: The Law applies to any personal data processing operation performed by a natural person or legal entity, public or private, regardless of the means, country of the headquarters or country where the data is located, as long as:

I – The data processing activity is performed in national territory;

II – The activity has the purpose of providing goods or services or processing data of individuals located in national territory; or

III – Personal data has been collected in national territory.

Exemptions: LGPD does not apply to data processing:

I – Performed by a natural person exclusively for personal and non-economic purposes;

II – Performed exclusively for journalistic or artistic purposes;

III – Performed exclusively for public security, national defense, State security or criminal investigation purposes;

IV – Performed exclusively for academic purposes, as long as a legal basis is defined for processing.

Enforcement

Supervisory Authority: The LGPD provides for the establishment of the National Data Protection Authority ("ANPD"), responsible for ensuring, implementing and monitoring compliance with the LGPD throughout the national territory.

The ANPD has already been established and is issuing guidance on the application of the LGPD, as well as applying the sanctions set forth in the legislation.

Registration/Approval Requirements: No registration requirements have been determined by the LGPD.

Data Processing

Good faith and 10 other principles, listed below, are established by the LGPD:

- Purpose;
- Adequacy;
- Necessity;
- Free access;
- Data Quality;
- Transparency;
- Security;
- Prevention;
- Non-discrimination; and
- Accountability.

Supervisory Authority

Enforcement (Fines, Criminal Penalties): LGPD foresees many sanctions, to wit:

(i) fines up to 2% of the company's annual turnover, limited to BRL$ 50 MM;
(ii) (daily fines;
(iii) (warnings;
(iv) publicization of the infringement;
(v) blocking of personal data;
(vi) elimination of personal data;
(vii) suspension of the database;
(viii) suspension of the data processing activity for 6 months;
(ix) total or partial prohibition of activities related to personal data.

Brazil Privacy Principles

Legal Basis for Processing: Personal Data:

(i) consent;
(ii) compliance with legal or regulatory obligations;
(iii) performance of public policies, by the public administration;
(iv) performance of research, by research entities;
(v) performance of a contract;
(vi) regular exercise of rights in judicial, administrative or arbitral procedures;
(vii) protection of life or physical protection of the data subject or a third party;
(viii) health protection when performed by health professionals;
(ix) legitimate interests; and (x) credit protection.

Sensitive Personal Data: LGPD defines sensitive personal data as: racial or ethnic origin, religious beliefs, political opinion, union membership, filiation to religious, philosophical or political organizations, data related to health, sexual life, genetic or biometric data.

Processing of sensitive personal data cannot be performed based on legitimate interests, or performance of a contract, as legal basis defined above. However, it can be performed for fraud prevention.

Transparency Requirements

LGPD has transparency as one of its principles, meaning that data subjects must be aware of how their personal data is performed, through terms of consent, privacy notices and other related documents.

pwc

Individual Rights

LGPD foresees data subject's rights as pert article 18.

- **Right to access:** Yes
- **Right to correction:** Yes
- **Right to restriction:** Yes
- **Right to deletion/be forgotten:** Yes
- **Right to portability:** Yes

Right to opt out of all or specific processing: Right to revoke consent or opt out from other data processing activities, especially when performed by legitimate interests.

Other: Anonymization, confirmation if the processing exists and information about data sharing with private or public entities.

Other Business Obligations

Data Protection Officer: Appointing a DPO is mandatory for data Controllers, except when considered small size data processing agents, as per ANPD guidance.

Risk Assessments: Data processing agents have to evaluate risks related to data processing activities. A DPIA has to be performed when data processing activities might lead to risks to the civil rights and freedoms of the data subject.

Audits: The ANPD has the right to perform audits to verify discriminatory aspects related to data processing, or for other enforcement activities.

Record Keeping: Controllers must keep record of the data processing activities, through a RoPA. Small size data processing agents have the right to keep records in a simplified manner, as per ANPD guidance.

Security & Data Breaches

Security Requirements: APP 11 requires an APP Entity to take such steps as are reasonable in the circumstances to protect personal information that the APP Entity holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Data Breaches: The Notifiable Data Breach (**NDB**) scheme in Part IIIC of the Privacy Act applies to APP Entities that have an obligation under APP 11 to protect personal information they hold. The NDB requires regulated APP Entities to notify impacted individuals and the OAIC if an 'eligible data breach' occurs (i.e. when personal information is accessed, disclosed or lost without authorisation and a reasonable person would conclude that this is likely to result in serious harm to any of the individuals to whom the personal information relates). However, if remedial action effectively prevents serious harm there will not be an 'eligible data breach' for the purposes of the Privacy Act, and notification will not be required.

Notification to individuals and supervisory authorities: The NDB scheme requires entities to notify affected individuals and the OAIC where they have reasonable grounds to believe there has been an 'eligible data breach and complete an assessment within 30 days.

Cross-Border Transfers

Cross-Border Data Transfers: Cross-border transfers can only be performed in the following situations:

I - To countries or international organizations that provide a level of protection for personal data appropriate to that provided for in the LGPD;

II - When the controller offers and proves guarantees of compliance with the principles, the rights of the data subject and the data protection regime provided for in the LGPD, in the form of: (a) specific contractual clauses for the transfer; (b) SCCs; (c) global corporate rules; (d) regularly emitted seals, certificates and codes of conduct;

III – For international legal cooperation;

IV – When transfer is necessary for protecting the life or physical safety of the data subject;

V – When authorized by the ANPD;

VI – When necessary for international cooperation agreements;

VII – When necessary for the performance of public policies; and

VIII – Upon data subject's consent.

Let's connect to discuss how we can help:

Enrique Tello Hadad
Digital and Data Protection Leader
Partner, Loeser e Hadad Advogados (Brazil)

+55 (11) 98178 7997
enrique.hadad@lhlaw.com.br