HOW TO COMPLY WITH THE BRAZILIAN DATA PROTECTION LAW

FOR LARGE AND SMALL BUSINESSES /STARTUPS

campos thomaz
& meirelles advogados

INDEX

1 Is the Brazilian Data Protection Law (known as 'LGPD') applicable to my organization?

The General Data Protection Act ("LGPD") regulates the processing of personal data performed by private and public organizations, including large, small-sized companies and startups. The LGPD aims to protect the fundamental right to privacy, personal data, and the free development of an individual's personality.

Like the General Data Protection Regulation (GDPR), the LGPD defines personal data as any "information related to identified or identifiable natural persons". Therefore, any information relating to natural persons collected or processed by the organization must be used following the requirements of the LGPD. Personal Data typically includes but is not limited to name, email, telephone, Tax ID, home address, behavioral information of the data subject. In practical terms, most private organizations are subject to LGPD rules because they process the personal data of their employees, customers, and third parties.

As for international organizations, the LGPD shall apply regardless of the data controller location. To the extent the controller processes personal data in Brazil or collects personal data from individuals in Brazil, the LGPD shall apply. Any operation carried out with personal data, including the collection, classification, transfer, processing, storage, and deletion, is subject to the LGPD.

The LGPD also imposes more restrictive requirements for processing sensitive personal data. Sensitive personal data is qualified as information relating to the racial or ethnic origin, religious conviction, political opinions, trade union membership, religious, philosophical, or political opinion, health or sexual life, genetic or biometric data of the data subject. This information is commonly seen in daily business operations, e.g., in employees' medical exams.

Some business activities typically carry out a risk of violating the LGPD. Please find below a non-exhaustive list of such activities:

- Processing of candidate's data in recruitment;
- Admission, payment, evaluation, and dismissal of employees;
- Treatment of leads in the context of marketing activities;
- Processing of individuals' data for the provision of products and services;
- Sharing customer and employee data with third parties.

If your organization carries out some of the activities above, the LGPD shall be observed.

2

Risks of not complying with the LGPD

Please find below a non-exhaustive list of the benefits and risks of not complying with LGPD:

- Avoid reputational risks, such as to the company's image and brand, arising from a data leak or incident
- Possibility to participate in public bids
- Lack of customers and partners confidence
- Avoid the devaluation of stocks and assets
- Contract with third parties that require LGPD compliance as a prerequisite to enter into an agreement
- Using personal data as a competitive advantage against non-compliant competitors

3

Step by step to comply with the LGPD

Please find below a step-by-step walkthrough to help organizations achieve initial compliance with the LGPD. The step-by-step defined below is a framework that needs to be tailored to each organization's needs, size, and risks.

STEP 1

Data mapping and information life cycle

To obtain an assertive legal gap analysis, the organization needs first to conduct a data mapping and document the information life cycle, including internal and external information flows.

This step might require an internal investigation or research consisting of the following (non-exhaustive list):

- Identify which personal data is processed by each of the organization's business areas, including for what purpose such personal information is used;
- Identify the organization's internal and external data flows;
- Identify specific practices for collecting and processing data from employees, customers, and third parties;
- Identify whether there is a governance structure in privacy and data protection in place, including what measures have already been taken to achieve compliance with the LGPD and other sector-specific laws involving privacy and data protection in Brazil; and
- Internally document the information obtained and data flows identified in the steps immediately preceding; this documentation is mandatory for adequacy to the LGPD; documentation shall be kept preferably in Portuguese.

The information above makes it possible to identify the organization's maturity level from a privacy and data protection perspective. If the organization conducted a data mapping abroad, it might consider translating it into Portuguese

STEP 2

Gap Analysis and Action Plan

The next step is to develop a gap analysis, consisting of the study of requirements met versus those requiring additional compliance effort. Such efforts might include changes in internal documents or business practices. Following the gap analysis, the organization shall create an action plan to prioritize measures to obtain compliance.

Typically, the high-risk processing activities are eliminated first and after the residual risks.

STEP 3

Implementation

The internal documents and business practices are adjusted following the Action Plan prepared in Step 2 above in the implementation. Please find below a non-exhaustive list of implementation activities that might be included in this phase:

- [ ] Creation of a governance program in privacy and data protection, with attribution of responsibilities to each business area involved;
- [ ] Appointment of the data protection officer (DPO);
- [ ] Creation of a channel for internal consultations and evaluation of new business processes, products, and services, by DPO or legal department, from a privacy and data protection perspective;
- [ ] Creation or adaptation of communication channels to respond to data subjects requests;
- [ ] Review or development of corporate policies, including:
    - [ ] privacy notices
    - [ ] acceptable use of personal data policy
    - [ ] data retention and elimination of documents
    - [ ] information security
    - [ ] acceptable use of corporate devices and systems
    - [ ] bring your own device policy
    - [ ] employee monitoring (labor-related restrictions apply)
    - [ ] recruitment of candidates, including the procedure for conducting background check (labor-related restrictions apply);
    - [ ] internal investigations
    - [ ] collection, processing, and sharing of sensitive personal data of employees, such as those related to health plans, medical tests, mandatory admission examinations, or employees health monitoring;
    - [ ] collection, processing, and sharing of leads' data in the marketing area;
    - [ ] acceptable practices in human resources, marketing, commercial, and other business areas;
- [ ] Preparation of consent terms for the processing of personal data, where applicable;
- [ ] Development of data sharing policy with third parties

- [ ] Review of contracts for sharing personal data with third parties, such as suppliers;
- [ ] Implementation of a mechanism that allows the international transfer of data;
- [ ] Review or preparation of a data incident response plan;
- [ ] Review or preparation of a communication plan with the applicable authorities, including the Brazilian Data Protection Authority (ANPD);
- [ ] Preparation of data protection impact assessments (DPIA); and
- [ ] Development of training and awareness programs for employees and third parties.

STEP 4

Training and Maintenance

The culture of privacy and data protection should permeate business activities. Thus, the guidelines regarding the acceptable use of personal data by employees should be reflected in the internal documents of the organization but also be continuously communicated through training and awareness actions.

After completing the initial compliance effort, new products, services, and business processes should be continuously assessed for privacy and data protection. Maintaining compliance to the LGPD implies a continuous work and assessment of business practices, products, and services.

4 I am a small business or startup. Should I comply fully with the LGPD, or is there some flexibility?

The Brazilian Data Protection Authority (ANPD) issued Ordinance No. 2/2022 ("Resolution 2") to make more flexible some of the LGPD requirements for small-sized processing agents. According to Resolution 2, the following types of national organizations are considered as small-sized processing agents:

Microenterprises (ME)	Small Business (EPP)	Startups
Revenues up to R$ 360,000/year	Revenues up to R$ 4.8 million/year	Revenues up to R$ 16 million/year*
Non-profit legal entities	Individuals who act as controllers (E.g. Self-employed)	Depersonalized entities (E.g., residential condominiums)

*Or revenues of R$ 1.33 million/month, multiplied by the number of months of activity in the previous year, when the legal entity was created for

International organizations with no legal entity in Brazil might not benefit from the more flexible requirements introduced by Resolution 2. Such a benefit is unavailable if the data processing activity results in high risk for the rights of affected data subjects. Under Resolution 2, high-risk activities are those that combine at least one general criterion and one specific criterion provided below:

Processing that resulting in high risk for data subjects =

One general criterion + one specific criterion

General Criteria:

- Large-scale processing of personal data

  (Analyze: Volume of data subjects, data volume, duration, frequency and geographical extent of treatment to identify whether there is a large scale in the processing of personal data);

- Processing of personal data that could significantly affect the interests and fundamental rights of data subjects

  (Examples: use of health data, political or religious orientation, biometric data, or information revealing a data subject's financial capacity)

Specific Criteria:

- Use of emerging or innovative technologies
- Surveillance or control of publicly accessible areas
- Processing of sensitive personal data or data regading children and teenagers
- Automated decisions that may affect the interests of data subjects

Please find below a comparison chart of the more flexible requirements introduced by Resolution 2:

	Full compliance Agentes que não se enquadram como pequeno porte	**Flexible requirements** Small-sized processing agents
Record of Processing Activities (ROPA)	Controllers shall prepare and keep a record of personal data processing operations	Controllers shall prepare and keep a record of personal data processing operations in a simplified format
Form and Deadline for Communication of Security Incidents (Data leakage and security incidents that may cause significant damage or risk to the data subject)	Must report security incidents following the LGPD Deadline for notification: Reasonable period to be defined by the ANPD (the recommendation of the ANPD, not yet binding, is to report data incidents within two working days)	Must report security incidents following a simplified procedure Deadline for notification: two times the period for non-small sized processing agents (when defined) (The double deadline shall not apply in the event of incidents that may compromise the physical or moral integrity of the data subjects or national security)

	Full compliance Agentes que não se enquadram como pequeno porte	Flexible requirements Small-sized processing agents
Appointment of Data Protection Officer	Mandatory	Not mandatory
Information Security – Technical and Organizational Measures	The controller and processor shall adopt technical and organizational security measures to protect personal data from any unlawful use or data incident	The controller and processor might adapt essential technical and organizational measures with reduced information security requirements (For this item, it is recommended to comply with the minimum information security requirements set out in a guide prepared by the ANPD in 2021)
	The controller and processor shall implement an information security policy	The controller and processor might adapt essential technical and organizational measures with reduced information security requirements
Data Subjects Requests	The controller must respond to requests within 15 days	TThe controller must respond to requests within 30 daysnumber of requirements

Despite the flexibility presented above, small-sized processing agents still need to comply with the other requirements in the LGPD, as illustrated in item 3 of this booklet.

5 After the initial compliance effort, do I still need to comply with the LGPD?

In many cases, business activities change constantly. Suppliers and employees change, business processes change (thus changing how personal data is processed), and the organization can develop new products or services.

In this regard, each personal data processing operation and information flow shall be continuously documented and updated. New business processes, services, and products developed by the organization must be constantly evaluated from a privacy and data protection perspective to comply with the legislation. It is common for the ANPD to update recommendations on achieving compliance with LGPD periodically.

Thus, the maintenance of the governance program in privacy and data protection is necessary throughout the organization's entire existence. Without being exhaustive, maintenance activities may include:

- Risk assessment of new business processes, products, and services offered, with the implementation of risk mitigation measures (legal and technical);
- Preparation of data protection assessments (DPIA), when required;
- Continuous training and awareness of employees;
- Update of the record of processing activities (ROPA);
- Periodic review of documents, such as privacy notices and corporate policies;
- Monitoring of new recommendations published by the ANPD;
- Monitoring and response to data and security incidents; and
- Vendor management, including assessing data sharing activities and data protection clauses in contracts.

Conclusion

As demonstrated above, obtaining compliance with the LGPD is essential to observe legal requirements and prevent harm to image, brand, or business relationships with third parties. Although the initial adequacy project is complex and robust, engaging local experts to develop and create privacy and data protection governance is one of the most assertive ways to go through the LGPD compliance effort.

Our recognitions

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 & 2022)

Leaders League (2021 & 2022)

Transactional Track Record (2021 & 2022)

The Legal 500 (2022)

Meet our Partners

Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Partner

Corporate, M&A, Venture Capital and Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Partner

Intellectual Property, Technology, Agreement and Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Follow us

campos thomaz & meirelles advogados

Subscribe to our newsletter