



# **A Practical Guide for Data Processing Agents**

THE MAIN PROVISIONS OF THE BRAZILIAN  
DATA PROTECTION LAW AND RECENT  
REGULATORY ACTIVITY IN BRAZIL

**MATTOS FILHO**

## Data protection in Brazil: the general landscape

The **Brazilian Data Protection Law** (Federal Law No. 13,709/2018 – LGPD) is the main law governing the **processing of personal and sensitive data** by companies and individuals in Brazil.

The LGPD establishes detailed rules for collecting, using, processing, and storing personal data. It affects throughout the economy, including relationships between customers and providers of products and services, employees and employers, transnational and domestic commercial relations, as well as other situations in which personal data is collected in both physical and digital environments.

### When is the LGPD applicable?

The LGPD applies to any and all processing activities carried out by companies and individuals, irrespective of the jurisdiction where they are based or the jurisdiction the data is located in, provided that:

- The data is **processed in Brazil**;
- The data is processed in **order to offer or provide goods** or services to data subjects located in Brazil; or
- The personal data was **collected in Brazil** (while the data subject was in Brazil).

The **Brazilian Data Protection Authority** (*Autoridade Nacional de Proteção de Dados – Brazilian DPA*) is responsible for enforcing the LGPD and ensuring personal data is protected in Brazil.

## Key definitions of the LGPD



**Personal data:** any information related to an identified or identifiable individual.



**Sensitive personal data:** personal data linked to an individual's racial or ethnic origin, religious beliefs, public opinions, membership of a labor union or religious, philosophical, or political organization, as well as an individual's health, sex life, genetic or biometric data.



**Data processing:** any activity carried out with personal data, such as data collection, production, reception, classification, use, access, reproduction, transmission, distribution, filing, storage, elimination, evaluation, control of information, communication, transfer, dissemination, or extraction.



**Data processing agents:** data controllers and data processors.



**Data controller:** an individual or a public or private legal entity that is responsible for personal data processing decisions.



**Data processor:** an individual or a public or private legal entity that processes personal data on behalf of a data controller.



**Data subject:** an individual to whom the personal data being processed pertains.

## Data processing agents

The Brazilian DPA's **Data Processing Agents and Data Protection Officers Guide** establishes **data controllers' responsibility for defining the core elements and characteristics of the data processing** (such as the purpose of data processing, the categories of personal data to be processed, and the duration of data processing).

**Resolution CD/ANPD No. 2/2022** regulates how the LGPD applies to small processing agents, which may encompass microenterprises, small businesses, and startups. Small processing agents are exempt from certain LGPD-related obligations, as explained below.

## Main obligations imposed by the LGPD

In summary, the LGPD requires data processing agents to:



Keep a **record of the data processing activities (RoPA)** they carry out. The Brazilian DPA has established simplified rules for small processing agents in relation to preparing RoPA, as per **Resolution CD/ANPD No. 2/2022**.



Comply with the data processing **principles** established by the LGPD (e.g., necessity, adequacy, transparency, free access, non-discrimination, etc.).



Comply with **data subjects' rights** (e.g., rights to data access, rectification, erasure, withdrawal of consent, data portability, etc.).



Rely on a **legal basis established by the LGPD to justify the data processing for a specific purpose** (such as the data subject's consent, compliance with legal and regulatory obligations, performance of a contract, legitimate interests, and more).

The Brazilian DPA's **Guide on Legitimate Interest** provides guidance on interpreting and applying these legal bases in a practical sense, defining related concepts, and offering parameters for the Legitimate Interest Assessment (LIA).



Adopt data protection measures by design upon developing any new technology or products (privacy by design).



As a rule, data processing agents must appoint a Data Protection Officer (DPO) to act as communication channel between the data processing agent, data subjects and the Brazilian DPA. However, this is not mandatory for small processing agents.

**Resolution CD/ANPD No. 18/2024** outlines DPOs' duties and obligations, processing agents' liability in the event the LGPD is not complied with, as well as situations that may give rise to conflicts of interest. The Brazilian DPA has also published a non-binding guide with good practices for data processing agents concerning the roles and duties of the DPO, including templates for formally appointing the DPO.

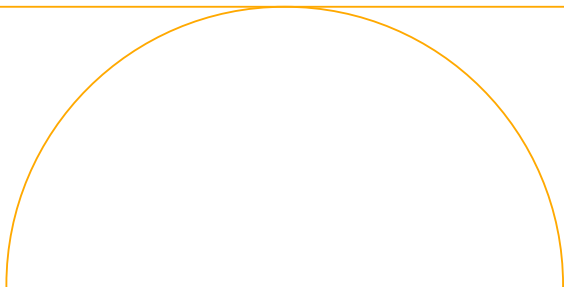
## Data breaches

The LGPD requires processing agents to adopt security measures to protect personal data from any adverse event related to the breach of the properties of confidentiality, integrity, availability, and authenticity of personal data security (data breaches). If a particular data breach entails subjecting the affected data subjects to material risk or harm, the data controller must notify both the Brazilian DPA and the affected data subjects.

The **Brazilian DPA's Resolution CD/ANPD No. 15/2024** provides guidance on data breach reporting obligations, as follows:

- **Data breach reporting to the Brazilian DPA:** as a rule, within three business days of becoming aware of the incident affecting personal data.
- **Supplementary notification:** additional information on the data breach may be provided in a reasoned manner to the Brazilian DPA within 20 business days from the date of the first notification.
- **Data breach reporting to affected data subjects:** within three business days of becoming aware of the incident affecting personal data.

As a rule, data controllers must keep a **record of data breaches** for a minimum of **five years**. Such records must also contemplate events not reported to the Brazilian DPA and/or data subjects.



## International data transfers

Under the LGPD, international personal data transfers are only permitted under specific circumstances, such as when:

- The receiving country or international organization provides an adequate level of data protection;
- The controller can demonstrate compliance with the principles, rights, and protections provided for in the LGPD. These guarantees may be provided through specific contractual clauses, standard contractual clauses, global corporate rules, seals, certificates, or codes of conduct; or
- The data subject consents to the transfer.

The Brazilian DPA has approved its [Regulations on International Data Transfers](#). These regulations apply to personal data transfers between processing agents from Brazil to other countries. They establish rules for transfers to countries with adequate protection (as recognized by the Brazilian DPA) or when companies use contractual clauses or global corporate rules to comply with the LGPD. Currently, no countries have yet to be granted adequacy status, though an adequacy decision involving the EU is anticipated to happen in the future.

In the meantime, companies must rely on alternative mechanisms under the LGPD, such as:

- **Brazilian DPA-approved standard contractual clauses:**  
These clauses must be adopted in full, without changes and incorporated into contracts. Companies that rely on this mechanism have until August 22, 2025, to implement them;

- **Equivalent standard contractual clauses:** The Brazilian DPA may recognize standard contractual clauses from other countries as equivalent;
- **Specific contractual clauses:** Companies can request the Brazilian DPA to approve tailored clauses for transfers when standard ones are not feasible; or
- **Global corporate rules:** These are binding mechanisms for international data transfers between entities within the same group or corporate conglomerate.

The Brazilian DPA has also launched a specific [webpage](#) in both Portuguese and English where data processing agents can find detailed guidance on the subject, including instructions on how to submit requests for the analysis of international data transfer mechanisms.

## Liability under the LGPD

Data processing agents are held liable for **material and non-material damage** stemming from LGPD violations, as follows:



When data processors breach the LGPD or when they fail to follow the controller's lawful instructions, they will be jointly and severally liable with the controller for damage caused in the data processing; and



Controllers will be jointly and severally liable when they are directly involved in the data processing activity.

Specific **liability exceptions** are outlined in the LGPD and include cases where:

- The processing agent (controller or processor) did not carry out the data processing activity attributed to it.



- No violation of the LGPD actually occurred (even though the processing agent carried out the data processing attributed to it).
- The damage is exclusively the fault of the data subject or a third party.

Data subjects may defend their interests and rights through administrative or judicial proceedings, either individually or collectively. They may also file a lawsuit in Brazilian courts to seek compensation for material or non-material damages resulting from violations of privacy rights or lodge a complaint with consumer protection authorities (such as PROCONs) or the Brazilian DPA itself.

## Penalties imposed by the LGPD

In the event processing agents fail to comply with the LGPD, they may be subject to one or more of the following administrative penalties:

- An official warning notice;
- Having the violation publicly disclosed;
- The erasure or blocking of data until remedies have been implemented;
- Being suspended or totally/partially prohibited from processing data; and/or
- A fine worth up to 2% of the infringing entity's economic group's annual turnover in Brazil, capped at BRL 50 million (approximately USD 8.3 million) per offense.

[Resolution CD/ANPD No. 4/2023](#), which regulates the calculation and application of administrative penalties, defines the criteria and parameters that the Brazilian DPA must apply to monetary and non-monetary sanctions, as well as criteria for pecuniary sanctions.

## The Brazilian DPA's upcoming actions

The **Brazilian DPA's 2025-2026 Regulatory Agenda** outlines the Brazilian DPA's priority actions for the upcoming years. The initiatives of the 2025-2026 Regulatory Agenda are categorized into phases, in order of prioritization, as follows:

### Phase 1

Topics on the 2023-2024 Regulatory Agenda still pending regulation

Compliance with data subjects' rights

Preparation of data protection impact assessments (DPIA)

Data sharing by public authorities

Processing of personal data related to children and teenagers

Processing of sensitive personal data (in particular biometric data)

Implementation of security, technical and administrative measures

Data processing and artificial Intelligence

Data processing deemed "high-risk"

Data processing by religious organizations

Implementation of anonymization and pseudonymization techniques

### Phase 2

Topics to be regulated within one year

Guidelines for the National Policy on Personal Data Protection and Privacy

Best practices and governance rules

Personal data aggregators

Processing of sensitive personal data (in particular, health data)

## Phase 3

Topics to be regulated within 18 months

Consent

## Phase 4

Topics to be regulated within two years

Legal basis of credit protection

In addition, the Brazilian DPA has launched a dedicated [webpage](#) aimed at facilitating access to information regarding its monitoring activities, enforcement actions, and administrative sanctioning procedures, as well as data breaches. The new page also provides a simplified explanation of the supervisory process, ensuring greater transparency and accessibility for stakeholders.

The Brazilian DPA notably intensified its supervisory activities in 2024, with a particular focus on ensuring the LGPD compliance by data processing agents on the following **key areas**:

**Complying with data subjects' rights**

**Processing personal data related to minors**

**Data sharing involving payroll loans**

**Disclosing the DPO's contact details**

**Generative Artificial Intelligence (AI)**

**Data subject communication channels**

# MATTOS FILHO

SÃO PAULO CAMPINAS RIO DE JANEIRO BRASÍLIA NEW YORK LONDON

[mattosfilho.com.br](http://mattosfilho.com.br)