Guide to the Brazilian Data Protection Law

MATTOS FILHO >

Mattos Filho, Veiga Filho,
Marrey Jr e Quiroga Advogados

July 2019

TABLE OF CONTENTS

We hope the following pages will serve as a navigation guide for this new reality. Mattos Filho is available to assist you as you face this challenge.

Enjoy your read!

* This Guide cannot be used as a legal opinion and it does not constitute legal advice.

GUIDE TO THE BRAZILIAN DATA PROTECTION LAW

THE BRAZILIAN DATA PROTECTION LAW (LAW NO. 13,709/18 OR "LGPD") REGULATES THE MANNER IN WHICH ORGANIZATIONS MUST USE PERSONAL DATA OF AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL IN BRAZIL.

The LGPD significantly transformed the data protection system in Brazil, aligning it with the European legislation, the General Data Protection Regulation – GDPR. The LGPD establishes detailed rules for the collection, use, processing and storage of personal data and it will affect all sectors of the economy, including the relationship between customers and suppliers of products and services, employees and employers, transnational and national commercial relations, as well as other relations in which personal data is collected in the digital environment or outside the digital environment.

The main topics addressed in the LGPD are dealt with in this guide in an objective and direct manner in order to give the reader a clear idea of its impacts in the business and the measures that should implemented during the 24 months that anticipate the effectiveness of the LGPD.

Mattos Filho Data Protection and Cybersecurity practice is well-equipped to be your partner in this moment of legislative and cultural change in Brazil with respect to the protection of personal data, offering the following services:

Assistance in adapting the company's policies to the requirements of the law

- Mapping (gap analysis) and adoption of measures required for compliance with the LGPD;
- Review of internal procedures, policies and flows for processing personal data to comply with the LGPD.

Legal advice on the relationship between processing agents and data subjects

- Preparation or review of privacy policies and terms of use for processing personal data;
- Preparation and review of contracts and other documents for the hiring of service providers that collect or process personal data on behalf of the company in Brazil and in other countries.

Preparation of internal corporate policies and other documents

- Preparation of cybersecurity policies and other corporate policies to regulate the processing of personal data;
- Legal advice on the preparation of internal policies to record the processing of personal data;
- Legal advice on the preparation of privacy impact assessment reports.

Training sessions on best data protection practices and measures

- Advice on the preparation of educational materials for employees, service providers and other affiliates, focusing on matters of privacy, data protection and information security;
- Internal trainings.

Legal advice on the international transfer of personal data

- Advice on procedures and flows related to international transfers of data and potential restrictions or modifications;
- Preparation and review of contracts, clauses, codes and binding corporate rules for international transfers of data.

Legal advice on data breach and cybersecurity incidents

- Advice on the development of preventive measures related to security incidents;
- Creation of internal processes to properly respond to security incidents with data subjects, authorities and other third parties;
- Coordination of data breach incidents in other jurisdictions in partnership with local firms.

Interaction with the National Data Protection Authority and supervisory authorities

- Legal advice on the defense of company interests with regulatory and investigative authorities responsible for supervising and imposing sanctions for noncompliance with the LGPD.

Legal advice on the interaction with other countries or regions and on the compliance by Brazilian companies with the European legislation (GDPR)

- Advice on the compliance with the European legislation (GDPR) in partnership with foreign firms, in a one-stop-shop format;

- Analysis on the compatibility between the Brazilian legislation regarding corporate policies, procedures and practices related to processing of personal data with that of other countries or blocks (such as USA, APEC).

PARTNERS IN THE DATA PROTECTION AND CYBERSECURITY PRACTICE

Fabio Ferreira Kujawski
kujawski@mattosfilho.com.br
55 11 3147 2795

Paulo Marcos Rodrigues Brancher
pbrancher@mattosfilho.com.br
55 11 3147 4684

Thiago Luís Sombra
thiago.sombra@mattosfilho.com.br
55 61 3218 6010

DEFINITIONS

Personal Data

Is information related to an identified or identifiable individual, that is, any information that identifies or can identify a person, such as names, numbers, identification codes, or addresses.

Sensitive Personal Data

Is personal data related to the racial or ethnic origin of an individual, his/hers religious belief, public opinion, membership in a union or religion, philosophical, or political organization, data related to the health, sex life, genetics or biometrics, when linked to an individual.

Processing

Is any activity carried out with personal data. For example: collection, production, reception, classification, use, access, reproduction, transmission, distribution, filing, storage, elimination, evaluation, control of information, communication, transfer, dissemination or extraction.

Controller

Is the person who has the ability to make decisions related to the processing of personal data. This person may be an individual or entity, whether public or private.

Processor

Is the individual or entity, whether public or private, that conducts the processing of personal data on behalf of the controller.

Processing Agents

Are the controllers and processors.

Data Protection Officer

Is the person indicated by the controller or processor to act as a communication channel between the controller, the data subject and the National Data Protection Authority (ANPD).

National Data Protection Authority (ANPD)

It is the governement entity with technical and decision-making autonomy, responsible for regulating, drafting guidelines and supervising compliance with the LGPD.

SCOPE

In which situations is the LGPD applicable?

WHAT YOU MUST KNOW

— It regulates the processing of data related to individuals only;

— It applies regardless of the form the data is processed; it imposes rules for processing data whether or not it is carried out in the Internet, or using digital media;

— It applies to processing activities that occur within the Brazilian territory and outside the country, when:

- personal data are collected in Brazil;
- data are related to individuals located in the Brazilian territory, or
- their goal is to offer products and/or services to individuals, Brazilian or foreign, in Brazil.

— It does not revoke or inhibit the application of sector standards that also regulate personal data;

— It will go into effect in August 2020, but some topics require further regulation.

— On July 08, 2019, Law 13,853/2019 was sanctioned, creating the National Data Protection Authority (ANPD) and amending some provisions of the LGPD.

WHAT MEASURES SHOULD YOU TAKE?

Organizations that process personal data within the Brazilian territory or offer products or services to individuals in Brazil should try to understand the impact of the LGPD on their activities and how to comply to its rules. The hiring of technical and specialized legal consultants to diagnose the company's specific risk is advisable.

Organizations should verify whether there are other sector standards for data protection applicable to their activities besides the LGPD.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Sections 1, 3 and 4

LEARN MORE

The LGPD regulates the processing of information related to individuals only and it does not apply to data of deceased persons or entities. Public and private sector organizations must comply with the law when processing data of individuals. Furthermore, the LGPD regulates the processing of personal data carried out by any form, whether or not in the Internet, or using digital media.

Territorial and Extraterritorial:
The LGPD applies to any processing activity carried out within the national territory, or even outside the national territory, regardless of where the processing agents are domiciled or the data are located, as long as:

- the purpose of the processing activity is to offer or provide goods or services in the Brazilian territory;
- the purpose of the processing activity is to process personal data of individuals located in the Brazilian territory;
- the personal data being processed have been collected in the Brazilian territory.

Non-Application of the LGPD:
The LGPD does not apply to the processing of personal data:

- Conducted by individuals exclusively for private and non-economic purposes;
- Carried out exclusively for journalistic, artistic, or academic purposes;
- Carried out exclusively for public security, national defense, or State security;
- In activities investigating or suppressing criminal offenses;
- Originated in other countries or for other countries that only passes through the national territory without any processing carried out in Brazil.

Sector Specific Regulations:
The LGPD does not revoke or obstruct the application of other sector specific regulations that also involve processing of personal data, which must be complied with.

Effectiveness:
The LGPD will go into effect in August 2020, but some topics must be further regulated.

PRINCIPLES

What are the LGPD principles and what do they establish?

WHAT YOU MUST KNOW

The principles established in the LGPD impose new guidelines and limitations on how personal data can be processed, as follows:

Principles

- **Purpose;**
- **Adequacy;**
- **Necessity;**
- **Free Access;**
- **Data quality;**
- **Transparency;**
- **Security;**
- **Prevention;**
- **Non-discrimination; and**
- **Liability and Accountability.**

Pursuant to the LGPD, processing agents must adopt effective (and demonstrable) measures for processing data to comply with the expected principles of LGPD.

WHAT MEASURES SHOULD YOU TAKE?

Review and modify policies (internal and in relation to third parties), contracts, procedures and other activities that involve the processing of personal data (of customers as well as employees) to the principles established in the LGPD.

Maintain records, preferably in writing, that demonstrate the adoption of measures for processing activities that are in compliance with the principles established in the LGPD, regardless of the size of the existing database.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Section 6.

LEARN MORE

The principles established in the LGPD, listed on this page, introduce new guidelines and limitations on how personal data can be processed in Brazil. Processing of personal data is subject to the following principles, besides good faith:

Purpose:
The processing of personal data must be carried out for legitimate, specific and explicit purposes and be communicated to the data subject, observing the established purpose the data was collected.

Adequacy:
The data processing must be limited to the purpose for which that data was collected.

Necessity:
Limitation on the processing of personal data to the minimum necessary for fulfilling its purpose, using appropriate and proportional data that are not excessive when compared to the purpose of its processing.

Free Access:
Guarantee to data subjects the right to easily and freely require the means and duration of processing, as well as the integrity of their personal data.

Data quality:
Guarantee to data subjects that their data is accurate, clearly displayed and highlighted, as well as the right to update it, according to the necessity and to fulfill the purpose of its processing.

Transparency:
Guarantee to data subjects clear, precise, and easily accessible information regarding the processing of data and its processing agents, observing trade and industry secrecy rules.

Security:
Use of appropriate technical and administrative measures to protect personal data from unauthorized access and accidental or illicit destruction, loss, change, communication, or dissemination events.

Prevention:
Adoption of measures to prevent damages as a result of processing of personal data.

Non-discrimination:
Prohibition from processing data for illegal or abusive discriminatory purposes.

Liability and Accountability:
The processing agent must demonstrate the adoption of effective measures to prove the observance and fulfillment of personal data protection standards, including the efficacy of these measures.

LAWFUL BASIS

In which situations is the processing of personal data considered legal?

WHAT YOU MUST KNOW

Although the Brazilian Internet Act only permits the processing of personal data after the data subject consents, the LGPD establishes ten cases in which data can be processed, besides the consent of the data subject, including the legitimate interest of the controller or third parties, for the fulfillment of a contract or a legal or regulatory obligation.

In addition to consent, the cases for processing sensitive personal data are more restricted and do not permit processing based on legitimate interest or for credit protection, for example.

The LGPD establishes specific rules for obtainment of consent, which may be null if it is only a generic authorization or if it is based on information with misleading or abusive content.

There are specific rules for processing personal data of children and adolescents.

The processing of personal data that is public must take into account the original purpose, good faith, and public interest that justify making such data available.

WHAT MEASURES SHOULD YOU TAKE?

Carefully evaluate which lawful basis are applicable for processing data in your specific case.

When the processing of personal data is based on consent, the controller should keep supporting documentation demonstrating that the consent was obtained in accordance with legislation.

When the processing of personal data is based on legitimate interest, the controller must adopt measures to guarantee the transparency of the processing, which may be reviewed by the national data protection authority.

Maintain records and justification for processing of personal data, especially when based on a legitimate interest.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Sections 5, XII; 7 to 16; and 37

LEARN MORE

The LGPD establishes an exhaustive list of cases that justify the processing of personal data:

- Through consent of the data subject;
- For the fulfillment of a legal or regulatory obligation by the controller;
- By the government, for the processing and shared use of data necessary to implementation of public policies established by law and regulations;
- To conduct studies by research institutes, ensuring, whenever possible, the anonymization of the personal data;
- When necessary for the execution of a contract or for preliminary contract procedures;
- For the protection of life or the physical safety of the data subject or third parties;
- The regular exercise of rights, including contractual performance, and in court, administrative, or arbitration proceedings;
- When necessary to fulfill the legitimate interest of the controller or third party, except when the data subject's fundamental rights and freedom require the protection of personal data;
- For the protection of health, exclusively, in procedures conducted by health care professionals, health care service providers or health authorities;
- For the protection of credit, including to observe legislation.

Consent:

The LGPD establishes that consent is a free, informed and unequivocal manifestation of the data subject that authorizes the processing of personal data for a certain purpose. Generic authorizations, that is, authorizations that do not have a specific, explicit and informed purpose are null.

Consent will be provided in writing or by any other expressive action by the data subject that demonstrates his/her will. Implicit consent will not be admitted under any circumstance.

Consent will be considered a temporary authorization because it can be revoked at any time by the data subject by a free and easy procedure.

If there is any change in the purpose for processing personal data for which the data subject's consent was obtained and if that is not compatible with the original consent, the controller must inform the data subject about this change.

In case the data is publicly available or publicly disclosed by the data subject, such data may be processed for new purposes, provided that those purposes are legitimate and specific, and the data subject's rights and principles established in the LGPD are observed.

Legitimate Interest:

The processing of personal data required to meet the legitimate interest of the controller or third parties is permitted by the LGPD, as long as said processing does not violate the fundamental rights and freedom of the data subject and appropriate measures are adopted to guarantee the transparency of such processing.

Legitimate interest will be verified based on the analysis of a specific situation and based on the principles of the LGPD and it may be reviewed by the national data protection authority. For example, the LGPD establishes a list of purposes that could justify the legitimate interest of the controllers or third parties, depending on the specific situation, as follows:

- Support and promotion of the controller's activities;
- Protection of the data subjects regular exercise of rights or service provisions that benefit them, as long as their legitimate expectations are respected.

When processing personal data based on the controller's legitimate interest only, strictly required data, considering the intended purpose, may be used.

Processing of Sensitive Personal Data:

The language in the LGPD is strict for processing sensitive data, considering the nature of such data, and requires more rigorous consent.

Consent for processing sensitive personal data must be provided in a specific and highlighted manner. That is, the processing agent in charge of obtaining the consent must obtain a special authorization for processing sensitive personal data.

Furthermore, the LGPD does not permit processing sensitive personal data to fulfill the legitimate interest of the controller or third parties or for credit protection. On the other hand, there is still the possibility of processing sensitive personal data when it is necessary to satisfy a legal or regulatory obligation by the controller, for the regular exercise of rights, including contractual performance and in court, administrative, or arbitration proceedings.

The communication or shared use of health data between controllers for the purpose of obtaining economic advantage shall only be permitted in the following circumstances:

- To allow the portability of the data, when requested by the data subject;
- To benefit the data subjects, in the provision of health care services, pharmaceutical care or health care;
- To allow the financial and administrative transactions resulting from the above mentioned services.

Processing of Personal Data of Children and Adolescents:

The processing of personal data of children and adolescents must be conducted in their best interest. The processing of personal data of children requires specific and conspicuous consent by at least one of the parents or guardian. Controllers must put forth every reasonable effort to verify that the consent was provided by the person responsible for the child.

The LGPD, however, permits the collection of personal data without the consent of parents or guardians in order to contact the parent or guardian. In this case, the personal data collected without consent may only be used once and it may not be stored under any circumstance, considering that its only purpose is to contact the parents or guardian.

Termination of Processing:

The termination of processing of personal data will occur when:

- It has been verified that the purpose for which the consent was obtained has been achieved or the personal data collected ceased to be necessary or relevant to achieve the specific desired purpose;
- The end of the processing period has been reached;
- The data subject makes any manifestation in this regard;
- There is a legal determination.

Upon the termination of processing of personal data, the data will be deleted, unless its storage is permitted by LGPD, such as in case of anonymization.

RIGHTS OF THE DATA SUBJECT

What rights can the data subject demand from processing agents?

WHAT YOU MUST KNOW

The data subject has the right to easily access information about the processing of his personal data and to demand correction for incomplete, inaccurate or outdated data.

He/she may also request the transfer of his/hers personal data to another service or product supplier through an express request.

When the data processing is exclusively based on automated decisions, the data subject has the right to request a review of such processing.

If noncompliance with the provisions in the LGPD has been verified, the data subject can oppose to the processing of his personal data if the processing was based on one of the cases in which consent is waived.

The data subject may also revoke a previously granted consent for processing his/hers personal data.

WHAT MEASURES SHOULD YOU TAKE?

Review and possibly modify the operational and technical structure of your organization to guarantee all the rights to the data subject.

Develop mechanisms to permit data subjects to exercise their rights in an easy and free-of-charge manner.

Verify whether the informative content provided to the data subject is in clear and proper language.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Sections 8, §5; 9, caput, §3; 14, §6; and 17 to 22

LEARN MORE

The LGPD establishes the protection of fundamental rights of freedom and of the privacy of individuals as its principal goals. As such, it presents a list of principles and rights especially geared towards the guarantee of clear information to the data subject and imposition of limitations to the processing of data.

Besides having the right to clear information about data processing, the data subject has the right to freely obtain the following measures, through an express request to the controller:

- Confirmation of the existence of processing and access to personal data;
- Correction of incomplete, inaccurate, or outdated data;
- Anonymization, blocking, or elimination of data that is unnecessary, excessive, or processed in noncompliance with the provisions in the LGPD;
- Portability of data to another service or product supplier;
- Elimination of personal data that is processed with the data subject's consent, except if the data is processed to fulfill any legal or regulatory obligation;
- Information regarding the shared use of personal data;
- Information on the possibility of not providing consent and the consequences of such refusal;
- Possibility of revoking the consent through a free and easy procedure.

Right to Information:
The data subject has the right to have easy access to information related to the processing of personal data, including, but not limited to, information regarding:

- The specific processing purpose;
- The form and duration of the processing;
- The identification and contact of the controller;
- The shared use of data and its respective purpose;
- The liability of processing agents;
- The processing of personal data as a condition for providing the product or service, or for exercising a right, if applicable;
- Other rights of the data subject, pursuant to the terms of the LGPD.

Such information should be provided in a clear, appropriate and emphasized manner.

Children:

In the case of processing of personal data of children, the information will be provided in a simple, clear and accessible manner, considering the physical-motor, perceptive, sensory, intellectual and mental characteristics of children. Companies may employ audiovisual resources or other similar resources to transfer the pertinent information. Besides providing information to the parents or guardian, who should consent to the processing of data, the child should also be able to understand it.

Confirmation of and Access to Personal Data:

At any time, the data subject has the right to obtain confirmation of the existence of processing of his/her data and access to the personal data. This can occur in two different manners:

- In simplified form, if the confirmation or access is provided immediately;

- By means of a clear and complete statement, indicating the origin of the data, nonexistence of records, criteria used and purpose of the processing, as the case may be, within fifteen days counted from the date of the request.

The information will be provided electronically or in hard copy, in accordance with the data subject's request.

In addition, when the processing of data is a result of a consent or a contract, the data subject may ask for a complete electronic copy of his personal data.

Correction, Anonymization, Pseudonymization, Blocking or Elimination of Personal Data:

The data subject may request the correction of data that he considers incomplete, inaccurate or outdated, as well as may ask for the anonymization, blocking or elimination of personal data considered unnecessary, excessive or processed in noncompliance with the rules in the LGPD.

For purposes of the LGPD, "anonymization" is a procedure through which certain data loses the possibility of identifying a data subject, whereas "blocking" means the temporary suspension of any personal data processing activity.

Furthermore, in case of data processing based on consent, the data subject may request the elimination of any data collected, except if the storage is permitted by the LGPD. The LGPD permits keeping data for compliance with a legal obligation by the controller or for the exclusive use of the controller in which case the data must be anonymized.

If the company shares data, the correction, anonymization, blockage or elimination of the data, when requested by the data subject, must be immediately informed to the other processing agents so that the procedure is repeated except in cases where such communication is demonstrably impossible or involves disproportionate effort.

In conducting studies in public health, research institutes may have access to databases with personal data, which will be processed exclusively within the institute and strictly for the purpose of conducting studies and researches. In this case, such data must be maintained in a controlled and secure environment, according to practices outlined in specific regulations and including, whenever possible, anonymization or pseudonymization of the data, as well as appropriate ethical standards related to the studies and research.

For the purposes of fulfilling this rule, "pseudonymization" is the process through which data loses the possibility of being associated, directly or indirectly, with an individual, without the use of additional information maintained separately by the controller in a controlled and secure environment.

Portability of Personal Data:
The LGPD created the right to portability, through which the data subject may request the transfer of his personal data to another service or product supplier through an express request.

Review of Automated Decision:
The data subject may request the review of a decision taken solely based on automated processes, including decisions for the creation of profiles. The data subject may also request the provision of clear and proper information regarding the criteria and the procedures used in the development of automated decisions.

And in the event of impossibility of immediate compliance?
If it is not possible to immediately comply with the measure requested by the data subject, the controller may send the data subject a justification with the reasons why immediate compliance with the right exercised is not possible or a communication indicating he is not the processing agent of the data and, if known, specifying who the agent is.

OBLIGATIONS

Which obligations may the data subject demand from the controller?

WHAT YOU MUST KNOW

Among the obligations established in the LGPD, the controller must:

Obligations

- **Prove the consent was obtained in accordance with the LGPD;**
- **Keep a record of the personal data processing activities executed;**
- **At the request of the national data protection authority, prepare a privacy impact assessment report;**
- **Inform the data subject if there is any change in the purpose for data collection;**
- **The controller is jointly liable with processor, if damages are caused to third parties due to a violation of the LGPD.**

WHAT MEASURES SHOULD YOU TAKE?

Adopt technical measures that guarantee data processing in a secure manner.

Develop internal processes and create policies that permit creating and maintaining records of data processing activities.

Preserve the data, seeking to fulfill the purpose for which they were collected and to comply with legal and regulatory obligations.

Appoint a data protection officer.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Sections 5, 7 §5, 8 §2, 9 to 11, 14, 16, 18, 20, 33, 37 to 42, 48, 50 and 52

LEARN MORE

The controller is responsible for making the decisions about personal data processing, as well as to care for preservation of data and to meet the requirements and demands from the authorities. In this regard, the LGPD imposes the following responsibilities on the controller:

- Prove that consent was obtained in compliance with the law;
- Confirm the existence or provide access to personal data at the request of the data subject, in a simplified format, immediately, or through a clear and complete statement, which indicates the origin of the data, the nonexistence of records, the criteria used and the purpose of the processing, within 15 (fifteen) days;
- Keep a record of activities related to personal data processing; the national authority may determine the preparation of a privacy impact assessment report (related to personal or sensitive data) of processing activities.
- If the national authority requests the report, the controller must enter, at a minimum, the following information:

  - Description of the types of data collected;

  - Methodology used for collecting data;

  - Methodology used for guaranteeing security of information;

  - Analysis of the controller in relation to these measures, safeguards and mechanisms adopted for mitigating risks.

The controller is also responsible for indicating who is the data protection officer, publicly disclosing in a clear and objective manner, preferably in his website, the identity of the person and his contact information. Generally, the activities the data protection officer consist of:

- Accepting complaints and notifications from data subjects, providing clarifications and adopting necessary measures;
- Receiving notifications from the national authority and adopt measures;
- Instruct employees and contracted parties of the organization about the practices to be taken in relation to the protection of personal data; and
- Executing other activities determined by the controller or established in supplementary regulations issued by the national data protection authority.

In the event the consent is required, the controller must inform the data subject if there is any change in the purpose for the collection of data and at this time, the data subject may opt to renew the consent or revoke it.

If the data subject does not give consent, the controller may process personal data if there is a legitimate purpose. Only personal data strictly necessary for the intended purpose may be processed and measures should be adopted to guarantee transparency.

The controller responds jointly with the processor if, when processing personal data, he causes property or non-material damage, whether individually or collectively, in violation of the LGPD.

The controller is authorized to create good practice and governance rules that stipulate conditions for organization, procedures, security and technical standards, obligations, internal mechanisms of supervision and risk mitigation, as well as other aspects related to the processing of personal data, as long as capacities are respected.

The controller is permitted to maintain data when the processing period ends in order to permit compliance with legal and regulatory obligations.

The controller may also make exclusive use of data, as long as anonymized, but its access by third parties is expressly prohibited by law.

NATIONAL DATA PROTECTION AUTHORITY

What is the role of ANPD?

WHAT YOU MUST KNOW

The ANPD is a government entity, with technical and decision-making autonomy. The ANPD is connected to the Cabinet of the Presidency.

ANPD's structure include the Board of Directors, the National Council for Protection of Privacy and Personal Data, the Inspector's Office, the Ombudsman's Office, the legal advisory body and administrative units for the enforcement of the LGPD.

The ANPD shall coordinate its activities with other government bodies and entities with jurisdiction related to the protection of personal data. The ANPD will be the main entity responsible for interpretating of the LGPD.

We highlight the following main responsabilities of the ANPD:

- Monitoring, auditing and applying sanctions in case of processing carried out in violation of the LGPD;
- Communicating criminal offenses to the competent authorities, promoting knowledge of public rules and policies, and preparing studies and contents that facilitate privacy and data protection activities in the society;
- Requesting information at any time from controllers and operators of personal data that perform data processing operations;
- Providing different deadlines, standards, guidelines and procedures for small companies and startups in order to facilitate compliance with the LGPD.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Sections 55

INTERNATIONAL TRANSFER OF DATA

What if the data is processed outside Brazil?

WHAT YOU MUST KNOW

The international transfer of data is permitted as long as the conditions established in the LGPD are observed. Generally, the LGPD only permits international transfers to countries with an adequate level of protection.

To receive the data, the country or international organization shall provide an adequate level of data protection, which will be evaluated by the National Data Protection Authority.

WHAT MEASURES SHOULD YOU TAKE?

Adopt caution in sending data to organizations abroad and ensure that they will comply with the requirements established in the LGPD.

Adopt procedures and prepare documents, including contracts and binding corporate rules that document the compliance with data processing according to the LGPD.

Inform the national authority if there is any change in the guarantees that has been understood as sufficient for making the international transfer of data.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Sections 3, 33, 34 to 36

LEARN MORE

The LGPD is applicable to any data processing activity, regardless of the country of domicile or the country in which the data is located. Please see the section "Scope" in this guide.

The LGPD expressly determines the cases in which an international transfer of data is permitted, as follows:

- To countries or international organizations that offer an adequate level of personal data protection as established in the law;
- When the controller offers and demonstrates compliance with principles in the LGPD, the data subject rights and the data protection system established in the law, through specific contractual clauses for a given transfer, standard contract clauses, binding corporate rules or regularly issued seals, certificates and codes of conduct;
- When the transfer is necessary for international legal cooperation between government intelligence, investigations, and prosecution authorities, according to instruments of international law, or when it is the result of a commitment established in an international cooperation agreement;
- When the transfer is authorized by the national data protection authority;
- When the transfer is necessary for the execution of public policies or public service activities;
- When the data subject has provided specific and conspicuous consent for the transfer upon prior information regarding the international character of the activity, clearly distinguishing this from other purposes for data processing;
- When it is necessary for the fulfillment of a legal or regulatory obligation on the part of the controller;
- For the execution of a contract or procedures related to the contract in which the data subject is a party, as long as required by the data subject himself;
- The regular exercise of rights, including contractual performance and in court, administrative, or arbitration proceedings.

However, the level of data protection of the foreign country or of the international body will be evaluated by the national data protection authority, which will observe, among other things, the adoption of security measures, the nature of data and the general standards in effect in the country of destination or in the international body.

SECURITY AND NOTIFICATIONS

What if there is some incident that results in data leaks?

WHAT YOU MUST KNOW

Security measures must be adopted with the purpose of guaranteeing the protection of personal data against unauthorized accesses and accidental or illicit situations. The first step is to identify the nature of the data subject to the incident. If they are encrypted or anonymized data, for example, the risks will be lower.

Security incidents must be informed, within a reasonable period, to the National Data Protection Authority and to the data subject.

Depending on the seriousness of the incident, the authority may determine the adoption of certain measures and communications to other regulatory bodies, such as the Brazilian Securities Commission (CVM) and Central Bank of Brazil (BACEN).

Controllers and processors that, when failing to adopt security measures cause damage, will be held liable. The liability regime will be joint and several.

WHAT MEASURES SHOULD YOU TAKE?

Develop systems to identify and combat security incidents and train the I.T. team to guarantee the execution of these procedures.

Review security agreements to guarantee coverage in case of security incidents.

Create internal policies and procedures and develop partnerships with technical service providers and legal consultants to respond to incidents efficiently and satisfy the requirements in the LGPD.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Section 44, sole paragraph and sections 46 to 51.

LEARN MORE

Processing agents will protect the personal data against unauthorized accesses and accidental or illicit situations such as destruction, loss, change, communication or any form of improper or illicit handling of personal data. For such, a series of technical and administrative security measures will be adopted.

It will be up to the National Data Protection Authority to determine the minimum technical standards for the protection of personal data, especially for sensitive data. Sector authorities, such as health and financial sectors, may also establish such requirements.

Although any person who intervenes in the processing of data has the obligation to guarantee security, processing agents who give rise to damages respond for damages resulting from non-compliance with security measures.

Processing agents should also adopt technical measures that make the personal data affected unintelligible so that unauthorized third parties cannot access them. The adoption of such technical measures will be taken into account to analyze the seriousness of the incident.

Security incidents that may entail significant risk or damage to data subjects must be communicated to the: (i) National Data Protection Authority and the (ii) data subject, within a reasonable period (to be defined by the authority) and (iii) specific regulatory bodies.

This communication must contain, at a minimum, the following information:

- description of the nature of the personal data affected;
- the data subjects involved;
- the technical and security measures used for data protection;
- the risks related to the incident;
- the reasons for the delay, if the communication was not immediate;
- the measures adopted to revert or mitigate the effects of the loss caused by the incident.

Depending on the seriousness of the incident, the National Data Protection Authority may determine the adoption of measures, such as broad disclosure of the fact in the media and measures to revert or to mitigate the effects of the incident.

Processing agents may, individually or through associations, create good practices and governance rules about the processing of personal data, which establish:

- the conditions of the organization, operation and procedures applicable to the processing of personal data (including complaints and petitions by data subjects);
- security and technical standards;
- specific obligations for the various parties involved in the processing;
- educational actions;
- internal mechanisms for supervision and mitigation of risks;
- other aspects related to the processing of personal data.

The controller, applying the principles of security and prevention, may implement a privacy program and demonstrate its effectiveness, whenever appropriate.

SANCTIONS

What if there is noncompliance with the LGPD?

WHAT YOU MUST KNOW

Besides the responsibility for indemnifying the data subject, the LGPD establishes administrative sanctions in the event of noncompliance with its rules.

The administrative sanctions applicable range from warning to monetary sanctions that could reach 2% of the group's revenues in Brazil, limited to BRL$ 50 million per violation.

The sanctions may be applied cumulatively, by day and violation, but always based on the seriousness and extent of the violation.

WHAT MEASURES SHOULD YOU TAKE?

Conduct an analysis to verify compliance of data processing procedures with the LGPD to identify complete compliance with the rules.

In the event of noncompliance, always try to cooperate and minimize the damage immediately.

Have an internal and external team at your disposal that can readily respond to the requests of the national data protection authority, seeking to reduce the risk of sanctions at their highest levels.

WHERE CAN I FIND THIS TOPIC IN THE LGPD?

Sections 52 to 54

LEARN MORE

Due to violations of LGPD standards, processing agents are subject to the following penalties:

- warning, which will include a deadline for the adoption of corrective measures;
- fine of up to 2% of the company or group income, limited to BRL$ 50 million per violation;
- communication of the violation after it is verified and its occurrence confirmed;
- blocking of personal data corresponding to the violation until it is corrected;
- elimination of personal data corresponding to the violation.

All the sanctions will be preceded by an administrative proceeding that guarantees ample defense of the violating party. The sanctions will be applied considering the particularities of each case and the following criteria:

- the seriousness and nature of the violation and personal rights affected;
- the good faith of the offender;
- the benefit sought by the offender;
- the economic condition of the offender;
- recurrence;
- degree of damage;
- cooperation of the offender;
- repeated and demonstrated adoption of internal mechanisms and procedures capable of mitigating the damage;
- adoption of good practice and governance policies;
- quick adoption of corrective measures;
- proportionality between the seriousness of the offense and the severity of the sanction.

When calculating the amount of the fine, the national authority may consider the total income of the company or group of companies.

The ANPD is exclusively responsible for imposing the sanctions set forth in the LGPD. ANPD's jurisdiction shall prevail over other entities or bodies of the governement, when related to data protection.

When applying sanctions with daily fines, the national authority must justify the application of sanctions, observing the seriousness of the violation and the extent of the damage or loss caused.

In incidents involving transnational leaks, the fines applied in one jurisdiction will not be compensated or reduced by those applied in another in which effects of the event were also verified.

MATTOS FILHO >

Mattos Filho, Veiga Filho,
Marrey Jr e Quiroga Advogados