

Machado
Meyer

M

FEDERAL LAW 13.709/18
PROVISIONAL MEASURE 869/18

**GENERAL DATA
PROTECTION LAW**

CONTENT

	pág.
Overview	3
1. Main goals	6
2. Main Concepts	8
3. Processing agents and national data protection authority	14
4. Data security and secrecy	17
5. Accountability	19
Civil accountability and duty to repair	20
Administrative sanctions	21
6. Labor and employment relations	22
7. Groups / dynamics of work to comply with LGPD	25
Fourth Industrial Revolution	26
Conclusions	27
Key trends in personal data protection	28
Compliance strategy	29
Basic plan	30
Our contact information	31

OVERVIEW

M

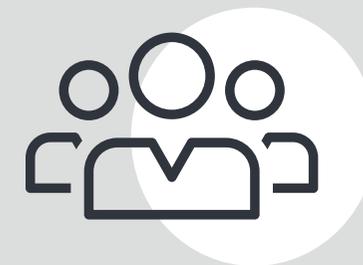
Law No. 13,709/18, or the General Data Protection Law (LGPD, in its acronym in Portuguese), sets forth rules for personal data protection and treatment in Brazil.

Inspired by the also recent General Data Protection Regulation (GDPR) of the European Union, its main purpose is to grant data subjects control over their personal data.

In the so-called data driven economy, driven by Big Data, the IoT, and artificial intelligence, businesses and transactions are increasingly based on data.

Transversality: the new act set forth rules for the use of personal data in Brazil, in the private and public sectors, regardless the method used for processing data, whether or not computerized, online or off-line.

Measures necessary to ensure compliance with the new legislation



Analysis of business model, mapping of personal data and analysis of the applicable rules.

Diagnosis and planning of technical and organizational measures to comply with the law.

Implementation of security measures, good practices and governance.

LGPD will result in important competitive impacts that should be addressed individually by each company in relation to its business model, considering the costs of compliance and rules governing the respective liability.

LGPD enters into force on August, 2020, 24 months after its official publication (art. 65, amended by PM 869/18)



1

MAIN GOALS

1 MAIN GOALS



RIGHTS	Ensuring a more robust system for protection of privacy and civil liberties.
STANDARDIZATION	Establishing more consistent rules, regardless of the industry.
ACCOUNTABILITY	Compliance with LGPD principles and the ability to demonstrate compliance with such principles.
INNOVATION	Fostering innovation.
LEGAL CERTAINTY	Ensure legal certainty and the data subject's trust in his/her data treatment.
DEVELOPMENT	Fostering economic development, ensuring free enterprise, free competition and consumer protection.



2

MAIN CONCEPTS

2 MAIN CONCEPTS



PERSONAL DATA

Any data related to an individual who may be identified from the data collected. This is the central concept of the LGPD, which seeks to guarantee the data subject's privacy related to his/her data treatment (art. 5, I).

DATA SUBJECT

An individual whose personal data is subject to data processing (art. 5, V).

PROCESSING

Any operation carried out with personal data, such as collection, use, processing, storage, and erasure (art. 5, X).

CONTROLLER

Individual or legal entity responsible for making decisions regarding personal data processing (art. 5, VI).

PROCESSOR

Any individual or legal entity performing personal data processing on behalf of the **controller** (art. 5, VII).

SCOPE OF APPLICATION

Individuals or private or public legal entities processing or collecting personal data in Brazil, or, further, processing it in order to provide goods or render services to data subjects located in Brazil, regardless of the means, country of their headquarters, or country where the data is located (art. 3).

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

The principles set forth in the art. 6 of **LGPD** should substantiate any operation of personal data processing and function as a test of compliance with the law. Processing activities shall observe the principle of good faith and the following principles:

- **Purpose:** must be legitimate, specific, explicit and informed.
- **Adequacy:** compatibility of the means used in view of the purpose.
- **Need:** limitation of processing to the minimum required to achieve its stated purpose.
- **Free access:** simplified and free consultation regarding the processing process guaranteed to the data subjects.
- **Quality of data:** guarantee of integrity of personal data and the right to keep it updated.
- **Transparency:** clear, accurate and accessible information about the processing conditions.
- **Security:** adoption of technical and administrative measures to protect personal data.
- **Prevention:** adoption of measures to prevent the occurrence of damages.
- **Non-discrimination:** prohibition on processing data for discriminatory, unlawful or abusive purposes.
- **Liability and accountability:** demonstration and proof of compliance with the law.

PROCESSING REQUIREMENTS

Personal data may only be processed in one of the following cases (**art. 7**):

- With the consent of the data subject.
- To comply with a legal or regulatory obligation of the controller.
- To execute public policies by the public administration as provided for in applicable legislation.
- To carry out studies for research bodies.
- Whenever it is necessary to perform under a contract or preliminary procedures involving a contract to which the data subject is a party, at the data subject's request.
- To regularly exercise rights in judicial, administrative or arbitral proceedings.
- To protect the life or physical integrity of the data subject or a third party.
- For the promotion of health, in the event of a procedure performed by healthcare professionals or providers.
- Whenever it is necessary to meet the legitimate interests of the controller or a third party, except when the fundamental rights and civil liberties of the data subject prevail and require protection of the subject's personal data.
- For credit rating / scoring.

DATA SUBJECT'S RIGHTS

The new **legislation** establishes the following rights of data subjects (**art. 18**):

- Confirmation that the personal data is being processed.
- Access to their personal data.
- Correction of personal data that is incomplete, inaccurate, or outdated.
- Anonymization, blocking, or deletion of unnecessary and/or excessive personal data, or data processed in disagreement with the provisions of the LGPD.
- Personal data portability to another product of the service provider.
- Deletion of data processed without their consent.
- Obtaining of information on public and private entities with which the controller shared personal data.
- Obtaining information on the possibility of not consenting to personal data processing and on the consequences resulting from her/his denial.
- Revocation of consent given for personal data processing.

INTERNATIONAL DATA TRANSFER

Allowed only in the cases set forth in the LGPD (art. 33), such as:

- To countries that ensure a level of personal data protection that is deemed adequate under the LGPD.
- When the transfer is necessary for protection of the life or physical integrity of the data subject or third party.
- **When the data subject has given his specific and prominent consent regarding the transfer.**

3

PROCESSING AGENTS AND NATIONAL DATA PROTECTION AUTHORITY

3 PROCESSING AGENTS AND NATIONAL DATA PROTECTION AUTHORITY



- The **controller** and the **processor** are personal data processing agents and, therefore, they must keep records on the processing operations they carry out (art. 37).
- The **controller** must designate the person responsible for personal data processing (art. 41), observing the following aspects.
 - Such person can be an individual or a legal entity.
 - Such person must act as a communication channel.
 - The contact information of such person must be readily available (art. 41, §1).
 - Such person must receive complaints and communications from data subjects, provide clarifications, take measures, receive notices from competent authorities, guide employees and third-party vendors of the operator on the practices to be adopted in relation to data protection, among other activities that may be established by the competent authorities (art. 41, §2).
- The **processor** must process data in accordance with instructions given by the controller (art. 39).

3 PROCESSING AGENTS AND NATIONAL DATA PROTECTION AUTHORITY



PM 869/18 established the National Data Protection Authority (ANPD, in its acronym in Portuguese):

- The ANPD will be composed of a board of directors (BoD), the National Council for the Protection of Personal Data and Privacy (CNPDP, in its acronym in Portuguese), an internal inspection body, an ombudsman's office, an advisory body and administrative/specialized units for the application of LGPD.
- The BoD will be composed by 5 members appointed by the Brazilian President, with mandates of 4 years.
- The CNPDP will be composed of 23 members, all of them appointed by the Brazilian President, with 11 being from the State level (6 of the Executive Branch, 1 from the Senate, 1 from the Chamber of Deputies, 1 from the National Council of Justice, 1 from the National Council of the Public Prosecution Service and 1 from the Internet Governance Committee in Brazil), 4 from civic society entities, 4 from scientific institutions and 4 from the business sector.

- The ANPD will be responsible, among other duties, for issuing rules and procedures intended to regulate and interpret the LGPD and for supervising and applying the sanctions of the new law.
- The ANPD will coordinate its activities with the National System of Consumer Protection of the Ministry of Justice and other agencies and entities with sanctioning and normative competencies related to personal data protection. It will also be the central body that will carry out the interpretation of the LGPD and that will enact standards and guidelines for its implementation.

4

DATA SECURITY AND CONFIDENTIALITY

4 DATA SECURITY AND CONFIDENTIALITY



- Processing agents must adopt **security measures** (art. 46):
 - From its design through the execution of the product or services.
 - Capable of protecting personal data against unauthorized access, accidental or illicit events.
- Data must be deleted if (art. 15):
 - the purposes for which it was collected have been fulfilled.
 - consent has been revoked.
 - demanded by competent authorities.
- Data may be stored (art. 16):
 - to comply with legal or regulatory obligations.
 - for the exclusive use of the controller, provided that it is not accessed by third parties and that is anonymized.
- Obligation to report within a **reasonable time** the occurrence of a **security incident** (art. 48).
- Duty to repair the damage: **joint** civil liability between the controller and the processor(art. 42), without prejudice of the imposition of administrative sanctions.
- **Good practices and governance rules** (art. 50).
- Minimum technical standards may be defined by the competent authorities.
- **Personal data protection Impact Assessment** (art. 38):
 - Description of the types of data collected;
 - Methodology used for collection; and
 - The controller's review regarding the measures, safeguards, and risk mitigation mechanisms adopted.

5

LIABILITIES



CIVIL LIABILITY AND DUTY TO REPAIR

- The processor must process personal data in accordance with instructions given by the controller, who must oversee the activities.
- Controller and processor are liable for any damages caused by the data processing activity in violation of the law.
- Processor is jointly liable for damages when it fails to comply with the legislation or when it does not follow the lawful instructions of the controller.
- Such liability does not exclude other administrative, civil or criminal sanctions under the Brazilian law.
- Scenarios for exemption from liability: (i) was not the one that carried out the personal data processing ascribed to them; (ii) although they carried out the personal data processing ascribed to them, **there was no violation of the data protection law**; and (iii) the damage results from the sole fault of the data subject or a third party.

ADMINISTRATIVE SANCTIONS

- The LGPD establishes very strict penalties (art. 52):
 - Warning.
 - Obligation to disclose the incident.
 - Deletion of personal data.
 - Fine of up to 2% of the income of the private legal entity, group, or conglomerate in Brazil in its last fiscal year, excluding taxes, limited to R\$50 million per infraction.
- The penalties above do not replace the application of administrative, civil, or criminal sanctions set forth in specific legislation (art. 52, §2).



6

LABOR AND EMPLOYMENT RELATIONS

- The employer is responsible for data processing.
- LGPD applies to all phases of the employment agreement:
 - Pre-hiring acts.
 - During the employment.
 - Outsourcing.
 - After termination of employment.

RECRUITING AND SELECTION

- Candidates must give express consent to data processing during recruiting, evaluation, and selection processes.
- Should a candidate not be hired, the company must delete the personal data collected.
- Caution when using prior information on candidates (existence of labor claims): personal data relating to the regular exercise of rights by the data subjects cannot be used against them (art. 21).

EMPLOYMENT

- Legal grounds for processing employees' personal data:
 - Performance of contract.
 - Compliance with legal obligations.
 - Legitimate interest.
- Obligation of transparency and internal policies:
 - Which data will be processed.
 - Which duties will be fulfilled with such data.
 - With which public entities such data will be shared.

AFTER THE TERMINATION OF EMPLOYMENT

- Once employment is terminated, the employee's personal data must be deleted, except:
 - When there is a legal obligation to keep documents.
 - To comply with inspections.
 - Labor claims.

OUTSOURCING

- Caution in outsourcing contracts and relationships with third parties.
- Data required for performance under contract? Dependson the kind of data.
- Recipients of services are responsible for the use of data.

7

GROUPS / WORK FLOW TO COMPLY WITH LGPD

FOURTH INDUSTRIAL REVOLUTION

"We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before".*

- Artificial intelligence
- Big Data
- Internet of Things
- Augmented reality
- Robotics
- Synthetic biology
- Nanotechnology

* Klaus Schwab, The Fourth Industrial Revolution.

CONCLUSIONS

- Debated in Congress since 2012, the **LGPD was a response to approval of the GDPR** and recent scandals regarding manipulation of personal data and data leaks. It also reflects **Brazil's desire to better integrate with the international markets.**
- The **European model has prevailed** since 2012.
- **Cross-functional and unique**, the law affects all economic sectors, including the public power.
- It is complex and challenges the implementation of **a strict data protection practice in an environment without this cultural tradition.**
- Generally speaking, the law **does not restrict business models**, but compliance will be complex.
- The law will affect aspects of **competitiveness in the market.**
- Initially vetoed, the ANPD was recreated without institutional autonomy.
- There are various unresolved issues with respect to enforcement of the law. The text is good, but the practice may not be.

KEY TRENDS IN PERSONAL DATA PROTECTION

INFORMATION SECURITY WILL BECOME A GROWING AND MORE COMPLEX PROBLEM

- Geopolitical and economic disputes drive more attacks and more significant problems.
- Compliance challenges arising from the need for increased and customized upgrades, as well as cost pressure to fund these processes.
- Greater concern with the entire supply chain, including technology services (SaaS, PaaS, IaaS).
- Cyber insurance: increased liability of organizations will demand assurance products against information breach, reputation damage, loss of operational capacity, upgrade costs, among others.
- As the use of technology and data processing grows to a vast scale, discussions on the trade-off between security and privacy become more frequent and painful.

PRIVACY AND DATA PROTECTION ARE A STRATEGIC BUSINESS ISSUE

- The general population is more aware of privacy and data protection issues; organizations will face increasing pressure for more accountability.
- Privacy laws will proliferate and make compliance more complex. Models that previously exempted platforms from liability tend to be reviewed.
- Use of personal data through IoT, AI and machine learning will be under increasing scrutiny and companies will face increasing pressure to demonstrate ethics, transparency and openness to public debate about the use of personal data.
- The discussion will cover not only the ownership of the data but also the ownership and control of data processing.
- Private and public organizations will have to explain the use of technologies such as facial recognition and other biometric solutions that will allow greater control of human identification and behavior.

COMPLIANCE STRATEGY

CAUTION, PRUDENCE AND ACTION - WE ARE STILL DEFINING WHAT LGPD WILL ACTUALLY BE

- The ANPD has not been implemented yet.
- There are several unresolved issues in the regulations.
- We do not have a culture of data protection in Brazil.
- Precedents are incipient and conflicting.

LOOK INSIDE-OUT

- The compliance process must also take into account the interaction with public power, considering how the regulation will be applied and how the communication with public entities (also required to comply with the law) will take place.

AN INTEGRATED VIEW

- The LGPD is a business problem. It involves compliance costs, but also requires the analysis of opportunities and a business perspective.
- In the current context, it is highly recommended to adopt a strategic view of compliance, which considers priorities and opportunities related to the business model.
- Compliance involves thinking about the present situation and the relationship with data subjects; the relationship with service providers, third parties and partners; and, finally, a forward-looking view that takes into account new business strategies and new products.
- Compliance is a cost in the short term, but it can be a competitive advantage over the long run.

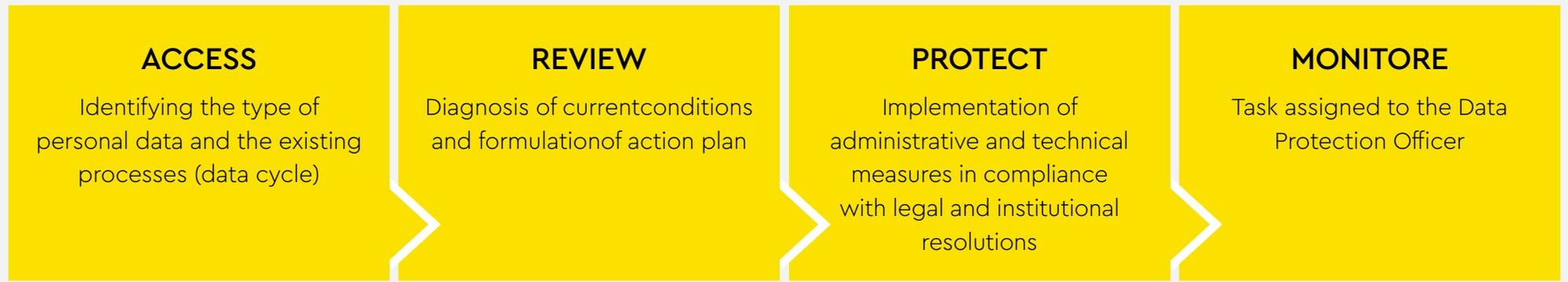
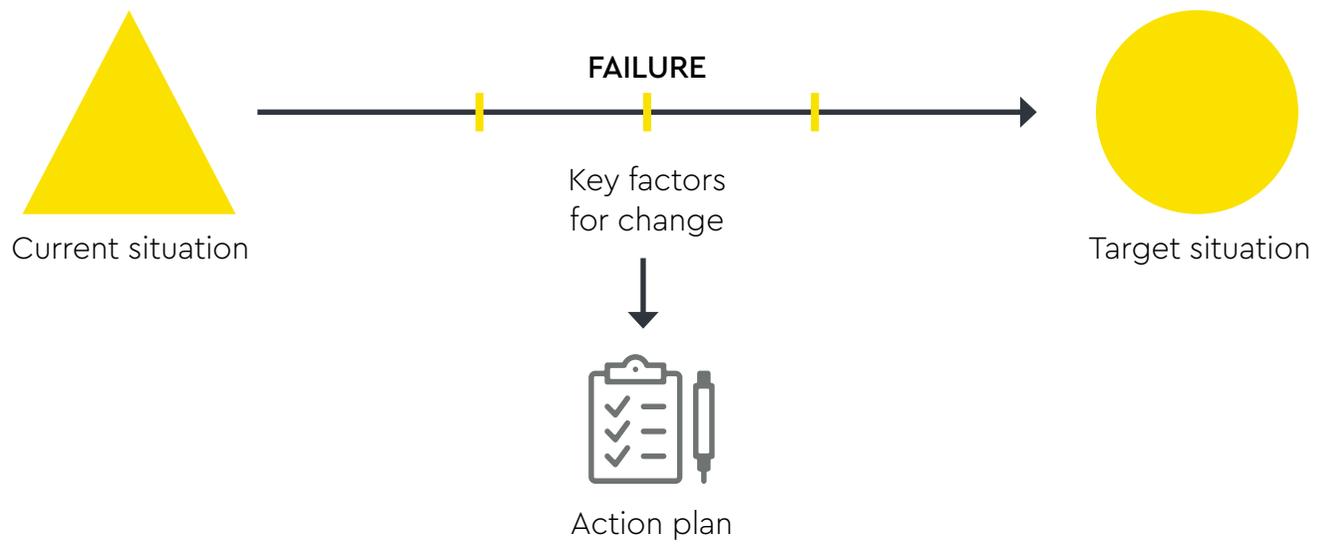
7 GROUPS / WORK FLOW TO COMPLY WITH LGPD



BASIC PLAN

First step:
ANALYSIS OF POTENTIAL INADEQUACIES

- Inadequacy IN legal obligations
- Analysis of internal corporate policies and practices





OUR CONTACT INFORMATION

ANDREA GIAMONDO
MASSEI ROSSI

PARTNER

agmassei@machadomeyer.com.br
+55 3150-7779

DANIEL
DIAS

PARTNER

dtd@machadomeyer.com.br
+ 55 11 3150-7478

DANIEL
GUARIENTO

PARTNER

dbt@machadomeyer.com.br
+55 11 3150-7778

DIEGO DE LIMA
GUALDA

PARTNER

dlgualda@machadomeyer.com.br
+55 11 3150-7774

EDUARDO
PERAZZA

PARTNER

epmedeiros@machadomeyer.com.br
+55 11 3150-7691

ELTON
MINASSE

PARTNER

eminasse@machadomeyer.com.br
+55 11 3150-7652

GLÁUCIA
COELHO

PARTNER

gmcoelho@machadomeyer.com.br
+55 11 3150-7198

LUANNA
R. PEPORINI

PARTNER

lpeporini@machadomeyer.com.br
+55 11 3150-7042

LEGAL INTELLIGENCE PORTAL

Our view on issues that affect your businesses.

Access our content: www.machadomeyer.com/legalintelligence

