CAPCO

THE COUNTDOWN TO LGPD

HOW TO COMPLY WITH THE BRAZILIAN GENERAL DATA PROTECTION LAW

GENERAL CONTEXT IN DETAIL – WHAT IS LGPD?

LGPD is the acronym for Lei Geral de Proteção de Dados (General Data Protection Law). Specifically, it refers to Law No. 13,709 from 2018, which lays down rules regarding personal data processing by individuals or corporations mainly to protect the fundamental rights of freedom and individual privacy.

What is the origin of LGPD?

The general definitions of the LGPD started with Act 12,065/14, known as a civil rights framework for the internet." After Europe enforced GDPR (General Data Protection Regulations), the Brazilian agency responsible for the law, started revising it and introduced updated regulations and concepts. Then, on August 14, 2018, the 'first current version' of LGPD was passed.

Who does the LGPD apply to?

The LGPD applies to any processing operation conducted by individuals or corporations, regardless of the means, the country where they are based or the country that the data is located, provided that:

- The processing operation is performed in the territory of Brazil
- Data processing activities are related to the offering of goods or services or to processing of data of individuals who are within the territory of Brazil
- Personal data processed have been collected in Brazil

But beware! The law is not applicable if the data is processed for strictly personal purposes, and not commercial purposes, or if the data is exclusively for journalistic purposes, for national security, national defense, or criminal investigation activities.

When does the law come into effect?

As of the publication of this article in June 2020, LGPD will take effect in January 2021, with sanctions that can be applied from August 2021. However, there are discussions in the Brazilian Congress on the postponement of these dates, due to COVID-19, understanding that part of the companies would not be prepared to meet the requirements of the law.

What will change in organizations?

There will be many changes. The main change refers to the 'purpose' of inspections. Once LPGD comes into effect, companies should not wait for inspections or audits to make adjustments. They must proactively inform the ANPD (Brazil's National Data Protection Authority) about their compliance with the Law, especially in terms of the relationship with personal data owners (individuals) and contracts with processors.

The roles of parties involved in the personal data processing lifecycle have also changed. All organizations must be aware of these concepts and identify them within their structures to make it possible to identify all involved parties so that any potential actions can be adequately addressed.

What are the consequences of noncompliance?

If data leaks, severe financial sanctions may be imposed against organizations, and regulators can add up to 2 percent

GENERAL CONTEXT IN DETAIL – WHAT IS LGPD? (CONTINUED)

of the annual sales revenue of the company with a cap set at fifty million reais (BRL 50,000,000.00) per violation. There are also other consequences, such as daily fines for each day of noncompliance until the organization makes the necessary technical and organization adjustments, blocking personal data (related to the violation), and warnings with a deadline for corrective actions to be taken.

One point to highlight is that if any violation occurs, the controller, and not the processor or data protection office, is accountable. However, the last two are involved in the recovery plan. Read more about these roles in section two of this article.

Another consequence concerns the company's reputation. Any company whose clients' data leaks may watch its shareholders withdraw money they invested in the organization or lose the trust of its clients, who may ask their data to be transferred to a competitor (see item 1.6.6 of this article).

ANPD (Brazil's National Data Protection Authority) will examine violations on a case by case basis and validate, for example, whether the company has taken preventive actions, such as adopting good practices and putting proper governance in place, or corrective actions. These outcomes will affect decisions on the sanction to be applied.

What are the advantages for the general population?

Once the LGPD comes into force, all Brazilian citizens will have protections in place to ensure the transparency of their personal data processing.

Citizens will have:

- **Right to be informed:** data subjects must be informed, clearly and transparently, of the collection and processing of their data, as well as of the intended purpose
- **Right to access:** data subjects must have free access to their data
- **Right to rectification:** data subjects will have the right to have any inaccurate data corrected
- **Right to deletion:** data subjects will have the right to be forgotten, that is, to delete their data from the controller's database. However, it is essential to highlight that, upon the controller's legitimate interest, the controller may keep specific data, e.g., data related to debts
- **Right to limit processing:** data subjects will have the right to request that their data stop being processed
- **Right to portability:** this refers to exporting personal data to be sent to data subjects or another controller
- **Right to objection:** this refers to the individual's right to object to the processing of their data.
- **Right involving automated decisions:** data subjects have the right not to be exclusively subject to decisions based on automated processing, including being included in profiles

GENERAL CONTEXT IN DETAIL – WHAT IS LGPD? (CONTINUED)

What should happens if personal data leaks?

If personal data leaks, the controller must report what happened to the national authority and the data subject.

Article 48 of the law describes that the breach shall be reported: "in a reasonable time period." Thus, the GDPR standards should apply, i.e., the controller shall notify the breach to regulators no later than 72 hours afte become aware of it.

The notification must contain, at least, a description of the breached personal data, information on the data subjects concerned, technical and security measures taken to protect the personal data (keeping trade and industrial secrets confidential), any risks related to the incident; and the measures that were/ are being taken to cancel out or mitigate the adverse effects.

Communication and governance for cases of data leaking should be implemented to ensure the process is standardized and traceable by the ANPD (Brazil's National Data Protection Authority).

GENERAL DEFINITIONS

The definitions below must be known by all organizations which the law applies to, as the ANPD will include these terms in its communications and audits.

ANPD - Brazil's National Data Protection Authority

Introduced by law 13,853, 2019, the ANPD is a federal government body tied to the Brazilian Presidency. It will help regulate and supervise compliance with the LGPD, including amending data protection rules, monitoring compliance with the law, implementing tools to improve communication among companies, authorities and data subjects, conducting studies on data protection abroad, and applying sanctions.

Controller

The LGPD defines the controller as "individual or legal entity, governed by public or private law, that will make the decisions on personal data processing."

The controller is responsible for ensuring that personal data are processed per the LGPD requirements and will usually be the entity having direct contact with the public.

The legal burden of the GDPR and LGPD falls mainly on the controller, i.e., the controller is accountable should violations occur and must ensure personal data are processed following the regulations.

GENERAL DEFINITIONS (CONTINUED)

The controller's core activities include:

- Defining the purpose of processing activities
- Appointing a DPO (if required by law)
- Safeguarding data subjects rights
- Adopting technical and organizational measures to ensure the protection of personal data and to demonstrate data processing complies with regulations
- Implementing appropriate policies and governance
- Conducting data protection impact assessments (DPIAs)
- Ensuring third-party processors abide by GDPR and LGPD rules
- Reporting any personal data violations to the supervisory authority and data subject, when required

Processor

The LGPD defines the processor as "individual or legal entity, governed by public or private law, that processes personal data on behalf of the controller."Processors are entities engaged by the controller to perform functions related to personal data.

The controller's core activities include:

- Undertaking processing activities under the supervision of a controller
- Ensuring people authorized to process personal data undertook to keep such data confidential or are under a statutory confidentiality obligation
- Raking all measures to keep data processing safe
- If a processor infringes the LGPD and is the one responsible for defining the purposes and processing methods, they will be considered a controller of such processing. Meaning, in the event of a violation, the primary responsibility will fall on the processor
- Determining the technical aspects of data processing, such as the systems used for processing, how data are stored, security measures, transfer mechanisms, etc

Note: The processor should not subcontract another processor without the controller's specific prior authorization in writing.

Data Protection Officer (DPO)

This is one of the roles introduced both by the GDPR and LGPD.

Also globally known as Data Protection Officer (DPO), as defined by the LGPD, a "person appointed by the data controller and processor to act as an intermediary between the controller, data subjects and the ANPD (Brazil's National Data Protection Authority)."

Below are some considerations on this role:

- The DPO must report to the controller's highest management level, ideally being part of a risk/compliance or governance department

GENERAL DEFINITIONS (CONTINUED)

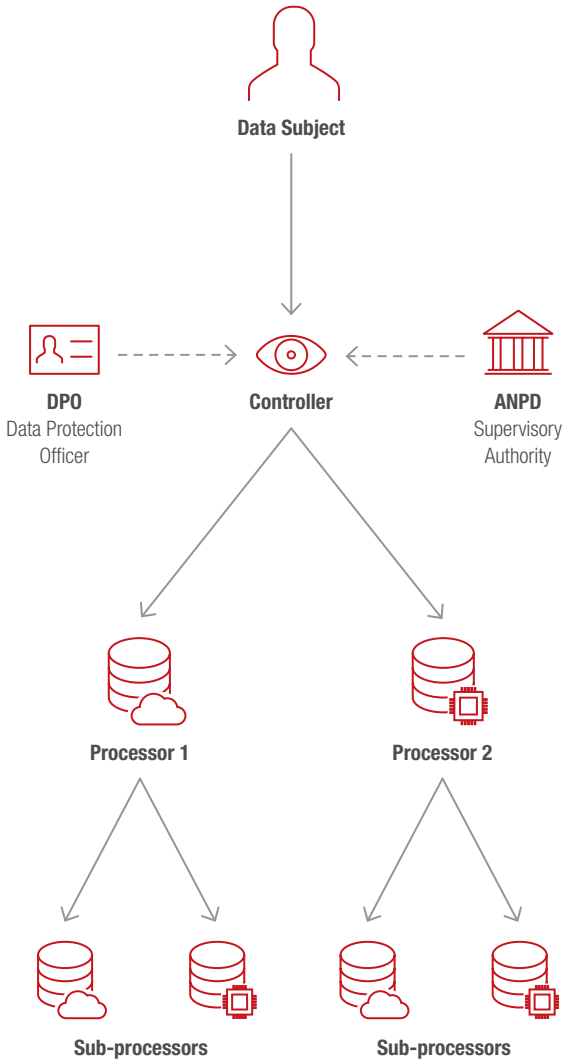
- In the personal data life cycle, the DPO can exist both for the controller (Company A) and the processor (Company B). Please see item 2.5 for greater clarity
- The DPO does not need to be an in-house employee or someone dedicated to this role
- A single DPO (provided that they are easily accessible) can be appointed by "a group of undertakings" and by "a group of public authorities or bodies." (Article 37 (2) of GDPR)

The DPOs core activities include:

- Informing and advise the controller or processor and as employees of their obligations under the GDPR and LGPR
- Monitoring compliance with GDPR/LGPD, including tracking documents, processes and records
- Giving advice, when asked for, related to the data protection impact assessment (DPIA)
- Cooperating with the supervisory authority
- Acting as liaison with the supervisory authority

Relationships between Controller, Processor, DPO, and ANPD

The following graphic helps illustrate the relationship among these roles. While this is a helpful example, the relationship is not limited to this format. Depending on the complexity of processing a processor can also be a controller and vice-versa.



Relationship between the roles provided in the LGPD

Please note that the DPO can be someone external to the organization. That is, the DPO can be the officer in one or more organizations. Under the LGPD and as described in this article, the DPO must be an individual and not a legal entity.

GENERAL DEFINITIONS (CONTINUED)

Personal Data and Sensitive Personal Data

According to the formal definition under the law, personal data means any information relating to an identified or identifiable individual.

Personal data is not limited to information that, if misused, can negatively affect the private and family life of an individual. Where the information is located is not relevant: personal data encompasses information available in any way – text, pictures, charts, photos, videos, acoustics, or any other possible means that allow data subjects to be directly or indirectly identified.

Sensitive personal data is any piece of information pertaining to racial or ethnic origin, political opinions, trade union membership, religious, philosophical or political associations, health-related data, data concerning a person's sex life or sexual orientation, genetic or biometric data.

Organizations need to provide firmly grounded justifications for the processing of sensitive personal data and may require formal consent from ANPD. The DPO will guide on a case by case basis.

DPIA - Data Protection Impact Assessment

Also known as DPIA, or Data Privacy Impact Assessment, the Data Protection Impact Assessment helps identify specific risks to personal data relating to processing activities. This assessment is more focused on the risk assessment required by ISO/IEC 27001.

The DPIA is a legal requirement under the LGPD. It must be conducted by the processor, with the support of the controller and DPO, and whenever needed to understand data processing better, assessing the necessity and proportionality of the processing operations.

Considerations:

- DPIAs identify and minimize privacy risks related to data processing
- DPIAs must be conducted before new processes, projects or policies are implemented; or
- DPIAs must be conducted to review existing systems

Under article 38 of the LGPD, the Data Privacy Impact Assessment Report (RIPDP, acronym in Portuguese) must contain at least:

- Description of the types of data collected
- The methodology used to collect information and ensure it is safe
- The assessment made by the controller concerning:
    - Measures
    - Safeguards
    - Risk mitigation mechanisms

WHAT DOES MY COMPANY NEED TO BE PREPARED?

If you have read this article up to this point, you must have noticed that the LGPD is far-reaching and complex and requires more than just amending contracts or taking technical security measures, such as firewalls, data encryption, etc.

Make sure that, from this point, you make a global assessment of your organization under the legal and technical requirements. Below are some actions you may take, broken down according to the main concepts presented.

Internal policies

- Review and adjust the (internal and third party-related) policies, contracts, procedures and other activities involving personal data processing (client and employee data) to the principles established in the LGPD

- Keep records, preferably in writing, to demonstrate that you are taking measures to adjust processing activities to the principles established in the LGPD, regardless of the size of the existing database

Legally

- Review and amend third-party (processors) contracts, requiring proof that they have taken technical measures to comply with the LGPD and ensuring the processing activity to be undertaken is clear

- Carefully assess which lawful basis for data processing can be used in your case

- When personal data processing is based on consent, the controller must keep the documents that prove the origin of the data

- When personal data processing is based on legitimate interest, the controller must take measures to ensure data processing is transparent (the ANPD can always review this) and keep records of such processing

Data subject rights

- Make adjustments to your organization's technical and operational structure to enforce and respect all rights established by the law for data subjects

- Develop mechanisms for allowing data subjects to exercise their rights (item 1.6 of this article), quickly and for free

- Check whether the information available to data subjects has clear and appropriate language

- In the case of children's personal data processing, information must be provided in a simple, clear, and accessible way, considering physical motor, perceptual, sensory, intellectual, and mental skills of the target audience.

WHAT DOES MY COMPANY NEED TO BE PREPARED? (CONTINUED)

Obligations

- Adopt technical measures to ensure data are safely processed
- Develop internal processes and create policies that allow for creating and keeping records of data processing activities
- Store the data to fulfill the purpose they were collected for and meet legal and regulatory obligations;
- Appoint the officer (DPO) responsible for processing personal data

International data transfer

- Be careful when sending data to organizations abroad and make sure they comply with the requirements set out in the LGPD
- Adopt procedures and draw up documents, including contracts and binding corporate rules, which document data processing adjustments to the LGPD requirements
- Inform Brazil's national authority of any changes made to guarantees that have been considered sufficient for the international transfer of data

Security and Notifications

- Develop systems to identify and fight security incidents, as well as train an IT team to ensure these procedures are followed
- Create policies and a governance structure, ensuring that technical service providers and legal advisors also follow the same procedures
- Review insurance contracts to ensure coverage in case of security incidents

Sanctions

- Assess whether data processing activities meet the LGPD requirements to identify full compliance with the law. In case of violation, always seek to cooperate and minimize the damage promptly
- Have an internal (and external, if needed) team available to immediately meet the needs of the Brazilian Data Protection Authority, aiming to reduce the risk of having the most onerous sanctions imposed

AUTHOR

Rodrigo Constantino, Principal Consultant
Data Protection Officer - Exin Certified
Rodrigo.Constantino@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO