INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

Brazil

Introduction

The Brazilian General Data Protection Law ("LGPD"), enacted in 2018 and enforced since 2020, serves as the cornerstone of the country's data protection framework. Its primary objective is to ensure the fundamental rights of data subjects and regulate how personal data is processed by processing agents. The LGPD outlines the rights and obligations of data controllers and processors, establishes enforcement mechanisms through sanctions and inspections, and fosters overall governance of data processing activities.

Before the LGPD, data protection and privacy rights were governed by a patchwork of sector-specific laws covering areas like consumer rights, finance, healthcare, the public sector, and criminal law. Additionally, the Civil Rights Framework for the Internet ("Marco Civil da Internet"), enacted in 2014 with its accompanying decree, laid the groundwork for processing personal data online.

Governing Data Protection Legislation

2.1.Overview of principal legislation

The LGPD, Federal Law No. 13,709/2018, aims to safeguard the fundamental rights of freedom and privacy, fostering the personal development of individuals. It represents a major regulatory advancement, aligning Brazil's data protection legislation with international standards. Signed by the President on August 14, 2018, published on August 15, 2018, and taking effect on September 18, 2020, the LGPD marked a significant shift in how personal data is treated in Brazil.

Further emphasizing this importance, the protection of personal data was expressly recognized as a fundamental right in Brazil's Federal Constitution (Article 5, LXXIX) in 2022. This inclusion highlights the high level of protection and priority assigned to safeguarding personal data within the country.

Contact Us

+55 (11) 3799-8100

https://klalaw.com.br/en/home/

accesar@klalaw.com.br

Av. Brigadeiro Faria Lima, 1355
São Paulo, SP 01452-919 Brazil

2.2. Additional or ancillary regulation, directives or norms

A key provision of the LGPD is the establishment of the Brazilian Data Protection Authority ("ANPD"). Beyond its main role in overseeing data processing and legislation adherence, the ANPD also offers comprehensive guidance and clarification on complex and important issues encountered by data controllers in their operations.

The ANPD has issued several regulations to enhance clarity and compliance within the LGPD framework, including the Regulation of the Inspection and Administrative Sanctioning Processes, specific to the ANPD's role and authority. The Authority has also issued regulations for applying the LGPD to small-scale data controllers and on the application of penalties, among others.

Scope of Application

3.1. Legislative Scope

The LGPD applies to any personal data processing activity carried out by individuals or legal entities, whether private or public. This applies regardless of the processing method (online or offline), the company's headquarters location, or the data's location, provided that: (i) the processing is performed in national territory; (ii) the processing activity has the purpose of offering or providing goods or services to individuals located in the national territory; (iii) the processing activities have, as purpose, the processing of data from individuals located in the national territory; or (iv) when the personal data has been collected in the national territory.

The country in which the processing agents were incorporated or have head offices, the nationality and place of residence of the data subjects and the country where the data is located are all elements that are considered irrelevant to the assessment of whether the LGPD shall apply to a given processing activity.

3.1.1. Definition of personal data

Personal data is defined as any information related to an identified or identifiable natural person. Under the LGPD, personal data encompasses not only directly identifying information, such as names, and identification numbers, but also information that, when combined or utilized in conjunction, enables the identification of an individual.

3.1.2. Definition of different categories of personal data

Sensitive personal data is classified as any personal information related to an individual's racial or ethnic origin, religious beliefs, political opinions, membership in trade unions, or religious, philosophical, or political organizations, as well as data concerning health, sexual life, and genetic or biometric details. The processing of these categories of personal data poses significant risks

to an individual's fundamental rights and freedoms, necessitating a higher standard of protection under the Law.

Anonymized data refers to information about a data subject that cannot be identified, considering the use of reasonable technical means available at the time of processing. The anonymized data falls outside the scope of the Law.

3.1.3. Processing of personal data and its different categories

The LGPD mandates that the processing of personal or sensitive personal data must follow the legal bases established for each category of data, as detailed in Articles 7 and 11. Information on the legal bases can be found in Section 5.1 of this Guideline.

3.2. Statutory exemptions

The LGPD and its regulations are designed to govern the processing of personal data about identified or identifiable natural persons. Consequently, data exclusively associated with legal entities (for example, The Brazilian National Registry of Legal Entities), falls outside the purview of the legislation.

Furthermore, the LGPD does not apply to data processing that is conducted by natural persons solely for personal, non-commercial purposes, or data processed exclusively for journalistic, artistic, public security, national defense, state security, or in activities connected with the investigation and repression of crimes. Additionally, data originating from outside Brazil that is not subject to communication or shared use with Brazilian processing agents is also exempt from the scope of the LGPD.

3.3.Territorial and extra-territorial application

Article 3 of the LGPD states that any processing activity conducted by a natural person, or a legal entity is subject to the law, irrespective of where the entity is located or where the data resides. This applies if the activity meets any of the following conditions: (i) the processing occurs in Brazil; (ii) the processing aims to offer goods or services or involves handling personal data of individuals in Brazil; or (iii) the personal data being processed was collected in Brazil.

Consequently, due to the extraterritorial application of the LGPD, factors such as the country of incorporation or location of the processing agents' head offices, the nationality and residence of the data subjects, and the location of the data are deemed irrelevant in determining whether the LGPD applies to a specific personal data processing activity.

Legislative Framework

4.1.Key stakeholders

4.1.1 Data subject

The term ‘data subject’ refers to the natural person associated with the personal data being processed. Essentially, it denotes the individual who is related to the personal data.

4.1.2. Controller

The controller is defined as the "natural or legal person, whether governed by public or private law, who is responsible for decisions relating to the processing of personal data". As the primary authority, the controller decides the purposes for which personal data is processed and sets the guidelines for processors on how to handle this data processing on their behalf.

4.1.3 Processor

The processor is defined as the “natural or legal person, whether governed by public or private law, who carries out the processing of personal data on behalf of the controller”. In practical terms, the processor is most often a company hired by the controller to carry out data processing following instructions provided by the controller.

Additionally, it is a common practice for processors to engage sub-processors to assist in data processing activities. Although the LGPD did not initially define this concept, the ANPD later acknowledged its legality. This recognition was made in the ANPD's 'Guidelines for Definitions of Personal Data Processors and DPO', where a sub-processor is defined as an entity 'hired by the processor to aid in processing personal data on behalf of the controller.' The Guidelines also clarify that the sub-processor maintains a direct relationship with the processor, rather than with the controller.

4.1.4 Data Protection Officer (“DPO”)

The Data Protection Officer (“DPO”) is designated by the controller to serve as the liaison among the controller, data subjects, and the ANPD. According to Article 41, the controller must appoint a DPO, who will oversee the data processing operations.

According to ANPD’s resolution[1], small processing agents are exempt from appointing a DPO. These agents include micro-enterprises, small businesses, startups, and legal entities governed by private law, such as non-profit organizations, as defined by current legislation. This category also extends to natural persons and depersonalized private entities involved in personal data processing and undertaking the typical responsibilities of a controller. However, if a small processing agent decides not to appoint a DPO, they must establish an alternative communication channel with the data subjects, to comply with the resolution.

[1] CD/ANPD RESOLUTION No. 2, OF JANUARY 27, 2022. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper

4.2. Role and responsibilities of key stakeholders

4.2.1 Controller

The Law defines the controller in Art. 5, item VI as a "natural or legal person, public or private law, to whom the decisions regarding the processing of personal data are incumbent." The controller acts as the key processing entity responsible for setting the purposes for personal data processing.

This role involves specifying the objectives, methods, and extent of personal data handling. Under the LGPD, the controller's essential duties include: (i) adopting adequate measures to safeguard the security and confidentiality of personal data; (ii) maintaining records of processing activities ("ROPA"); (iii) providing directives to processors operating under their guidance; (iv) alerting the ANPD about any personal data breaches that require reporting; (v) conducting a Data Protection Impact Assessment ("DPIA") to secure personal data, particularly sensitive personal data, concerning its processing activities.

4.2.2 Processor

The Law defines the processor in Art. 5, item VII as a "natural or legal person, public or private law, who processes personal data on behalf of the controller." As an agent tasked with processing personal data for the controller, the processor has several responsibilities, such as: (i) adhering to the controller's instructions; (ii) maintaining the security and confidentiality of the personal data; (iii) returning or erasing the personal data upon the controller's request; and (iv) documenting the ROPA.

Under the Law, processors are jointly liable with the respective controllers for any damages arising from their processing activities if they violate legal obligations or disregard instructions from the controller. In instances of non-compliance by the processor, they will be considered, for liability purposes under the LGPD, as equivalent to the controller.

4.2.3 DPO

The DPO attributions defined by the Law are: "(i) to accept complaints and communications from the data subjects, provide explanations and take action about such communications; (ii) to receive communications from the ANPD and take action about such communications; (iii) to advise the employees and any independent contractors of the company on its practices about the protection of personal data; (iv) to perform any other attributions determined by the controller or established in complementary norms."

Requirements for Data Processing

5.1. Grounds for collection and processing

The LGPD provides that personal data processing activities carried out

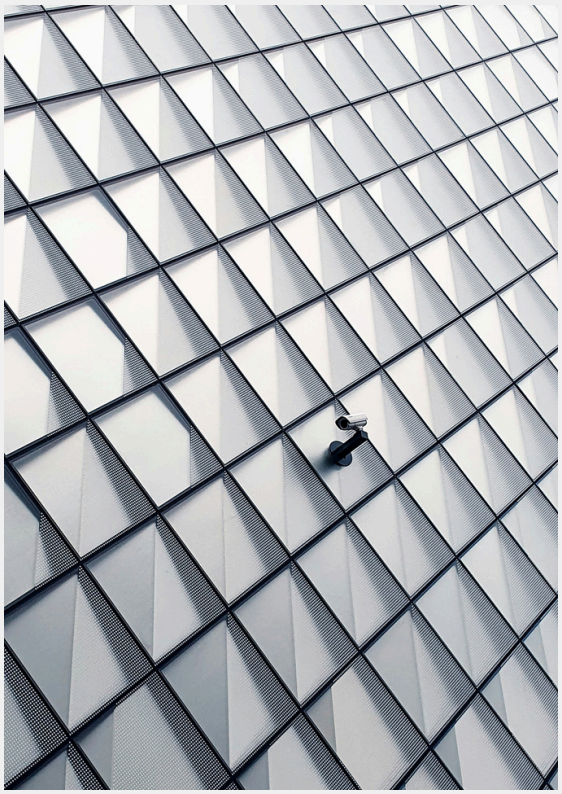
by entities may only be performed when relying on the following legal basis:

1. when the data subject has consented to the processing;
2. for the compliance with legal or regulatory obligations by the controller;
3. by the public administration, for the processing and shared use of data necessary for the execution of public policies provided in laws or regulations, or based on contracts, agreements or similar instruments, subject to the provisions of Chapter IV of this Law;
4. for carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data;
5. when necessary for the execution of a contract or preliminary procedures relating to a contract to which the data subject is a party;
6. for the regular exercise of rights in judicial, administrative, or arbitral proceedings;
7. for the protection of life and physical integrity of the data subject or third parties;
8. for the protection of health, in procedures performed by professionals of the health area or by sanitary entities;
9. when necessary to comply with the legitimate interests of the controller or of a third party, except when the fundamental rights and freedoms of the data subject prevails; and
10. for the protection of credit.

The art. 11 of the LGPD states that the processing of **sensitive personal data** can only be carried out:

1. with the express consent of the data subject or person responsible, for specific purposes or;

without the consent of the data subject, in cases where it is indispensable for:



2. compliance with a legal or regulatory obligation by the controller;

3. shared processing of personal data necessary for the execution, by the public administration, of public policies provided for in laws or regulations;

4. for studies carried out by research bodies, guaranteeing, whenever possible, the anonymization of sensitive personal data;

5. regular exercise of rights, including in contracts and in judicial, administrative, and arbitration proceedings;

6. protection of the life or physical safety of the data subject or a third party;

7. protection of health, exclusively in procedures carried out by health professionals, health services or health authorities; or

8. guaranteeing the prevention of fraud and the security of the data subject in processes of identification and authentication of registration in electronic systems.

Remarks on Consent: The LGPD defines consent as a freely given, informed, and unambiguous indication that the data subject agrees with the processing of their personal data for informed purposes. Consent must always be given in writing or by other means that evidence the effective manifestation of the data subject's free will, always under a clause separate from other contractual clauses and shall relate to determinate purposes, provided that any generic consent shall be deemed null. The data subject may, at any time, revoke their consent through a free and facilitated procedure that must be made available by the controller.

5.2. Data storage and retention timelines

Article 15 of the LGPD stipulates that personal data processing must cease upon the occurrence of any of the following conditions: (i) the purpose for processing the personal data has been achieved, or the data is no longer necessary or relevant for that specific purpose; (ii) the designated processing period concludes; (iii) the data subject requests the termination of processing, including as part of their right to withdraw consent, while considering public interest; or (iv) the ANPD mandates cessation due to a breach of the LGPD's regulations.

The LGPD mandates that, following the conclusion of personal data processing activities, the personal data must be deleted within the operational and technical constraints of these activities. However, personal data retention is permitted under specific conditions: (i) to fulfill a legal or regulatory obligation by the controller; (ii) for research purposes by a research entity, ensuring anonymization of the personal data whenever possible; (iii) for transfer to a third party, subject to adherence to the LGPD's data processing requirements; or (iv) for the controller's exclusive use, without third-party access, provided the data is anonymized.

5.3. Data correction, completion, updating or erasure of data

As established in Section 6.1, Article 18 of the LGPD grants data subjects

different rights regarding their personal data. Among these, individuals have the right to request that the controller correct any incomplete, inaccurate, or outdated personal data at any time upon their request.

5.4. Data protection and security practices and procedures

The LGPD mandates that controllers and processors implement technical and administrative safeguards to protect personal data against unauthorized access, as well as against accidental or illegal destruction, loss, alteration, disclosure, or any other form of improper processing.

Moreover, the Law encourages the development and implementation of best practices and governance frameworks by these entities. This encompasses addressing organizational conditions, operational protocols, internal procedures (including handling data subject requests), security policies, technical standards, specific responsibilities for those engaged in processing activities, educational initiatives, internal monitoring, and mechanisms for mitigating risks.

In this context, the ANPD is empowered to define minimum technical standards for data security and confidentiality. Reflecting this, in 2021, the ANPD released the Information Security Guide for Small Processing Agents to outline a range of security measures tailored to small-scale agents.

5.5. Cross-border transfer of data

Article 33 of the LGPD specifies the conditions under which international data transfer is permitted, including: (i) to entities in countries or international organizations that offer a level of personal data protection comparable to the LGPD; (ii) when the controller demonstrates adherence to LGPD principles and data subject rights through specific agreements or mechanisms like standard data protection clauses, corporate rules, or codes of conduct approved by the ANPD; (iii) for international legal cooperation among public intelligence or law enforcement agencies; (iv) to protect the life or physical safety of the data subject or others; (v) with authorization from the ANPD; (vi) under international cooperation agreements; (vii) for executing public policies or services; (viii) with explicit consent from the data subject, clearly informed about the transfer's international aspect; and (ix) to meet the requirements in items II, V, and VI of Article 7.

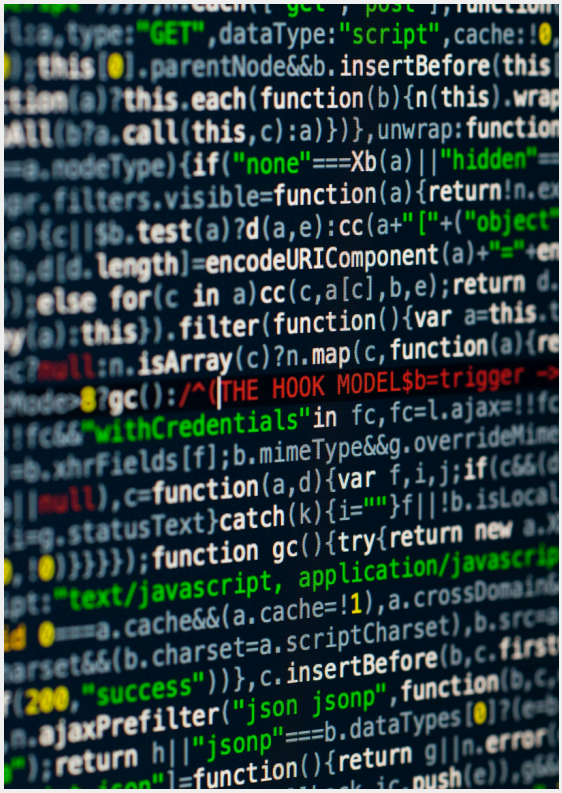
Furthermore, the ANPD is developing a regulation to specifically address international data transfers, covering definitions, requirements, transfer methods, approval processes, and standard contractual clause models for such transfers

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

The LGPD grants data subjects with the following rights, among others:

- obtain confirmation about the existence of processing activities of their data;
- access the data that is subject to processing;
- the right to correct incomplete, inaccurate or outdated data;



- have unnecessary or excessive data anonymized, blocked or eliminated;
- portability of data to a different provider of goods or services;
- eliminate data that is processed based on their consent;
- obtain information about public and private entities with which their data is shared;
- obtain information on the possibility of not giving their consent and also on the consequences of such an option;
- revoke their consent; and
- petition against the controller before the ANPD as well as before consumer defense bodies, where applicable.

Data subjects also have the right to request the revision, by a natural person, of decisions made exclusively based on automated personal data processing activities that affect their interests, including any decisions that are destined to define their personal, professional, consumer, or credit profile, or the aspects of their personality.

Data subjects shall have simplified access to information about the processing of his/her personal data, which shall be made available in a clear, adequate, and ostensive form, indicating: (i) the specific purposes of processing; (ii) the form and duration of the processing; (iii) the identification and contact information of the controller; (iv) information on the shared use of data by the controller and the purposes of such shared use; (v) the responsibilities of the agents involved in the processing; and (vi) the rights of the data subject.

https://klalaw.com.br/en/home/

6.2. Duties

No duties are imposed on data subjects under the LGPD.

Processing of Children or Minors' data

The LGPD is based on the premise that the processing of children's and adolescents' personal data must respect their fundamental rights, especially the right to freedom, privacy, and the free development of their personality. This entails considering the unique needs and preferences of each child or adolescent in an individualized and contextualized manner whenever there are multiple interpretations or applications of the Law.

In May 2023, the ANPD released Statement No. 01/CD/ANPD, acknowledging that the processing of personal data of children and adolescents is justified by all the legal bases outlined in the LGPD, as long as the minor's best interests are observed and prevail, to be assessed in the specific case, by art. 14 of the Law.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

The ANPD, as the central authority responsible for ensuring the protection of data subjects' personal data, oversees data processing activities and regulates any matters that require further clarification under LGPD. Established as an autarchy of a special nature linked to the Ministry of Justice and Public Security, the ANPD began its activities in November 2020.

In addition to the ANPD, other authorities also play roles in data protection cases within their specific competencies. For instance, the Consumer Protection and Defense Foundation (PROCON) may apply sanctions provided in the Consumer Protection Code to data processing agents who violate data subjects' rights in connection with consumer rights. Meanwhile, the Judiciary Branch is responsible for adjudicating any lawsuits involving privacy and the protection of personal data, such as claims for compensation for moral or material damages arising from data leaks or misuse of personal data.

8.2. Role, functions and powers of authorities

Among the functions and powers assigned to the ANPD are the duties to (i) ensure the rights of data subjects, (ii) supervise personal data processing activities carried out by public and private agents, (iii) apply administrative sanctions in the event of violations of the LGPD, (iv) guiding and educating society on the rights and duties related to personal data, and (v) promoting national and international cooperation on the subject.

8.3. Role, functions and powers of civil/criminal courts in the field of data regulation

The Judiciary Branch's role is to analyze, interpret the LGPD, and resolve legal disputes concerning privacy and data protection.

However, it does not have the authority to regulate data protection matters. Instead, its responsibility is to enforce and apply the regulations and guidelines already established by the LGPD and the ANPD.

Consequences of non-compliance

9.1.Consequences and penalties for data breach

Article 48 of the LGPD mandates that any controller or processor who, due to their personal data processing activities, causes property, moral, individual, or collective damage to others in violation of the LGPD, is required to provide compensation for such damage. This ensures that data subjects receive effective compensation for any harm they suffer due to non-compliance with data protection laws.

The LGPD stipulates that processors share joint and several liability with controllers for any damages caused by processing activities. This applies if they fail to comply with data protection laws or disregard lawful instructions from the controller. In such cases, processors are held equally responsible alongside controllers for any resulting damages.

Additionally, in cases where there are joint controllers directly involved in the processing activity that leads to damage, they are deemed jointly and severally liable. This means that each controller can be held responsible for the full amount of the damage, providing a stronger protection mechanism for data subjects.

https://klalaw.com.br/en/home/

Importantly, Article 43 of the LGPD outlines scenarios in which processing agents may be exempt from liability. These exemptions apply if the processing agents can demonstrate (i) that they did not perform the personal data processing activity assigned to them; (ii) that they did perform the assigned processing activity, but there was no violation of data protection legislation; or (iii) that the damage is solely due to the fault of the data subject or a third party.

9.2. Consequences and penalties for other violations and non-compliance

Article 52 of the LGPD outlines a comprehensive range of administrative sanctions for data processing agents found in violation of its regulations, emphasizing the law's commitment to enforcing data protection principles. The potential sanctions include: (i) warning, with a deadline for adopting corrective measures; (ii) fines up to two percent (2%) of the turnover of the private legal entity, group, or conglomerate in Brazil for the last financial year, excluding taxes, with a cap of fifty million reais (R$50,000,000.00) per infraction; (iii) daily fines, subject to the total limit of fifty million reais (R$50,000,000.00); (iv) publicization of the infringement after its occurrence has been duly ascertained and confirmed; (v) blocking of the personal data to which the infringement relates until the activity is regularized; (vi)

deletion of the personal data to which the infringement relates; (vii) partial suspension of the operation of the database to which the infringement relates for a maximum period of six (6) months, extendable for the same period, until the controller regularizes the personal data processing activity; (viii) suspension of the personal data processing activity to which the infringement relates for a maximum period of six (6) months, extendable for an equal period; and (ix) partial or total prohibition of the exercise of activities related to personal data processing.

The LGPD ensures that the application of these sanctions considers a variety of factors, such as the severity and nature of the breaches; good faith of the breaching party; economic condition of the breaching party; extent of the damage; and cooperation of the breaching party with the authorities.

Conclusion

Brazil has taken significant steps in data protection regulation with the enforcement of the LGPD in recent years. This landmark legislation serves as a cornerstone for protecting personal data, ensuring compliance with key principles, and aligning Brazil with international privacy and data protection standards. The ANPD plays a crucial role in this landscape, actively enforcing the LGPD's requirements for data controllers and processors.

This collaborative effort between the legislative framework and the ANPD marks a major advance in Brazil's approach to data protection. This positions the country as a player in the global dialogue on data protection standards.

Contact Us

+55 (11) 3799-8100
https://klalaw.com.br/en/home/
accesar@klalaw.com.br
Av. Brigadeiro Faria Lima, 1355
São Paulo, SP 01452-919 Brazil