AUGUST/2020

GENERAL LAW OF DATA PROTECTION

in 16 infographics

#LGPD2YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

INTRODUCTION

The General Law of Personal Data Protection (LGPD) is a milestone for the Brazilian law. Published on August 15, 2018, the legislation entered into force only on September 18, 2020, given a series of postponements - the last due to the new coronavirus pandemic. For this reason also, the administrative sanctions provided for by LGPD will only be applied from August 2021 on.

With LGPD, the protection of personal data in Brazil now counts on specific legislation, which provides legal safety for data holders and processing agents, whether from the private sector or from the government.

And, of course, legal safety is essential to have a favorable environment for economic development, since the country adopts the best international practices regarding data protection. It is worth mentioning that the fundamental right to privacy, set forth in article five, item X, of the Federal Constitution, is strengthened with LGPD.

The publication of LGPD in the Federal Official Gazette occurred in the same year in which the General Data Protection Regulation (GDPR) came into force, the European data protection regulation, deemed a worldwide reference. But that is not the only characteristic shared by these legislations. Much more than that, as LGPD was in fact inspired by GDPR, with grounds, principles, and provisions in common.

In a digital economy like today's, with the massive use of data by companies and the government, the holders' rights shall be protected, with clear rules that enable economic development without any damage to citizens' privacy.

For LGPD to exercise its role, the National Data Protection Authority (ANPD) must be fully operational. At the end of August of this year, Decree 10.474/2020 structured ANPD, an organ linked to the Presidency of the Republic with the functions of regulation, inspection and sanction.

ANPD's work shall prioritize constructive engagement with the private sector through dialogue, support, mutual cooperation, guidance, awareness and information. The administrative sanctions provided for in LGPD, which can only be applied as of August next year, shall be the last option - only in cases of willful violation or exponentially negligent practices, repeated or very serious conducts.

It is important to note, however, that although the administrative sanctions provided for in LGPD have been postponed, companies hereby have the duty to notify in the event of an incident involving personal data. This is because sectorial bodies and the Judiciary Branch itself will be able to substantiate their acts based on LGPD to apply administrative measures and judgment against for civil liability.

In this e-book for free download, part of the campaign #LGPD2YEARS, we gathered 16 info graphics that highlight the main points of this legislation. Our purpose is to draw attention to the importance of data protection and privacy in Brazil, encouraging companies and the government to fully comply with the law.

For more information, our teams of Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados remain at your disposal.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

TABLE OF CONTENTS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

LGPD APPLICATION

LGPD covers all activities that involve processing in an analogical or digital means of personal data, being applied to individuals and corporate entities, of public or private law.

The exception is due to the data processing carried out by individuals for strictly domestic purposes (for example, telephone book, sending e-mails, among others).

As to the territorial scope, LGPD applies whenever data processing is carried out in Brazilian territory or if the activity involves the offer of products or services of people who are in national territory.

The law also provides for some situations in which LGPD does not apply.

LGPD APPLICATION

LGPD applies to processing of personal data carried out in digital or analogical means

TO WHOM DOES LGPD APPLY?

Legal person
of public or private law which carries out personal data processing

Natural person
except for the one who processes date for private and not economic purposes (telephone book, sending e-mails among others)

TERRITORIAL APPLICATION

- processing operation carried out in national territory
- Processing activity which offers assets or services to individuals located in the national territory
- personal data of the processing collected in national territory

APPLICATION EXCEPTIONS

- exclusively for journalistic, artistic or academic purposes
- processing aimed at public security, national defense, State security or activities of criminal prevention and repression

LGPD does not apply to personal data coming from outside the national territory and that are not the purpose of communication, shared use of data with Brazilian processing agents or the object of international data transfer with a country other than the country of origin, provided that this provides a degree of protection of personal data appropriate to LGPD.

LGPD 2 YEARS

KINDS OF DATA

Article 5 of LGPD provides concepts for understanding the legislation, such as personal data, sensitive personal data anonymous; and data rendered pseudonymous (the latter available in Article 13, § 4).

Knowing the differences between these concepts is essential for the controller to understand whether LGPD is applicable in order to subsequently assess the respective legal basis.

To learn more on sensitive data, check out the articles "Sexual orientation as sensitive data" and "Gender identity as sensitive data", by lawyers Bernardo Fico, Guilherme Sicuto and Henrique Meng Nóbrega, from our Data Protection area.

To go deeper into data rendered anonymous, read the article "The effectiveness of personal data rendered anonymous", by Ricardo Maffeis (our senior litigation consultant) and Daniel Bittencourt Guariento.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

KINDS OF DATA

PERSONAL

Any information that identifies an individual or that can lead to his identification. There are two types of personal data:

Direct: CPF, voter registration, RG, name, among others.

Indirect: Consumption habits, profession, gender, age, among others.

SENSITIVE PERSONAL

Racial or ethnic origin, health, sex life, genetics, biometrics, religion, political opinion, skin color, among others. It is worth remembering that the inferred personal data also receives the same PROCESSING as the sensitive personal data (Art. 11, § 1°)

RENDERED ANONYMOUS

Datum related to a holder that cannot be identified, considering the use of reasonable and technical means available at the time of its processing.

RENDERED PSEUDONYMOUS

Personal datum that, through processing, loses the possibility of being associated directly or indirectly with an individual, unless the controller uses additional information that was kept separately in a safe environment. **Examples:** encrypted data and hashing use as authentication.

- This datum rendered pseudonymous is also a personal data.
- Art. 18 guarantees the data holder the right to obtain from the controller the unnecessary or excessive data that are rendered anonymous.
- Once rendered anonymous, art. 12 sets forth that such data are no longer considered personal data.
- Personal data made public remain protected by law.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

PROCESSING AGENTS

The definition of who is in the position of controller or operator, according to the respective personal data processing activity, is important to determine the obligations and responsibilities of each of these processing agents.

This evaluation and definition can be simple or extremely complex tasks, due to the dynamics of the processing operations that usually involve their agents.

For more information on the issue, check out the article "Third party management in LGPD era" from the e-book "Best Practices for Governance and Compliance with LGPD", authored by our Data Protection team.

PROCESSING AGENTS

CONTROLLER

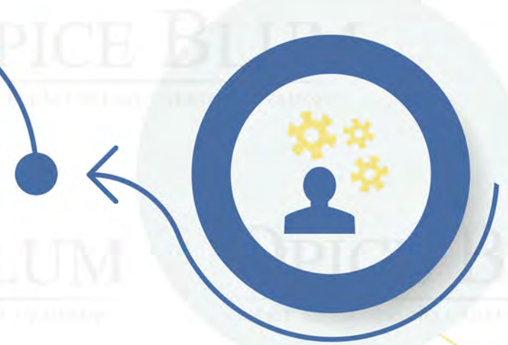
Individual or corporate entity of public or private law, that:

- Takes all decisions regarding the processing of personal data throughout their life cycle
- The agent determines the purposes and means of processing personal data
- The agent assesses the legal framework of treatment
- Can be held directly responsible for LGPD violations
- It assesses the classification of the legal grounds for processing

OPERATOR

Individual or corporate entity of public or private law, that:

- Carries out the processing of personal data on behalf of the controller
- He has no decision-making power
- He can also perform complex tasks and with some discretion, but always under the command of the controller
- The operator can be held jointly liable for violations that he/it may cause to LGPD



LGPD 2 YEARS

• The operator will always obey the controller, who is the one who effectively determines the purpose of the data processing. But if the operator uses these same data for another purpose, he also becomes a controller, with the responsibilities inherent to the position.
• Joint controller: data control is possible. What defines whether this is possible is the analysis of processing activity.

INFORMATIVE SELF DETERMINATION

Informative self determination is one of the grounds of LGPD, from which various principles, rights and obligations set forth in the legislation.

"The essential point for companies that process personal data in their activity is the understanding that such data belong to their holders, to whom they owe satisfaction, in the form of accountability. It is the so called informative self determination, which LGPD brought as one of its grounds, inspired by the well-known precedent of the German census of 1983, which defined it as the power conferred to the individual to decide whether and to what extent aspects of his personal life will be exposed", state our partner Renato Opice Blum and our associate Ana Maria Roncaglia, in the article LGPD: Retrospective of 2019 and perspective for 2020.

To know more about informative self determination, check out the article "A new historical landmark of Protection of Personal Data in Brazil – Trial of MP 954/20 in the STF".

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

INFORMATIVE SELF DETERMINATION

It is the holders' right to control the processing of his personal data

It is one of LGPD basis

It is reached by the compliance with the principles rights - specially the confirmation of the processing, the free access to the data, the consent revocation, the portability and the opposition to processing

At LGPD it is supported mainly by compliance with the principle of the purpose, necessity and transparence of the processing of personal data

To understand the informative self determination is to understand LGPD essence. The organizations that understand and apply this ground shall be able to face the journey in an easier way.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

The principles bring the essence of privacy and data protection.

According to the principles set forth at LGPD, as transparence, purpose, necessity and safety, the companies will be in the way to legal compliance.

The set of principles confers coesion to the law transmitting purposes to the provisions which deal with duties, responsibilities, rights and penalties.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

Article 6 of LGPD brings together the principles that shall be complied with throughout the life cycle of personal data. They also serve as guidelines for practices involving the processing of personal data.

Liability and accountability:
demonstration of adoption of effective measures to comply with the rules

Non discrimination:
not to use personal data for discriminatory, illegal or abusive purposes

Transparency:
clear and accurate information to holders

Safety:
use of technical and administrative measures to protect personal data from loss, destruction, modification, transmission or not permitted access

Prevention:
adoption of measures to prevent damage to holders

\+

Good faith: loyalty and correctness in data processing

Quality of the data:
accurate data, clear and in accordance with reality

Purpose:
lawful, specific, explicit and informed purposes. The holder shall be aware of them before any processing

Adequacy:
processing only of data compatible with the purposes informed to the holder

Necessity:
use of only strictly necessary data

Free access:
easy access to treatment and integrality of the data

LGPD purpose is neither to harm nor hinder the data processing. The ideia is to protect the holders' rights and guide the processing agents.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

PRIVACY BY DESIGN

"Privacy by Design" was adopted by LGPD as a way to guarantee that privacy and data protection are present in the entire life cycle of products and services, since their conception.

The concept was developed by Canadian Ann Cavoukian, who has served as Data Protection Commission Agent in Canada.

To deepen in the issue, read the article "Privacy by design: Innovation with safety" of the e-book "Best Practices of Governance and Compliance with LGPD", produced by Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

PRIVACY BY DESIGN

- It is the care for privacy and protection of personal data from the conception of the product or service

- At the time of the development of products or services that use personal data, the controller shall use adequate technical, security and administrative means to guarantee legality during the entire life cycle of the data

- It is grounded on the following principles, idealized by Ann Cavoukian:

- Proactivity
- Privacy as Standard (Privacy by Default)
- Privacy incorporated into the design of the product or service
- Total functionality of the product or service
- Visibility and transparency
- Respect for the user's privacy, which shall be at the center of attention

In adapting to the LGPD, it is essential that the processing agents define processes to apply Privacy by Design (article 46, §2) or make adjustments to their innovation activities and improvement of products and services in a way compatible with the governance rules internally instituted.

LGPD 2 YEARS

LEGAL GROUNDS

LGPD provides in Article 7 the legal hypotheses for the processing of personal data. LGPD provides in Article 11 the legal hypotheses for the processing of sensitive personal data.

It is important to note that several hypotheses of treatment - also known as legal grounds - are common to both personal data and sensitive personal data. Some legal grounds, however, do not apply to the processing of sensitive data.

The law only allows the processing of personal data minus a legal basis. If it is not possible to fit the activity in one of them, the organization shall reconsider the processing activity at issue.

To demystify some beliefs around legal grounds, check out article "5 myths created on the General Law of Data Protection", co-authored by our partner Caio Lima and the coordinators of our Data Protection area, Henrique Fabretti and Tiago Furtado.

LEGAL GROUNDS

Uncontroversial hypotheses of data processing provided for by law

PERSONAL DATA

- Consent
- Compliance with legal or regulatory obligation
- Execution of public politics by Public Administration
- Undertaking of studies by research organs
- Due exercise of rights, including in contract and in legal, administrative and arbitral processes
- Protection of the holder or third parties' life or physic unharmed condition
- Health guardianship
- The controller or third parties' lawful interest
- Credit protection
- For execution of contracts and preliminary procedures related to them

SENSITIVE PERSONAL DATA

- Consent
- Compliance with legal or regulatory obligation
- Execution of public politics by Public Administration
- Undertaking of studies by research organs
- Due exercise of rights, including in contract and in legal, administrative and arbitral processes
- Protection of the holder or third parties' life or physic unharmed condition
- Health guardianship
- Guarantee of fraud and the holder's safety prevention

LGPD 2 YEARS

Treatment shall fit on at least one legal ground. There is no hyerarchy between the common legal grounds. But for sensitive personal data, the law priorizes consent.

CONSENT

Consent is one of the legal hypotheses for the processing of personal data. The holder shall be free to accept or refuse consent, as well as to receive the information in the appropriate language and form to understand what will be done with his data.

For the consent to be valid there can be no doubt that the holder has consented without defects.

Therefore, consent shall presuppose affirmative action.

To get deeper into the issue, get to know the #EntendoLogoConcordo, movement in favor of transparency and accessibility in the privacy notices and terms of use.

LGPD 2 YEARS

CONSENT

It is one of the legal hypotheses for processing personal data, with no hierarchy in relation to the others, except for sensitive data. Furthermore, it is also one of the hypotheses for international data transfer

The consent for international transfer of personal data and processing of sensitive personal data and children's data shall be highlighted and specific for the purpose

Its manifestation shall be free, informed, unambiguous and specific to each purpose. For this, the holder shall receive the information in an accessible and transparent form to solve all doubts before giving his consent, in a proactive and affirmative way. The holder shall also be free to refuse and/or revoke it

It indicates that the holder agrees with the processing of his personal data for a certain purpose. Generic authorizations will be void

In accordance with the law the controller is liable for the burden of proof that consent was obtained

LGPD 2 YEARS

There is no need to renew consent in the case of changes in purpose for the processing that are not compatible with the original consent. But it is necessary to inform the holder.

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

LEGITIMATE INTEREST

LGPD innovated by bringing legitimate interest to the Brazilian legal system as a legal basis for the processing of personal data.

Unlike what happens with consent, there is no legal provision for revoking the legitimate interest by the holder. However, the controller assumes greater responsibility when using it, and he shall first analyze the applicability of this hypothesis through the Legitimate Interests Assessment (LIA).

To ensure that there is no abuse in the use of this legal basis, ANPD may request the controller to report the impact on the protection of personal data when the processing is based on legitimate interest.

LEGITIMATE INTEREST

It is one of the legal possibilities for processing personal data by the controller and third parties

The use of legitimate interest as a legal hypothesis of processing cannot override the fundamental rights of data holders

It cannot be used in sensitive data processing

LGPD cites exemplary and non-taxing hypotheses for the use of legitimate interest, such as in supporting and promoting the activities of the controller and in protecting, in relation to the holder, the due exercise of his rights or provision of services that benefit him

The national authority may request the controller for an impact report on the protection of personal data, when the processing is based on its legitimate interest

Although there is no express legal provision in LGPD, the Legitimate Interests Assessment (LIA) is a good practice to assess the application of legitimate interest, always analyzing the concrete case

LGPD 2 YEARS

Although the legitimate interest is one of the most flexible and already versatile, legal bases, the controller assumes greater responsibility when using it, and he must evaluate and respect the legitimate expectations of individuals.

DATA HOLDERS' RIGHTS

LGPD innovated by bringing together, in only one place, the data holders' rights. Before LGPD, there were sparse provisions in several laws, as the Consumer Protection Code and *Marco Civil da Internet*.

The holder can exercise these rights over his personal data at any time, upon request to the controller. It is worth mentioning that it is the controller's obligation to be properly prepared to receive and render such requests effective.

Find out more in the article "How to fulfill the holders' rights" of the e-book "Best Practices of Governance and Compliance with LGPD", produced by Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

DATA HOLDERS' RIGHTS

- Confirmation of processing existence and access to data
- Correction of incomplete, inaccurate or outdated data
- Anonymizing, blocking or deleting unnecessary, excessive or illegally processed data
- Data portability to another controller/ supplier of products or services
- Elimination of personal data processed wit the holder's consent
- Information on the entities with which the controller shared data
- Information on the possibility of not providing consent
- Revogation of the consent
- Review of decisions made exclusively on the basis of automated processing of personal data
- Complaint to the national authority
- Opposition to irregular processing

LGPD 2 YEARS

Confirmation of the existence or access to personal data shall be provided immediately in a simplified format or within 15 days by means of a clear and complete declaration, in compliance with the commercial and industrial secrets. There is no term expressly defined in LGPD for compliance with the other holders' rights.

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

GOVERNANCE IN DATA PROTECTION

The development, implementation and perennial maintenance of the Privacy Governance and Protection of Personal Data structure corresponds to one of the main points of any LGPD compliance journey.

It is also important to remember that the National Data Protection Authority will take into account the adoption of good practice and governance policies as a parameter to mitigate the penalty in occasional administrative procedures.

To create and manage an efficient Privacy program that brings an adequate level of compliance with LGPD, read the article "Five elements required to create a Privacy and Data Protection program" in the ebook "Best Governance Practices and Compliance with LGPD", produced by Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.

Also check out the article "Governance as the epicenter of the compliance journey in Personal Data Protection - LGPD and GDPR", by our partner Rony Vainzof.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

GOVERNANCE IN DATA PROTECTION

LGPD encourages controllers and operators to adopt internal compliance rules.

Demonstrate commitment to adopting internal processes and policies that ensure compliance with rules and good practices

Be applicable to the entire set of personal data under controllers and operators' control

Be adapted to the structure, scale and volume of its operations, as well as the sensitivity of the data processed

Establish appropriate policies and safeguards based on a systematic assessment of impacts and privacy risks

Establish a relationship of trust with the holder through transparent action that ensures participation mechanisms

Be integrated with its general governance structure and establish and apply internal and external supervisory mechanisms

Have incident response and remediation plans

Be constantly updated based on information obtained from continuous monitoring and periodic evaluations

Demonstrate the effectiveness of your program

LGPD 2 YEARS

The governance rules must be published and updated periodically and may be recognized and disclosed by the National Data Protection Authority.

DATA PROTECTION OFFICER OR PERSON IN CHARGE

The Data Protection Officer (DPO) is called Person in Charge by LGPD.

Two of the most important measures of governance of organizations are evaluating and defining the appointment, the position and powers of the DPO, with autonomy and resources to perform the duty effectively.

It is recommended that he responds to the highest hierarchical level of the organization, being a key player in due compliance with the applicable laws and in mitigating risks.

To learn more about the issue, check out the article "Outsourcing of the Person in Charge – Far beyond DPO as a service", by our partner Rony Vainzof.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

DATA PROTECTION OFFICER OR PERSON IN CHARGE

One of the most important governance measures for organizations are to assess and define the DPO's appointment, position and duties, with autonomy and resources to perform the function effectively. It is recommended that he responds to the highest hierarchical level of the organization, being a key player in due compliance with the applicable laws and in risk mitigation.

Although LGPD does not describe the profile of the DPO, it is suggested:

- Legal and regulatory knowledge
- Risk management and audit and compliance
- Leadership and proactivity
- Awareness provider/educator
- Public/government relationships
- Knowledge in Technology and Information Security

Functions provided for at LGPD and recommended

- Monitor compliance of the processing agent regarding LGPD, other data protection rules and their own internal policies related to the issue
- Accept holders' complaints and communications , provide clarifications and take action
- Receive communications from the national authority and take action
- Perform the other duties determined by the controller or set forth in complementary rules
- Train and raise awareness among employees and third parties of processing agents to create a data protection culture

• The law does not require the Person in Charge to be employed by the controller/operator, and it is possible to outsource this function (DPO as a Service).
• If the DPO performs other duties in the organization, it is recommended that there be no conflict of interest between the DPO's function and such duties.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

REPORT ON DATA PROTECTION IMPACT

The Personal Data Protection Impact Report (RIPD) is provided for in article. 5, XVII, of the General Personal Data Protection Law (LGPD).

In practice, this is the documentation in which the controller describes the processes for personal data processing that may generate risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms.

By conducting a RIPD, the controller will be more confident as to the compliance with the different foundations of the Law concerning privacy; informative self determination; freedom of expression, information, communication and opinion; the inviolability of intimacy, honor and image; consumer protection; and human rights, the free development of personality, dignity and the exercise of citizenship by individuals.

To learn more on the issue, read the chapter "Impact Report on the Protection of Personal Data", authored by our partner Rony Vainzof, in the work *Data Protection - Challenges and Solutions to Adequate to the Law*, organized by our founding partner and chairman, Renato Opice Blum.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

REPORT OF IMPACT TO DATA PROTECTION

- Document to be prepared by the controller describing the processing of personal data that could jeopardize the fundamental rights
- This document must contain at least the description of:
- Allows the assessment of the treatment activity risk before it is actually carried out, in order to mitigate risks
- ANPD may request the impact report for processing data that involve legitimate interest, as well as determining that it is done for processing that involves sensitive data

- Kinds of data collected
- Methodology used for data collection and information security
- Controller's analysis on measures that can be implemented to minimize risks

LGPD 2 YEARS

The Report on Data Protection Impact is a way of assessing the existence of risks to fundamental rights and identify potential risks to the principles set forth in LGPD.

MAIN HYPOTHESES OF INTERNATIONAL TRANSFER OF PERSONAL DATA

LGPD will specifically provide on the international transfer of personal data to countries or international organizations. This will be possible in the cases provided for in Article 33, including, among other eight cases, countries that enjoy a certain level of data protection.

To evaluate whether the country of destination has the appropriate degree of data protection, the National Data Protection Authority (ANPD) will take into account some factors such as:

- The general and sectoral rules of the legislation in force in the destination country;
- The nature of the data;
- Compliance with personal data protection principles and holders' rights provided for in LGPD.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

MAIN HYPOTHESES OF INTERNATIONAL TRANSFER OF PERSONAL DATA:

- Country of destination with a degree of protection appropriate to the LGPD. This evaluation will be ANPD responsibility
- Upon specific and prominent consent of the holder
- Upon international cooperation agreement
- To protect the holder or third party's life or physical safety
- Regarding international legal cooperation for the purposes of research and for the execution of public policy
- Upon guarantees offered by the controller:
  - specific contractual clauses
  - global corporate rules
  - contractual standard rules
  - stamps, certificates and codes of conduct
- When authorized by the National Data Protection Authority

The hypotheses set forth for international data transfer are mandatory and shall be complied with by the controllers.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

NATIONAL DATA PROTECTION AUTHORITY - ANPD

On July 8, 2019, President Jair Bolsonaro signed Law No. 13.853/2019 (Law of Conversion of Provisional Measure No. 869/2018), which created ANPD as a federal public administration body, part of the Presidency of the Republic, ratifying the proposal for a regulatory authority presented in the Provisional Measure.

Only on August 27, 2020, Decree No. 10,474, which structures ANPD, was published in the Federal Official Gazette. In Annex I, the Regulatory and Organizational Structure of this regulatory, inspection and sanction body, including nature, purpose and competencies.

ANPD shall have the authority to ensure personal data protection Privacy; promote knowledge of the rules and public policies on data protection and security measures; apply administrative penalties; among others.

For this reason, it is essential that ANPD be installed, since the law without this Authority may hinder the achievement of the desired legal security.

To deepen your reflection, be sure to read the articles "Data protection in Brazil 4.0", by our partner and chairman, Renato Opice Blum, co-authored with the lawyer Shirly Wajsbrot; and "ANPD and the Executive's omission", by Sandra Rogenfisch.

NATIONAL DATA PROTECTION AUTHORITY - ANPD

It is the regulatory, supervisory and sanctioning body, whose main duties are:

- Protect personal data
- Develop guidelines for the National Policy on Protection of Personal Data and Privacy
- Stimulate knowledge on personal data protection in the population
- Cooperate with other data protection authorities
- Implement simplified mechanisms for registering complaints on processing that does not comply with the law
- Consider petitions from holder against controller after proof of non-resolution within the regulated period
- Enact regulations and procedures on personal data protection, privacy and reports on the impact on personal data protection

- Deliberate on the interpretation of LGPD and its competences in cases of omissions
- Conduct audits or determine their performance for inspection activities
- To supervise and apply penalties upon administrative proceedings
- Enact simplified rules, guidelines and procedures for micro and small companies, disruptive companies, startups or innovation companies
- Encourage the adoption of standards for services and products that facilitate holders' control over their data
- Articulate with public regulatory authorities on their competencies in sectors of regulated economic activities
- Enact simplified and differentiated guidelines and procedures so that microenterprises, small and/or disruptive companies and startups can adapt to the law

It is important that the future ANPD prioritizes constructive engagement with the private sector, giving priority to dialogue, support, mutual cooperation, guidance, awareness and information. Penalties shall be the last option, to be applied when there is a willful violation or exponentially negligent practices, repeated or very serious conducts.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

ADMINISTRATIVE SANCTIONS PROVIDED FOR IN LGPD

Bill No. 1,179/2020, later converted into Law No. 14,010/2020, postponed the entry into force of articles related to LGPD administrative sanctions until August 1, 2021.

It is important that there is an adaptation period, in which ANPD (National Authority for the Protection of Data) is more focused on guiding and disseminating good practices than punishment.

To go deeper into the issue, check out the article "The extension of LGPD sanctions and the relevance of ANPD", authored by our partner Rony Vainzof.

LGPD 2 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

ADMINISTRATIVE SANCTIONS PROVIDED FOR IN LGPD

Applicable from August 1, 2021 (Law No. 14,010/2020):

- Warning
- Simple fine (up to 2% of the revenue up to the limit of R$ 50 million)
- Daily fine
- Possibility of publication of the infraction
- Blocking of the personal data involved
- Elimination of the personal data involved
- Partial suspension, for up to 6 months, of the database involved
- Partial or total prohibition on the exercise of activities related to data processing

ANPD will take into account:

- Severity and nature of the violation
- Offender's good faith and cooperation
- Advantage obtained with the infraction
- Offender's economic conditions
- Recurrence and severity of the damage caused
- Adoption of internal mechanisms and procedures of data protection
- Adoption of good practice and governance policy
- Prompt adoption of corrective measures
- Proportion between the gravity of the infringement and the intensity of the sanction

• ANPD will define the methodologies that will guide the calculation of the base value of fine sanctions through its own regulation on sanctions for breaches of the LGPD. This will further be subject to public consultation.
• Before any sanction is applied, there will be due publication so that the processing agents are aware of the methodology to be applied.

LGPD 2 YEARS

CREDITS

PARTNERS

José Roberto Opice Blum
Renato Opice Blum
Marcos Bruno
Juliana Abrusio
Rony Vainzof
Caio Lima
Camilla Jimene
Danielle Serafino

EDITORIAL COORDINATION

Lara Silbiger

LEGAL CONTENT

Ana Maria Roncaglia
Bruno Toranzo

REVIEW

Rony Vainzof
Caio Lima
Danielle Serafino
Henrique Fabretti
Tiago Neves Furtado

ART AND DESIGN

Paola Cosentino

INTERN

Lucas Fernandes

LGPD 2 YEARS

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF