Updated version on

SEPTEMBER/2021

with the inclusion of new infographics

GENERAL DATA PROTECTION LAW

in 22 infographics

#LGPD3YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

INTRODUCTION

LGPD (General Data Protection Law), in force since September 18th, 2020, sets forth guidelines for the processing of personal data. Inspired by GDPR (General Data Protection Regulation) of the European Union, the Brazilian law was a milestone for data protection in the country.

Since August 1st, 2021, companies that are not compliant with the LGPD may suffer administrative sanctions, under the exclusive competence of ANPD (Data Protection Supervisory Authority), according to Article 52 of the Law, that may vary from a warning to a fine of up to 2% of the company's annual revenue, limited to R$ 50 million per infraction.

This booklet, which is part of the #LGPD3YEARS (#LGPD3ANOS) campaign, is an update of the material published in 2020 and now has 22 infographics that highlight the main points of data protection law. The goal is to draw attention to the importance of data protection and privacy in Brazil, encouraging companies and the government to comply with the LGPD.

Others topics are covered in this booklet, with emphasis on the application of LGPD; types of data; Incident Response Plan; transparency and Visual Law techniques; informative self-determination; general principles of data protection; Privacy by Design and Privacy by Default; legal grounds, such as consent and legitimate interest; rights of the data subjects; data protection governance; data processing agents - controller, joint controller, processor, sub-processor; DPO; Data Protection Impact Assessment; international transfer of data; Data Protection Supervisory Authority (ANPD); and administrative sanctions provided for by LGPD.

Have a good reading! For additional information contact our team.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

INDEX

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

LGPD APPLICATION

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

The exception is the data processing carried out by natural person for strictly domestic purposes (for example, telephone book, sending emails, and others).

As to the territorial scope, LGPD applies in the cases that 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 brings some situations in which the LGPD does not apply, as the infographic shows on the next page.

LGPD APPLICATION

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

TO WHOM LGPD APPLIES?

Legal entity
by public or private law, that carries out personal data processing

Individual
Except for the one who processes data for private and non-economic purposes

TERRITORIAL APPLICATION

Processing operation carried out in national territory

Processing activity which offers goods or services to individuals located in the national territory

Processing personal data collected in the national territory

APPLICATION EXCEPTIONS

exclusively for journalistic, artistic or academic purposes

processing that aims public safety, national defense State security or criminal prevention and repression activities

LGPD does not apply to personal data coming from outside the national territory and that are not the object of communication, shared use of data with Brazilian processing agents or the object of international data transfer with a country other than the source country, if this last one provides a level of personal data protection adequate to the LGPD.

LGPD 3 YEARS

TYPES OF DATA

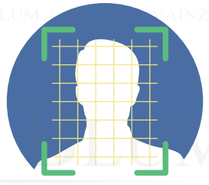
Article 5 of LGPD provides the concepts for understanding the law, such as personal data; sensitive personal data; anonymized data; and pseudonymized data (available in Article 13, Paragraph 4).

Knowing the differences between these concepts is essential for the controller to understand if LGPD is applicable and then evaluates the appropriate legal ground.

If you want to know more about sensitive data, check out the articles "Sexual orientation as sensitive data" and "Gender identity as sensitive data" written by our Data Protection lawyers.

In order to investigate the knowledge about the anonymized data, read the article "The effectiveness of anonymization of personal data", written by the lawyers Ricardo Maffeis and Daniel Guariento.

TYPES OF DATA



PERSONAL

It means any information that identifies or can identify an individual. There are two types of personal data:

Direct: Social Security Number, voter registration, ID (Identification), name, National Insurance Number, and others

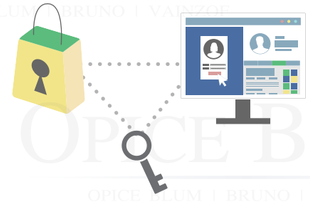
Indirect: consumption habits, occupation, gender, age, and others

SENSITIVE DATA

Racial-ethnic origins, health, sex life, genetics, biometrics, religion, political opinion, skin color, among others. Remember that the personal data also have the same processing of personal sensitive data. (Art. 11, § 1º)

ANONYMIZED

Data subjects data that can't be identified, considering the use of reasonable and available technical means at the time of their processing.



PSEUDONYMIZED

Personal data that miss the possibility of being directly or indirectly associated with an individual, unless the controller adds additional information that keep in secret. Example: Encrypted data and hash as authentication.

- Pseudonymized data are also a personal data.
- Article 18 guarantees to the data subjects the right to obtain from the controller the anonymization of the unnecessary or excessive data.
- Once anonymized, Article 12 states that the data aren't personal data.
- Personal data made public continue to be protected by law.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

DATA PROCESSING AGENTS

The data processing agents, according to Data Protection Supervisory Authority (ANPD), shall be defined based on their institutional character. Knowing who is the controller and the processor is important to determine the obligations and the responsibilities of each of these data processing agents.

In addition to these two data processing agents, ANPD mentions the joint controllers and sub-processor, that are not formally established by LGPD. The definition, however, can be a simple or a complex task, due to the dynamic nature of the processing that usually involves their agents.

DATA PROCESSING AGENTS

CONTROLLER

Individual or legal entity, whether public or private, who:

- Makes all decisions about the personal data processing during its lifecycle
- Determines the purposes and the means of the personal data processing
- Assesses the environments of the processing legal grounds
- May be held responsible for breaking the LGPD
- It is up to the controller to guarantee compliance with the rights of the data subjects

PROCESSOR

Individual or legal entity, whether public or private, who:

- Processes personal data behalf of the controller
- Does not have decision power
- It can also perform complex tasks and with some discretion in accordance with the instructions supplied by the controller
- The processor shall be jointly liable for any damages caused by the processing

LGPD 3 YEARS

• The processor must always obey the controller, that is the one who can determine the purpose of the data processing.
• Joint controller: it happens when two or more controllers jointly determine the purposes and means of processing.

NEW INFOGRAPHIC

DATA PROCESSING AGENTS

JOINT CONTROLLER: Depending on the context, the same personal data processing can have two or more controllers. The Article 42, paragraph 1, II, LGPD, determines that "any controllers that are directly involved in the processing which resulted in damages to the data subject shall be jointly liable, except in the events of exclusion established in article 43 of this Law".

Even if LGPD does not mention the joint controller concept, it is included in the legal data protection system.

LGPD 3 YEARS

NEW INFOGRAPHIC

DATA PROCESSING AGENTS

SUB-PROCESSOR: The sub-processor is hired by the processor to be the assistant on the personal data processing and both perform behalf of the controller. The sub-processor answers to processor directly.

About the responsibilities, the sub-processor shall be jointly liable with the processor, according to Article 42, §1, I, LGPD.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

DATA PROCESSING AGENTS

JOINT CONTROLLER

- Two or more controllers jointly determine the purposes and means of processing;
- Two or more controllers have a mutual interest in the same personal data processing; and
- Two or more controllers make common or convergent decisions about the purposes and the essential elements of the processing.

SUB-PROCESSOR

- This person is hired by the processor to assist him in the personal data processing on behalf of the controller;
- The sub-processor answers to processor directly, not to controller; and
- The sub-processor may have similar responsibilities to that of processor.

LGPD 3 YEARS

INFORMATIVE SELF-DETERMINATION

Informative self-determination is one of the grounds of LGPD (Article 2), with privacy and intimacy, and it is the way to everyone can exercise the control over the own data, being able to decide, in some situations, what data can be processed.

Even in cases that the personal data subject can't oppose of the processing, it is given to him the right to be informed about the purpose of the data processing and about the security of the process.

INFORMATIVE SELF-DETERMINATION

It is one of the grounds of LGPD

It is the way of the data subjects can control the details about the data processing

According to the LGPD, the Informative self-determination is based by compliance with the principles of purpose, necessity and transparency of the personal data processing

It is achieved by compliance the rights of the data subjects – the confirmation of data processing, the free access to data, the revocation of consent, the portability and the opposition to data processing

To understand the Informative self-determination is to understand the essence of LGPD. Organizations that understand and apply this foundation will be able to face the adaptation journey more easily.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

GENERAL PRINCIPLES OF PERSONAL DATA PROCESSING

The principles bring the essence of the privacy and the data protection.

By following the principles established in LGPD, such as transparency, purpose, necessity and security, the organizations will be on the way to legal compliance.

These principles give cohesion to the Law, ensuring some duties, responsibilities, rights and sanctions.

GENERAL PRINCIPLES OF PERSONAL DATA PROCESSING

Article 6 of LGPD brings together the general principles that must be compliant by the processing agents in the entire lifecycle of the personal data. They also can be a guide for the practices that involve the personal data processing

Liability and accountability: demonstration of effective measures able to prove compliance with the personal data protection rules

Non-discrimination: non-use of personal data for discriminatory, unlawful or abusive purposes

Transparency: it means the guarantee of clear and accurate information for data subjects

Security: it is the use of technical measures that able to protect the personal data from loss, destruction, modifications, diffusion or not allowed accesses

Prevention: it is necessary to take measures to avoid damage to the data subjects

Good Faith: Be correct and loyal in personal data processing

Data quality: guarantee, to the data subjects, accurate, clear, relevant and updated data

Purpose: legitimate, specific, explicit and informed purposes that must be communicated to data subjects before any processing

Suitability: compatibility of the data processing with the purpose communicated to the data subject

Need: data are only used in strictly necessary case

Free access: guarantee, to the data subjects, facilitated and free consultation of the personal data processing

LGPD 3 YEARS

LGPD's goal is not to harm or hinder the data processing. The idea is to protect the data subjects and guide the data processing agents.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

PRIVACY BY DESIGN

"Privacy by Design" was set up by LGPD as the way to ensure that the data privacy and protection may be present in the entire lifecycle of products and services, since their conception.

The concept was created by Ann Cavoukian, who has served as Commissioner of Data Protection in Canada.

To know more about it, read the article "Privacy by design: innovation with security" from the e-book "Best Governance Practices and Compliance with LGPD", produced by our team at Opice Blum, Bruno and Vainzof Advogados Associados.

Also check out the article "Privacy by Design and Privacy by Default", which is part of our booklet about DPO.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

PRIVACY BY DESIGN

- It's the way to take care of data privacy and personal data protection since the design of the product or service

- In the development of products or services that use personal data, the controller must use security and administrative technical means to ensure the compliance with the law during the entire data lifecycle

- It is based on the principles created by Ann Cavoukian:
  - Proactivity
  - Privacy by Default
  - Privacy incorpored into the design of the product or service
  - Total functionality of the product or service
  - Privacy throughout the product or service functionality
  - Visibility and transparency
  - Respect of user privacy, that shall be at the centre of attention

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

LGPD 3 YEARS

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

VISUAL LAW

In LGPD, according to the purpose principle, the data processing must be performed with a legitimate, specific and explicit way and has to be informed to the data subjects. For this reason, to make easier the understanding, Visual Law techniques are already applied, making possible to present the content through graphical representations. The Visual Law's proposal is to make easier the understanding of the complex legal information.

With the application of Legal Design (design of legal products and services), documents, such as privacy policy, can be created with a visual structuring, in order to make easier the understanding of legal terms.

For more information, check out our illustrated article about how to elaborate privacy policy by the application of Visual Law techniques.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

VISUAL LAW TECHNIQUES

- Videos
- Hyperlink
- Illustrated timelines
- Infographics
- Flowchart
- Sketches
- Graphics
- Icons (pictograms)

LGPD 3 YEARS

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

HOW TO APPLY VISUAL LAW IN LGPD CONTEXT

- Information about the personal data processing must be highlighted, to make easier the user access;
- Should be used a concise and easy language;
- According to ISO 29.184, the recommendation is to use short and objective sentences that do not offer doubt about the purposes of the personal data processing;
- The retention period of personal data must be in accordance with the purposes of the collect;
- The data subject should know who is responsible for the personal data processing. For this reason, the name and contacts of the controller must be included. The information shoud be easily visible to the data subject through the Visual Law techniques; and
- Finally, it is necessary to include the identity and contact information of the DPO, according to the first paragraph of Article 41, LGPD.

[ ] **name** - insert company name

email - for direct contact

phone - for direct contact

mailing address

FULL NAME, TELEPHONE NUMBER AND/OR EMAIL

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

LEGAL GROUNDS

LGPD mentioned in Article 7 the legal grounds to the personal data processing. And in Article 11 are the legal grounds to sensitive personal data processing.

It is important to pay attention that several processing grounds - also known as legal grounds – are common to personal data and sensitive personal data. However, some of legal grounds are not applied to the sensitive data processing.

It is only allowed by the law the personal data processing if there is at least one legal ground, otherwise the organization must rethink the viability of the personal data processing.

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

LEGAL GROUNDS

Exhaustive data processing grounds mentioned in the LGPD

PERSONAL DATA

- Consent
- Compliance with legal or regulatory obligation
- Execution of public policies by the Public Administration
- Conducting studies by research bodies
- Regular exercise of rights, including in contract and in judicial, administrative and arbitration proceedings
- Protection of life or physical safety of the data subjects or third parties
- Health care
- Legitimate interest of the controller or third parties
- Credit protection
- For enforcement of contracts and related preliminaries procedures

SENSITIVE PERSONAL DATA

- Consent
- Compliance with legal or regulatory obligation
- Execution of public policies by the Public Administration
- Conducting studies by research bodies
- Regular exercise of rights, including in contract and in judicial, administrative and arbitration proceedings
- Life or physical safety protection of data subjects or third parties
- Health care
- Guarantee of fraud prevention and security of the data subject

LGPD 3 YEARS

The processing must be fit at least to one legal ground. There is no hierarchy between the legal grounds, but LGPD prioritizes the consent for the sensitive personal data.

CONSENT

The data subject must be free to accept or refuse the data processing and also has the right to receive the information in an adequate way to understand how the data processing happens.

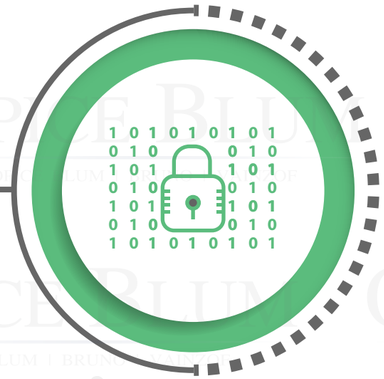
To validate the consent, it's necessary to have no doubt that the data subject consented, without defects.

Consent needs affirmative action.

To know more check out the tag #UnderstandThenAgree

CONSENT

It's one of the legal grounds of personal data processing. It is also one of the grounds of international transfer data.



The consent to international transfer of personal data, the sensitive personal data processing and the children's data should be collected according to the purpose of the processing.

The manifestation must be free, informed, unambiguous and specific for each purpose. For this reason, the data subject must receive the information in an accessible and transparent way, and then can settle all doubts before consent, in a proactive and affirmative way. The data subject must also have the right to refuse the data processing and/or to revoke the consent.

Indicates that the data subject agrees with the personal data processing according to a particular purpose. Generic authorizations are null.

The controller has the burden of proof the data subject consent.

There is no need to renew the consent if the processing purpose changes, but it is necessary to communicate the data subject.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

LEGITIMATE INTEREST

LGPD innovated by including the legitimate interest into the Brazilian legal system as a legal ground for the personal data processing.

Unlike the consent, there is no legal provision for the revocation of the legitimate interest by the data subject. However, the controller takes more responsibility when using it and should analyze the applicability of this ground by means of the Legitimate Interests Assessment (LIA).

To guarantee that the legal ground will not break the law, ANPD may request the Data Protection Impact Assessment for controller in the case of the data processing based on the legitimate interest.

LEGITIMATE INTEREST

It is one of the legal grounds of the personal data processing made by the controller and third parties

The use of legitimate interest as legal ground of data processing must not take priority over the fundamental rights of data subjects

It can't be used in the sensitive data processing

Some exhaustive possibilities are mentioned by LGPD about the legitimate interest application, such as in case of supporting the controller activities and for the data subject protection related to the regular exercise of his rights or for providing services that benefit him

ANPD may request from the controller the Data Protection Impact Assessment in the cases of the processing based on the legitimate interest

Although there is no mention in LGPD about the Legitimate Interests Assessment (LIA), it is a good way to guarantee the legitimate interest application, taking always into consideration the specific case

LGPD 3 YEARS

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

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

RIGHTS OF THE DATA SUBJECTS

LGPD innovated by bringing together at Article 17 the rights of data subjects, that were provided for sparsely in several laws, such as the Consumer Protection Code and the Brazil's Internet Bill of Rights. According to the General Data Protection Law, the data subjects may have these rights at any time through request to controller.

The law also mentions that the data subjects have the right to communicate against the data processing agents to the Data Protection Supervisory Authority (ANPD), that is responsible for the supervision and control over them (Article 18, Paragraph 1).

LGPD provides that the data subjects are entitled to request a review of decisions made by means of on the automated personal data processing that affects their interests (Art. 20). Finally, the exercise of these rights can be done individually by the data subject or by collective guardianship.

RIGHTS OF THE DATA SUBJECTS

- Confirmation of the existence of the processing and access to the data
- Correction of incomplete, inaccurate or outdated data
- Anonymization, blocking or deletion of unnecessary, excessive, or unlawfully processed data
- Data portability to another controller/supplier of products or services
- Elimination of the personal data processed with the consent of the data subjects
- Information of the possibility about not providing consent
- Can object to irregular data processing
- Information of the public and private entities with which the controller shared the data
- Revocation of consent
- Review the decisions taken exclusively by means of personal data automated processing
- Claim to the Data Protection Supervisory Authority (ANPD)

LGPD 3 YEARS

The confirmation of the existence or the access to personal data must be started immediately or within 15 days by means of a clear and complete statement, observing business and industrial secrets. There is no time limit mentioned by LGPD of complying with the others rights of data subjects.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

AUTOMATED DECISIONS AND ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is a research area with the goal to develop automated solutions by artificial systems or agents for solving problems that require human intervention.

The term "Artificial Intelligence" involves several methodologies, such as:

- Classical programming procedures (expert systems); and
- Machine learning (machine learning and its variants, such as deep learning and neural networks).

This kind of technology has been increasingly used to analyze big volumes of data and extract patterns, and create predictions about the people.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

AUTOMATED DECISIONS AND ARTIFICIAL INTELLIGENCE

Due to the complexity of how the Artificial Intelligence systems work, including the way how the algorithms operate, it is essential to guarantee to the data subjects the possibility of understanding how a decision that affects his interests was taken. There is a need for this so that the data subject can, if he wishes, challenge the decision of the AI.

Article 20 of the LGPD determines that the data subject has the right to request the review of decisions taken by automated processing, as well as sets out that the controller has the obligation to provide clear and understandable information about the company's procedures.

The data subject has:

The right to ask the controller any information about the processing and how works an automated decision.

The right to ask the controller to review decisions that affect his interests and have been taken solely based on the automated processing of his personal data.

LGPD 3 YEARS

If you want to know more, check out our report **"AI Regulatory Framework and the need for maturity of the debates"**.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

DATA PROTECTION GOVERNANCE

Developing, implementing and maintaining the governance framework for privacy and protection of personal data are the cornerstones of any LGPD compliance journey.

It is also important to remember that the Data Protection Supervisory Authority (ANPD) will take into account the adoption of good practices and governance policies as a parameter to mitigate the sanction of any administrative procedures.

To create and manage an effective Privacy program that brings an adequate level of compliance with LGPD, read the article "Five Elements Necessary for Creating a Privacy and Data Protection Program" from the e-book "Best Governance Practices and Compliance with LGPD", produced by Opice Blum, Bruno and Vainzof Advogados Associados.

Also check out the article "Governance as the epicentre of the Personal Data Protection Compliance Journey - LGPD and GDPR", by our partner Rony Vainzof.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

DATA PROTECTION GOVERNANCE

LGPD encourages controllers and processors to adopt internal compliance rules gathered in a privacy and data protection program

To demonstrate the commitment to adopt internal processes and policies to ensure the compliance with rules and good practices

To be applicable to the whole set of personal data under controller and processor's control

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

To set forth policies and adequate safeguards based on the systematic of impacts and privacy risks evaluation

To establish trust relationship with the data subject through transparent performance that ensures mechanisms for his participation

The program shall be integrated into the general structure of governance and shall establish and apply mechanisms of internal and external supervision

To be constantly updated based on information obtained through the continuous monitoring and periodic evaluations

To have incident response and remediation plans

To demonstrate the effectiveness of the program

LGPD 3 YEARS

The governance rules must be published and updated periodically and may be recognized and disclosed by the Data Protection Supervisory Authority (ANPD).

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

CONTRACTS MANAGEMENT

When mapping contracts that already exist or that will still be entered into by the company, it is necessary to verify in the contracts object whether there is personal data processing by the parties during its performance, which consists of any operation that uses personal data, and it is necessary to adapt this document to the General Data Protection Law (LGPD). With the mapping, it is also possible to identify, for example, if there is processing of sensitive data or of children and adolescents, which requires a little more attention.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

CONTRACTS MANAGEMENT

It is very important that personal data processing agents compliant with the rules in order to have all the contracts in compliance with LGPD:

- It is necessary to observe and understand mainly:

  (i) type of data handled (if there is sensitive, pseudonymized, data of children and teenagers or other vulnerable groups data); **(ii)** quantity of data; **(iii)** position of data processing agent (controller or processor); and **(iv)** if there is an international transfer.

- To mitigate any foreseeable legal risks, it is recommended that the companies have four clause models for each of the types of data they handle (sensitive personal data; personal datal; pseudonymized data; and anonymized data);

- Companies should note particular issues that may be relevant, such as:

  (i) liability limitation clause; **(ii)** sharing data with third parties; **(iii)** response to security information incidents; **(iv)** auditing; and **(v)** compliance with the rights of data subjects.

- After finishing the text, it is recommended that companies negotiate with their internal areas to verify and validate the contractual provisions prepared; and

- Finally it's time to send the contract to the counterparties so that, after signature, it can produce the legal effects.

For more information, read the article **"Control of contracts"**, written by our partner Caio Lima and available in our e-book about DPO. Click **here** to access.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

DATA PROTECTION OFFICER (DPO) OR ENCARREGADO

LGPD created Encarregado, importing the idea of the Data Protection Officer (DPO), available in the General Data Protection Regulation (GDPR).

According to Article 5, item VIII, LGPD, Encarregado is a person appointed by the controller, who acts as a channel of communication between the controller, the data subjects and the Data Protection Supervisory Authority (ANPD).

Encarregado must watch over the activities of the company's data processing, ensuring they are in compliance with LGPD and good governance practices. To do this, all the taken decisions and instructions shall be validated by the controller, since it is he who defines the parameters of the data processing process.

Check out our e-book "DPO: Management of data privacy and protection programs".

DATA PROTECTION OFFICER (DPO) OR ENCARREGADO

The DPO is the essential person for companie's compliance with the the data protection law, including in face of the application of administrative sanctions of LGPD, that are exclusive ANPD competence, which entered in force on August, 1st, 2021

Although LGPD does not describe the DPO characteristics, we recommend:

- Legal and regulatory knowledge
- Risk management and auditing and compliance
- Leadership and proactivity
- Awareness provider /educator
- Public/Government Relations
- Knowledge in Technology and Information Security

Assignments set forth in LGPD and recommended to the DPO:

- Follow-up and monitor the compliance of the data processing agent with LGPD, and the other data protection rules and its own internal policies related to the subject
- To receive complaints and communications from the data subjects, provide clarifications and take measures
- To receive communications from the supervisory authority and take measures
- To carry out any other duties established by the controller or in supplementary rules
- To instruct the employees and contractors of the entity on the practices to be adopted in relation to the personal data protection

• The law does not require the DPO to be employed by the controller/processor, it is possible to outsource this activity (DPO as a Service).

• If DPO has other duties within the organization, we recommend that it is ensured that there is no conflict of interest between the DPO function and these duties.

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

DATA PROTECTION IMPACT ASSESSMENT

The Data Protection Impact Assessment (RIPD) is specified by Article 5, XVII, LGPD, and it is a controller documentation that contains a description of the personal data processing that can generate risks to the civil liberties and to the fundamental rights, as well as measures, safeguards and mechanisms to mitigate risks.

One of the competences of the Data Protection Supervisory Authority (ANPD) is to regulate the RIPD in cases in which the processing represents a high risk to the guarantee of the general principles of personal data protection foreseen in LGPD (Article 55-J, XIII).

Since ANPD regulations shall also be preceded by regulatory impact analyses (Article 55-J, § 2), it is important to measure and evaluate under what circumstances the efforts to carry out RIPD, such as time and cost, are proportional to the protection against violations of individual rights and guarantees.

Thus, ANPD shall only request RIPD from the controllers when the processing presents a high risk. In other situations, it is understood that the report shall be voluntary. The expectation is that the Authority, however, will prepare a short list of examples of processing activities that directly represent high risk.

DATA PROTECTION IMPACT ASSESSMENT

- Document prepared by the controller, describing the personal data processing that may put in risk the fundamental rights
- The document must contain at least the description of:
- It allows the risk assessment of the data processing before it is actually carried out, in order to mitigate the risks
- The Data Protection Supervisory Authority (ANPD) may request the Data Protection Impact Assessment for the data processing that involves a legitimate interest, as well as determine that it is done for processing involving sensitive data

- Type of the collected data
- Methodology used for the collection and security of information
- Controller analysis of measures that can be implemented to minimize the risks

LGPD 3 YEARS

The Data Protection Impact Assessment is a way to assess the existence of risks to fundamental rights and identify potential risks to the principles set forth in LGPD. Check out the article written by our partner Rony Vainzof.

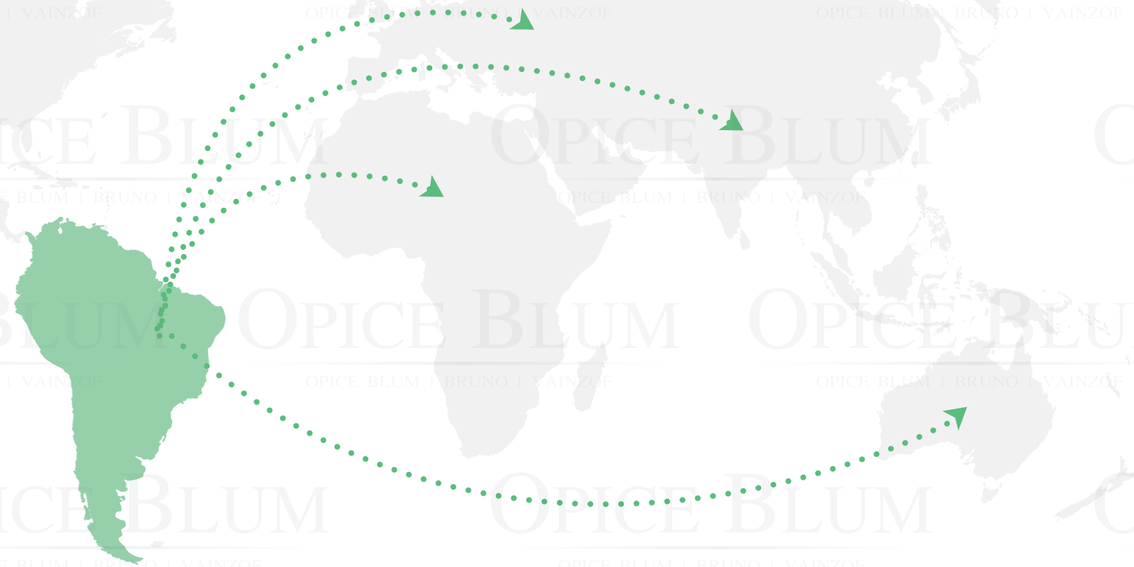
MAIN ASSUMPTIONS OF INTERNATIONAL TRANSFER OF PERSONAL DATA

LGPD provides, in articles from 33 to 36, specifically 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 countries that have a certain level of data protection.

To assess if the country of destination has the appropriate level of data protection, the Data Protection Supervisory Authority (ANPD) takes into account some factors such as:

- The general and sectorial laws in force in the destination country;
- The nature of the data; and
- Compliance with general principles of data protection and the rights of the data subjects.

MAIN ASSUMPTIONS OF INTERNATIONAL TRANSFER OF PERSONAL DATA



- Destination country with adequate level of protection for LGPD. This assessment shall be carried out by ANPD.
- In the cases that the data subject has given specific and highlighted consent for the transfer.
- In the case that the transfer results in a commitment undertaken by means of an international cooperation.
- To protect the life or physical safety of the data subject or a third party.
- Concerning international legal cooperation for research purposes and for the performance of public policy.
- In the cases that the controller offers guarantees:
  - specific contractual clauses;
  - global corporate standards;
  - standard contractual clauses; and
  - regularly issued stamps, certificates and codes of conduct.
- When authorized by Data Protection Supervisory Authority (ANPD).

LGPD 3 YEARS

The assumptions foreseen for international transfer of data are exhaustive and must be respected by the controllers.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

DATA PROTECTION SUPERVISORY AUTHORITY – ANPD

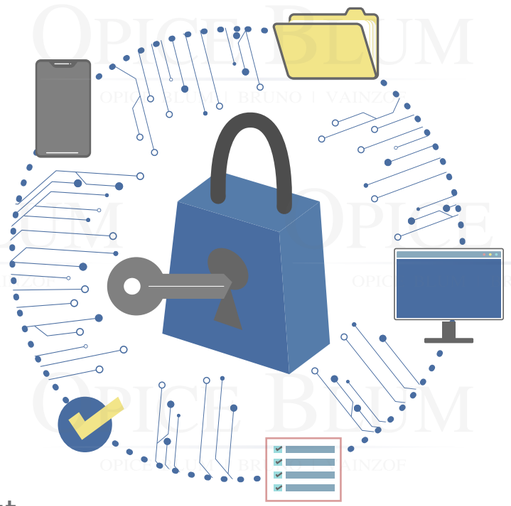
Created in 2018 by the Provisional Measure 869, later converted into Law 13.853/2019, sanctioned on July 8th, 2019, ANPD was structured a year later, by the Decree 10.474/2020, published on August 27th.

ANPD is responsible for ensuring the protection of personal data; preparing guidelines for the Personal Data Protection and Privacy National Policy; promoting knowledge of rules and public policies on data protection and security measures; applying administrative sanctions; etc.

DATA PROTECTION SUPERVISORY AUTHORITY – ANPD

It is the Authority responsible for regulating, inspecting and sanctioning, whose main attributions are the following:

- Ensure the protection of personal data, as provided in legislation;
- Elaborate guidelines for the Personal Data Protection and Privacy National Policy;
- Promote the knowledge of the norms and public policies on the protection of personal data and of the security measures to the general population;
- Promote cooperation initiatives with data protection authorities of other countries, of international or transnational nature;
- Implement simplified mechanisms, including by electronic means, in order to collect and record complaints on the processing of personal data non-compliant with LGPD;
- Receive pleadings from the data subject against the controller after the data subject has demonstrated that he/she presented a complaint against the controller that was not solved in the timeframe established in regulation;
- Amend regulations and procedures on the protection of personal data and privacy, as well as on data protection impact assessment reports in cases that the processing represents a high risk to the guarantee of the general principles of personal data protection foreseen in LGPD;



- Discuss, at the administrative level, on the interpretation of LGPD, its authorities and matters on which the Law is silent;
- Carry out audits, or to determine their occurrence regarding the processing of personal data carried out by processing agents, including public authorities;
- Monitor and apply sanctions for data processing that is not compliant with legislation, by means of an administrative process that ensures right to adversary proceeding, full defense and the right to appeal;
- Stimulate the adoption of standards for services and products that facilitate the control of data subjects regarding their personal data, which should take into account the specificities of the activities and the size of those responsible;
- Coordinate with public regulatory authorities to exert their authority in specific sectors of economic and governmental activities bound to regulation; and
- Enact rules, guidelines and simplified and special procedures, including deadlines, so that microenterprises and small businesses are able to adapt to LGPD, as well as incremental or disruptive business initiatives that declare themselves startups or innovation companies.

LGPD 3 YEARS

It is important that ANPD prioritizes a constructive engagement with the private sector, by means of dialogue, support, mutual cooperation, guidance, awareness and information. The administractives sanctions should be the last option and should be applied when there is an intentional breaking or in the case of negligent practices.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

ADMINISTRATIVE SANCTIONS APPLICABLE BY THE ANPD

ANPD also has a competence to apply the administrative sanctions mentioned in Article 52 of LGPD, that may vary from a warning to fine of up to 2% of the company's annual revenue, limited to R$ 50 million per infraction.

The Bill 1.179/2020, later converted into Law 14.010/2020, postponed the beginning of the validity of the administrative sanctions for the August 1st, 2021.

For more information, read our report about the administrative sanctions of article 52 of the LGPD.

ADMINISTRATIVE SANCTIONS APPLICABLE BY THE ANPD

Valid from 1st August, 2021 (Law 14.010/2020):

- Warning
- Simple fine of up to 2% of BRL 50 million per infraction
- Daily fine
- Disclosure and publicization of the infraction
- Blocking of the personal data to which the infraction refers
- Deletion of the personal data involved
- Partial suspension of the operation of the database related to the infraction for a maximum period of 6 months
- Partial or total prohibition of activities related to data processing

ANPD will take into consideration:

- The severity and the nature of the infractions
- The good faith of the offender
- The advantage received or intended by the offender
- The economic condition of the offender
- The recurrence and the level of damage
- The adoption of internal data protection and mechanisms procedures
- The adoption of good practices and governance policy
- The adoption of corrective measures
- The proportionality between the severity of the breach and the intensity of the sanction

LGPD 3 YEARS

- ANPD shall define the methodologies that will guide the calculation of the base value of fine sanctions through its own regulation on sanctions for violations of LGPD. This document has already been subject to public consultation.
- The methodologies shall be previously published to make possible that the data processing agents know the forms and methods used in the calculation.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

INCIDENT RESPONSE PLAN

Identifying an incident is not always a simple and quick task. On the contrary. It is common for a system to be hacked for months before the breach is found. Another common situation occurs when the company is informed by email (usually, the contact email available on the website) by the fraudster about the incident.

Therefore, those responsible for the Information Security of organizations must have routines implemented and checked frequently (which include the observation of alerts issued by tools dedicated to defend the systems), so that it is possible to identify the incident internally, and not by third parties.

After confirming the incident, it is necessary to understand, in greater detail, its extension, based on multi-sectorial action, which shall facilitate the proper response previously defined by the organization. The team responsible for this work must, at a minimum, contain representatives from the Departments of Technology, Information Security, Legal, Public Relations and Communications, who shall be called to compose the "Crisis Committee".

LGPD 3 YEARS

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

NEW INFOGRAPHIC

INCIDENT RESPONSE PLAN

15 steps to identify and respond to a security incident:

1. Preservation of the evidences
2. Communication to the insurance company, when relevant
3. Formation of the Crisis Committee
4. Identification of the root cause of the incident
5. Containment of vulnerability
6. Identification of data exposure
7. Web scanning: surface and deep web monitoring
8. Elaboration of the level of incident severity
9. Definition of communication to data subjects and authorities
10. Elaboration of script to answer consumers questions
11. Elaboration of relevant fact, if applicable
12. Elaboration of reactive notes to the press
13. Forensics Report of incident
14. Legal strategy for containment
15. Legal measures to identify the offender

LGPD 3 YEARS

You can find more information in the booklet "How to identify and react to security incidents". Click here and read it.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

CREDITS

PARTNERS

José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio César Carvalho Lima
Danielle Serafino

EDITORIAL COORDINATION

Bruno Toranzo

REVIEW

Rony Vainzof
Caio César Carvalho Lima
Giovana Figueiredo Peluso Lopes
Bruno Toranzo
Yasmin Brandão

ART AND DESIGN

Paola Cosentino

TRAINEE

Lucas Fernandes

LGPD 3 YEARS

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF