LEFOSSE
ADVOGADOS

17 August 2018

The Brazilian General Data Protection Act is approved

Brazil has now a comprehensive set of rules that reshape how Brazilian companies, organizations and public authorities have to collect, use, process and store personal data.

The Brazilian General Data Protection Act (*Lei Geral de Proteção de Dados* – "**LGPD**") was approved on 14 August 2018. The LGPD protects private and personal data of Brazilian citizens and is a data protection framework inspired by the General Data Protection Regulation ("**GDPR**"), which came into force in the European Union on 25 May 2018.

This new law represents a **radical change** in the way privacy of individuals is treated in Brazil. Individuals ("**data subjects**") now enjoy broad control and autonomy over their own personal data, which may only be collected, used, processed and stored under the strict rules imposed by the LGPD. These rules are in line with most advanced international privacy and data protection standards

The LGPD will **come into effect in 18 months from now (i.e., in 2020),** granting Brazilian companies and organizations a suitable transition period to adopt to the new rules.

Briefly, LGPD brings the following innovations:

- **Provides for 10 legal bases for data processing**, such as **consent** of the data subject, **legitimate interest** of the controller (i.e., the person responsible for the decisions related to the processing of personal data), compliance with **legal or regulatory obligation**, when necessary for the **performance of a contract**, among others;
- **Strict criteria** for the processing of **sensitive personal data**, defined as data revealing racial or ethnic origin, religious belief, political opinions, affiliation to labor unions or to religious, philosophical or political organizations, as well as data related with health or sexual life, genetic or biometric data, whenever pertaining to an individual;
- **Principles** that must guide data processing activities, such as the **principle of purpose**, which means that data processing can only be carried out for a specific and legitimate purpose, without any subsequent treatment in a manner incompatible with such purpose. Other principles provided for by the GDPR are also covered by the LGPD, such as **adequacy**, **accuracy**, **transparency**, **accountability**, among others.
- **Rights of data subject**, such as **right of access**, right of data **rectification**, **cancellation or exclusion**, **right to object** the processing, **right to revoke consent** previously given, **right of information and explanation** regarding the use of data, right of **data portability** amongst others;
- **Specific rules** for processing of personal data of **children and teenagers**;
- **Strict criteria** for **international transfer** of personal data;

- **Processing of personal data by public authorities** must be serve a public purpose, provided that all other legal requirements are met;
- **Data Protection Officer ("DPO")** must exist to ensure that the LGPD is duly complied with, as well as with any other regulatory rules issued by the data protection authority. The DPO position can be fulfilled by an officer, a manager, an employee, or even a third party provider, as long as his/her duties are performed with autonomy;
- **Liability of data controllers and processors**, which will require a clear definition of the scope of each of their attributions in data processing agreements;
- **Administrative and technical security measures** will be required to protect personal data from unauthorized access and accidental and unlawful situations of destruction, loss, modification, communication, or any other form of inadequate or unlawful processing;
- **"Privacy by design"** concept imposing **security measures** to protect personal data already as from the **conceptual stage** of a product or service until its **operation** or **performance**;
- **Mandatory data breach notifications** to the ANPD and data subjects, and
- **Administrative sanctions** in case of violations, including **fines of up to 2% of the Brazilian revenues of a company, economic group or conglomerate**, capped at R$ 50,000,000.00 per violation.

The original wording of the Bill approved by the Senate provided for the creation of the **National Authority for the Protection of Personal Data (ANPD)**, which would be a federal agency responsible for supervising the application of the LGPD. However, this provision was vetoed by the Brazilian President. There will be a new bill to create the supervising authority before the LGPD comes into effect.

The LGPD will significantly affect the Brazilian economy, resulting in considerable changes how personal data is treated in Brazil. The new law is likely to impact the business of financial institutions, hotels, tourism agencies, hospitals, health insurance operators, drugstores, pharmaceutical companies, healthcare providers, restaurants, retailers, universities, internet service and application providers, telecom service providers, technology companies, cloud computing providers, advertising agencies, law firms, public authorities, among others.

Moreover, the LGPD will affect the relations between suppliers and their customers, consumer relations, relationships between employers and their employees, among others that imply processing of personal data, either online or offline.

Please find below our key considerations on the LGPD:

Material and territorial scope of LGPD

LGPD is applied to **any operation involving processing of personal data** conducted by an individual or a public or private entity, which (i) **is carried out in Brazil**; (ii) has the purpose of **offering or supplying goods and services to** or **the processing of personal data of individuals located in the Brazilian territory**; **or** (iii) involves **personal data collected in Brazil**, regardless of the means, the country where the entity's headquarters is based or the country where the data is located.

Therefore, like the GDPR, the LGPD has an **extraterritorial application**, i.e., it is enforceable even against foreign companies, as long as they have an affiliate or subsidiary located in Brazil, offer goods or services in the Brazilian market, or collets personal data of individuals located in Brazil.

LGPD is not applicable to the processing of personal data:

- carried out by individuals for private purposes;
- for journalistic, artistic or academic purposes;
- for the exclusive purposes of public security, national defense, State's security, or activities of criminal investigation and repression of criminal offenses (in this latter case, there will be specific legislation); or
- originated from outside the national territory and that is not object of communication, shared use with Brazilian data processing agents or object of data transfer with other country which is not the country of origin, provided that the country of origin offers adequate degree of data protection in line with the LGPD.

Concept of "personal data"

"**Personal data**" is defined as **any information relating to an identified or identifiable natural person (called "data subject")**. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as IP number) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Concept of "sensitive personal data"

LGPD defines "**sensitive personal data**" as data revealing racial or ethnic origin, religious belief, political opinions, affiliation to labor unions or to religious, philosophical or political organizations, as well as data related with health or sexual life, genetic or biometric data, whenever pertaining to an individual.

It is worth mentioning that the processing of sensitive personal data is subject to even more strict requirements for processing.

Anonymized data

"Anonymized data" is defined as **data relating to a data subject that cannot be identified, considering the use of reasonable and available technical measures existing by the time of the processing.** By means of an anonymization process, a data no longer could be associated, directly or indirectly, to an individual. Therefore, anonymous data are out of the scope of the new Law.

Data processing

LGPG defines data processing **as any operation conducted with personal data**, such as the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, storage, elimination, evaluation or information control, modification, communication, transfer, diffusion or extraction.

Summarily, any activity carried out by using personal data is covered by this concept and subject to the LGPD.

Processing agents

Processing agents are individuals or companies that effectively collect and use the personal data, being the (i) **controller**, i.e., the individual or public or private entity responsible for the decisions related to data processing, and (ii) **processor**, defined as individual or public or private entity that performs personal data processing on behalf of controller.

Normally, controller enters into a data processing contract with a processor in order to enable the processing of personal data in accordance with the Law and instructions by the controller. For instance, a company may retain service provider for processing its employees' data. In this case, the contracting party (i.e., the employer) would be deemed the controller, whereas the service provider will be processor. In any case, it is usual that a single entity performs both activities, acting as controller and the operator.

Principles

LGPD provides a list of principles to serve as a guidance for data processing activities, such as:

- **Purpose**: personal data processing must be carried out only for fair, specific, legitimate and explicit purposes informed to the owner, without the possibility of subsequent treatment in a form incompatible with these purposes;
- **Adequacy**: data treatment must be compatible with the purposes informed to the data subject;
- **Necessity**: limitation of data processing only to the extent necessary to achieve the purposes;
- **Free access**: data subject should be able to consult, easily and free of charge, the form and duration of the processing, as well as the integrity of their personal data;
- **Quality of the data (accuracy)**: data subjects must be ensured that their data is accurate, clear, relevant and updated, in line with the conformity, necessity and purpose of the processing;
- **Transparency**: guarantee of clear, accurate and easily accessible information to data subjects with regard to the processing activities and the respective processing agents (controllers and processors);
- **Security**: use of technical and administrative measures to protect personal data from unauthorized access, incidents or unlawful acts that result in destruction, loss, alteration, communication or data disclosure;
- **Prevention**: adoption of preventive measures against occasional damages resulted from data processing;
- **Non-discrimination**: prohibition of data processing for purposes of discrimination, performance of unlawful or abusive acts; and

- **Accountability**: the controller or processor must adopt effective measures that provide evidence of compliance with data protection, as well as demonstrating the effectiveness of such measures.

Legal Requirements for Data Processing

LGPD provides 10 legal bases upon which personal data may be legally processed:

- Through **consent** by the data subject;
- For **compliance with legal or regulatory obligation by the controller**;
- By the **Public Administration**, for the processing of data that is necessary to the **implementation of political policies**;
- For carrying out **studies by research agencies**, provided that anonymization is ensured;
- Whenever it is necessary for the **performance of a contract**;
- **As a means of regular exercise of rights** in a judicial, administrative or arbitration proceeding;
- **For protection of life or physical integrity**;
- For **the protection of health**, when the proceeding is carried out by healthcare of professionals or sanitary entities;
- **Legitimate interests** of the controller or of third parties, unless in the event the fundamental rights of data subject prevail; and
- **Credit protection**, in accordance with the applicable laws and regulations.

Even though some of the legal requirements above may seem subjective and will be subject to further regulation, we understand that the legal basis of consent by the data subject and the legitimate interest of the controller are likely to raise more doubts and discussions.

In any event, regardless of the legal basis for data processing, each decision of processing and its respective legal basis must be duly registered and documented by the controller and processor.

Consent

Consent is defined by the LGPD as a **free, informed and unequivocal manifestation, through which the owner agrees with the treatment of his/her personal data for a specific purpose**.

The consent must be given in **writing** or by **any other means** which shows a **clear manifestation of the data subject's will**. In case of a consent in written form, it must be expressed in clauses that are highlighted and separated from the remaining clauses. Consent **must refer to specific purposes, which means that generic authorizations will be deemed null and void**. Therefore, in the case of change of a purpose for the processing of data that is not compatible with the consent originally granted, controller must previously inform the data subject about this change, what corresponds to requiring a new consent from the data subject.

The **consent may be revoked at any time** by express manifestation of the data subject, by means of a facilitated and free of charge proceeding.

In case of a **sensitive personal data**, consent must be given on a **specific and highlighted manner, solely for specific purposes**, being unnecessary only in exceptional circumstances provided for by the LGPD.

In practice, the new requirements for granting the consent represent the end of long and ambiguous terms of services and privacy policies that grants almost absolute powers to processing agents for generic and undefined purposes, which may even be harmful to data subjects.

Legitimate Interests of the controller

Pursuant to the LGPD, **legitimate interest of the controller** may only justify a data processing for legitimate purposes, to be considered based on **concrete situations**, such as the support and promotion of controller's activity, protection in relation to the data subject, the regular exercise of his/her rights or the rendering of services that may benefit him/her. Thus, whenever there are clear circumstances whereby data processing is necessary to meet the controller's legitimate interests, consent may be dismissed.

The legitimate interests of the controller as a legal basis for data processing has been subject of great discussion in Europe, given that this is also provided for by the GDPR, and it is still not clear what are the practical situations whereby the legitimate interest of the controller could be relied upon to justify processing. For instance, a company or an organization could have the legitimate interest when the processing of personal data is performed in the context of its relationship with a client, for direct marketing purposes, to prevent fraud, or even to ensure security of its network and information in its IT systems.

Regardless of the justification for the processing based on the legitimate interest of the controller, it will be necessary to **balance the interests of the controller and the rights of data subjects,** pursuant to the LGPD. In practice, even though there are clear justifications for data processing based on the legitimate interests of the controller, data subjects must always be informed about this fact and his/her rights and liberties may not be adversely impacted. Otherwise, the controller will not be entitled to rely upon its legitimate interests as a basis for processing.

In any case, the legitimate interest may turn out to be an important legal basis for processing activities carried out by technology companies active in data-driven innovation markets, such as data mining, data analytics, artificial intelligence, machine learning, as well as financial institutions, insurance companies, telecom operators, healthcare companies, amongst others.

Rights of data subject

LGPD clarifies that any individual is ensured with ownership of his/her personal data, granting them the fundamental rights of freedom, intimacy and privacy. Among the rights provided by LGPD, we highlight the following: **right to access of personal data**; **right of data rectification, cancellation or exclusion**; **right to oppose** to the processing; **right to revoke consent previously given**, **right of information and explanation** regarding the use of his/her personal data, amongst others.

The LGPD also provides for the **right of data portability** to another supplier of the product or service, by means of request by the data subject. For instance, the data subject may request that a

streaming provider, like Spotify, transfers his/her personal data to a competitor streaming service provider.

In this context, it is worth mentioning that data protection authority may establish standards of interoperability for purposes of portability and free access to data.

Other highlight is the **owner's right to request revision, by an individual, of decisions solely taken based on automatized data processing**, including those **decisions** that define the **personal, professional, consumer** or **credit profile** or aspects **of his/her personality**. Upon request, a controller must provide the data subject with **clear and adequate information** in connection with the criteria and the proceedings used for an automatized decision. This "right of human revision", or "explanation" of automatized decisions may affect companies that rely on automatized technological devices to evaluate credit applications, recruiting, insurance, among others.

Children and teenagers

LGPD sets forth specific rules for the **treatment of children's and teenagers' personal data**, which must be carried out by means of **specific and unequivocal consent granted by, at least, one of his/her parents or legal representative.** This consent may be dismissed whenever personal data must be collected in order to contact the parents or legal representatives.

International transfer of personal data

The LGPD provides for a clear and detailed framework for international transfer of personal data. We highlight the following circumstances that authorizes international transfers:

- Transfer to **countries or international organizations that provide a degree of protection of personal data that is compatible** with the standards of the LGPD;
- In case **the controller offers and demonstrates guarantees of compliance with the principles and rights of data subjects and with the data protection regime provided for by the LGPD** by means of specific **contractual clauses, standard clauses, global corporate norms, seals, certificates and codes of conduct**;
- When the transfer is **necessary for international legal cooperation between public intelligence, investigation and prosecution bodies**;
- When the data subject has given **specific consent and highlighted for the transfer, with prior information about the international character of the operation**, clearly distinguishing this purpose from others.

Data processing by public authorities

The LGPD sets forth that the processing of personal data by the Public Administration must fulfil its public purpose, for meeting a public interest, provided that:

- The hypotheses whereby personal data is processed are duly informed, thereby providing clear and updated information on the legal provision, purpose, procedures and practices relied upon to carry out these activities;

- A Data Protection Officer must be appointed when conducting data processing activities.

In addition, the LGPD also sets out that state-owned and mixed-capital companies operating on a competitive basis, conducting economic activity, are subject to the same legal treatment as private entities. In the case state-owned companies acting in the implementation of public policies, they will have the same treatment as the bodies and entities of the Public Administration.

Regarding the sharing of personal data by public authorities, the LGPD sets forth that the data shall be ept in an interoperable format and structured for shared use. The shared use of personal data by public authorities shall fulfill the specific purposes of execution of public policies and legal attributions by agencies and public entities. In turn, **it is forbidden for public authorities to transfer to private entities personal data contained in databases to which they have access, except:**

- in cases of decentralized execution of public activity that requires transfer, exclusively for this specific purpose, subject to the provisions of the Brazilian Access to Information Law;
- in cases in which the data are publicly accessible.

As a rule, in case of data sharing between public agencies and private companies, except for the hypotheses indicated above, or in situations whereby consent is legally waived, it will be mandatory to notify the data protection authority regarding such personal data sharing, as well as to obtain the prior consent of the data subject.

Data Protection Impact Assessment (DPIA)

Processing agents must keep records of all personal data processing operations, especially when based on the legitimate interests. In this context, the LGPD establishes that the data protection authority may request the controller to draft a Data Protection Impact Assessment (DPIA), a documentation containing a description of the proceedings of processing of the personal data that could result in risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate the risk

This DPIA must contain, at a minimum, a description of the types of data collected, the methodology used for collecting data and ensuring information security, as well as the analysis of the controller in relation to the measures, safeguards and mechanisms for mitigating risks.

Data Protection Officer (DPO)

The LGPD sets forth that the operator must appoint a Data Protection Officer, which should be an individual responsible for ensuring the company's compliance with the LGPD. This position could be fulfilled by an officer, a manager, an employee, or even a third party provider, as long as he/she has autonomy to perform his/her duties.

The Data Protection Officer will be responsible for: (i) **receiving complaints and communications from the data subjects**, provide clarifications and take measurers; (ii) **receiving communications** from the data protection authority and adopt measures; (iii) **advising employees and third parties on the practices and measures** taken in relation to data protection; and (iv) **perform other duties** determined by the **controller**.

In any event, we believe that the data protection authority may waive the need for its appointment. Indeed, there is no point in imposing an obligation on all entities to appoint a DPO. Depending on

how a company or organization is internally organized, this position could be absorbed by the compliance team, by the legal department, or even by the human resources department.

Liability of processing agents

The **controller and the processor that causes damages to data subjects as a result of processing** activities, in violation of the LGPD, will be required to indemnify individuals that suffer such damages. Except in exceptional circumstances, the **data processor will be jointly and severally liable** in case it **fails to comply with the LGPD** or in case it **has not observed the lawful instructions of the controller**, in which case the processor will be treated as the controller. **Controllers** that are **directly involved in** data treatment that cause damage to data subject will be **jointly and severally liable**.

Thus, if a processor performs its activities in compliance with the LGPD and strictly observes the instructions of the controller, it will not be jointly and severally liable for any damages caused by the controller to data subjects. Likewise, the controller that is not involved in data processing activities that eventually cause damages to data subjects will not be jointly and severally liable for damages caused by the processor. Therefore, when drafting data processing agreements, it is highly advisable to set out a clear definition of the attributions of the controller and the processor, as well as limitation of liability, in order to mitigate risks.

Information security

LGPD establishes the obligation for processing agents to adopt technical and administrative **security measures to protect personal data from unauthorized access and from accidental or unlawful situations** of destruction, loss, alteration, communication or any form of inappropriate or unlawful processing.

Privacy by design

Inspired by the GDPR, the LGPD incorporated the concept of "**privacy by design**", which requires the adoption of **security measures** aimed at protecting personal data **since the design stage** of a product or service **until its operation or performance**.

In practice, the concept of **privacy by design** means that data protection risks must be taken into account throughout the whole process of designing a new technology, product, service or business model. This includes internal projects, product development, software development, IT systems, among others. Therefore, it will be necessary to ensure that privacy and data protection are incorporated throughout the life cycle of a system or process. In practice, the concept should directly affect entities engaged in research, development and innovation, especially software and hardware developers.

Notification of data breaches

LGPD requires the controller **to notify the data protection authority and data subjects on the occurrence of information security incidents (data braches)**. Such notification must be issued within a **reasonable term**, to be defined by the ANPD, and shall mention, as a minimum:

- **Description** and **nature** of the personal data affected;

- Information on the **data subjects involved**;
- Indication of the technical and security measures relied upon to protect the data;
- The **risks** related with the incident;
- The **reasons for the delay**, in case the notification was not immediate;
- Measures that have been or will be taken to reverse or mitigate the effects of the damages.

Depending on the **severity of the incident**, the data protection authority may require from the controller additional actions, such as the **disclosure** of the facts in the **media** and **measures** to revert or mitigate the effects of the incident.

Administrative penalties

Violations of the LGPD may subject controllers and processors to the following administrative penalties to be enforced by the data protection authority, after an administrative procedure that ensures the full right of defense:

- **Warning**, setting a deadline for the adoption of corrective measures;
- Fine of up to 2% of the company's, group's or conglomerate's turnover in Brazil in its last fiscal year, excluding taxes, limited to the amount R$ 50,000,000.00 per violation;
- **Daily fine**, observing the total limit mentioned above;
- **Publication of the violation** after duly verified and confirmed;
- **Blocking of personal data** to which the violation refers until its regularization;
- Elimination of the personal data related to the infraction.

* * *

CONTACTS:

For further information, please contact:

Zeca Berardo
zeca.berardo@lefosse.com
Tel.: (+55) 11 3024 6244

Paulo Lilla
paulo.lilla@lefosse.com
Tel.: (+55) 11 3024 6347

Elen Lizas
elen.lizas@lefosse.com
Tel.: (+55) 11 3024 6391

Lefosse Advogados
Rua Tabapuã, 1227 - 14th floor
04533-014 São Paulo SP Brazil

Avenida Presidente Wilson, 231office 2703
20030-905 Rio de Janeiro RJ Brazil