THE NEW BRAZILIAN GENERAL DATA PROTECTION LAW

BAPTISTA LUZ
ADVOGADOS

BAPTISTA LUZ ADVOGADOS
R. Ramos Batista . 444 . Vila Olímpia
04552-020 . São Paulo – SP
baptistaluz.com.br

/ Renato Leite Monteiro

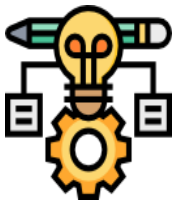
Brazilian General Data Protection Law: detailed analysis

Context

On July 10, 2018, bill of law PLC 53/2018 was approved in the Brazilian Federal Senate (access to the entire text, in Portuguese, here), which provides for the protection of personal data and amends the Federal Law 12.965/16 (known as the Brazilian Internet Civil Rights Framework, or "Marco Civil da Internet"), thus consolidating the Brazilian General Data Protection Law ("LGPD", in Portuguese). The public and legislative process began in 2010, with the opening of a public consultation on the subject, promoted by the Ministry of Justice, which later resulted in the filing of the bill of law PL 5276/2016, attached to the bill of law PL 4060/2012, before the House of Representatives. Now, after two years in the National Congress (House and Senate), two public consultations, more than 2500 contributions from national and international actors, from all sectors, numerous events, the legislative procedure comes to end and proceeds to presidential sanction (and perhaps, partial veto). If approved by President Michel Temer, the bill becomes law, with an adaptation period of 18 months.

on/offline

The LGPD creates a new legal framework for the use of personal data in Brazil, both online and offline, in the private and public sectors. It is important to note that the country already has more than 40 legal



Data Protection and Innovation

norms at the federal level that directly and indirectly deal with the protection of privacy and personal data, in a sector-based system. However, the LGPD is replacing and / or supplementing this sectoral regulatory framework, which was sometimes conflictive, marshy, without legal certainty and made the country less competitive in the context of an increasingly data driven society. The text, the result of a broad discussion, aims not only to guarantee individual rights, but also to foster economic, technological and innovation development through clear, transparent and comprehensive rules for the adequate use of personal data. By having a General Data Protection Law, Brazil enters the roll of more than 100 countries that today may be considered to have an adequate level of protection of privacy and the use of personal data.

What are the objectives of a General Data Protection Law?

- Right to privacy: guarantee the right to privacy and protection of personal data of citizens by allowing greater control over their data, through transparent and safe practices, aiming to guarantee fundamental rights and freedoms.

- Clear rules for companies: establish clear rules on collecting, storing, processing and sharing personal data for companies.

- Promote development: foster economic and technological development in a data driven society.

- Consumer law: ensuring free enterprise, free competition and consumer protection.

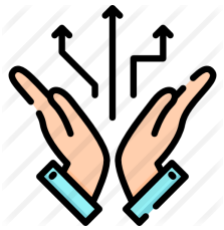
- Strengthen confidence: increase the confidence of society in the collection and use of your personal data.

- Legal certainty: to increase legal certainty as a whole in the use and processing of personal data.

What are the advantages of a General Data Protection Law?

- Unified rules: one set of harmonic rules on the use of personal data, regardless of the sector of the economy and society.

- Greater flexibility: allowing flexible, but secure, forms for the processing of personal data, such as legitimate interests, that consider a data-driven society in Big Data times.



- Reduce costs: reduce operational costs caused by systemic incompatibilities of data processing performed by different agents, as well as foster data quality among the data circulating in the ecosystem.

- Adapt the rules in Brazil: make Brazil able to process data from countries that require an adequate level of data protection, which can help foster information technology sectors.

- Data Portability: individuals can transfer their personal data from one service to another, increasing the competitiveness in the market.

What the law says

The LGPD has transversal and multisectoral application, both in public and private sectors, online and offline. It deals with the concept of personal data, lists the legal bases that authorize its use - and consent is only one of them, highlighting the possibility to process personal data based on the legitimate interest of the data controller - in addition to data protection general principles, basic rights of the data subject - such as right to access, exclusion of data and to explanation - obligations and limits that should be applied to any entity that process personal data. These are the main points of the new law:

- **Scope of application**: the LGPD will have transversal, multisectoral application to all sectors of the economy, both public and

private, online and offline. With few exceptions, any practice that process personal data will be subject to the law.

- **Extraterritorial application**: in a similar way to European regulation, GDPR, the General Law will have extraterritorial application, that is, the duty of compliance will exceed the geographical limits of Brazil. Any foreign company that has at least a branch in Brazil or offers services to the Brazilian market and collects and treat personal data of data subjects located in the country, will be subject to the new law.

- **Concept of personal data**: the LGPD provides for a broad concept of what should be deemed as personal data related to an identified or identifiable natural person. Any data, isolated or aggregated to another that may allow the identification of a natural person, or subject her or him to a certain behavior (interpretation possible from an integrative reading of the text). In Big Data times, which allows the rapid correlation of large, structured and unstructured databases, virtually any data can eventually be considered personal, therefore subject to the law.

- **Concept of sensitive personal data**: sensitive personal data is the type of data which by their very nature may subject the data subject to discriminatory practices, such as data on racial or ethnic origin, religious belief, political opinion, health or life data sexual; or allow unequivocally and persistently identification of the data subject, such as genetic data (this with both facets, discrimination and identification) or biometric. Such data should be treated in a differentiated manner, with additional security layers, and with different legal bases, such as the express consent of the data subject.

- **Anonymized data**: anonymized data refers to a data subject that cannot be identified, considering the use of reasonable technical means available at the time of the data treatment. In this way, anonymized data would be outside the scope of application of the law, except if the anonymization process can be reversed or if the data is used for

behavioral profiling purposes. Effectively anonymized data is essential for technologies within the scope of Internet of Things, artificial intelligence, machine learning, smart cities and analysis of large behavioral contexts.

- **Public data**: there is a great deal of discussion today about the limits on the use of publicly accessible personal data, such as those contained in databases managed by public bodies, official publications and notarial records, or those expressly made public by their data subjects, such as public profiles on social networks. The LGPD deals with such situations, treating them in different ways, and imposing certain limitations, such as the use limited to the purposes that led to the disclosure of the public accessible personal data.

- **Legal grounds for data processing - consent and legitimate interests**: to treat personal data, which includes the practice of collecting, it is always necessary to have a legal basis. The LGPD lists 10 hypotheses that authorize the use of personal data, and the unambiguous consent is only one of them. It should be noted that the legal basis known as "legitimate interest", that currently does not exist in the Brazilian legal data protection framework and would allow the use of the data for purposes other than those originally authorized by its data subjects or those that led to its disclosure. Through a proportionality test that considers the interests of the controllers and the rights of the data subject, this hypothesis would allow for new uses for the data, making it essential in times of Big Data, artificial intelligence, Machine Learning and innovative business models based on the use of personal data.

- **General Data Protection Principles**: The LGPD lists 10 principles that should be taken into account in the processing of personal data, such as purpose limitation, necessity, transparency, security, non-discrimination and - the new - principle of accountability, which makes it mandatory to the data controller and data processor to fully and transparently demonstrate the adoption of effective measures

capable of proving compliance with the rules for the protection of personal data, which can be done through data protection assessments, methodologies also provided for by law.

- **Data subjects basic rights**: data subjects will have their basic rights expanded, and they must be guaranteed in an accessible and effective manner. Among the listed rights, it is important to highlight the right to access to data, rectification, cancellation or exclusion, opposition to treatment, right to information and explanation about the use of data. The great novelty is the right to data portability, which allows the data subject not only to request an entire copy of her or his data, but also to have them provided in an interoperable format, which aims to facilitate their transfer to other services, even for competitors. Due to its nature, this new right has been a strong element of competition between different companies offering similar services based on the use of personal data.

- **National Data Protection Authority**: one of the most relevant points established by the law is the creation of an autonomous and independent public authority for the supervision of law and enforcement - in the bill, named as National Data Protection Authority (ANPD, in Portuguese). Its format has not yet been defined, but it should work in the same way as other regulatory agency, or supervisory bodies. The Authority may establish guidelines for the promotion of protection of personal data in Brazil. In summary, it should ensure the protection of personal data, elaborate the "National Policy on Data Protection and Privacy", as defined by law, monitor and apply sanctions in case of violation of the relevant laws, fulfill data subjects' requests against those responsible for the processing of their data, regulatory matters on data protection, among other activities. The LGDP also provides for the creation of the National Data Protection Council, a consultative body with a multisectoral composition, which can propose guidelines and strategies, conduct studies and disseminate knowledge on data protection in Brazil.

- **Data Protection Officer (DPO)**: The DPO is the natural person, nominated by the controller, who acts as a communication channel between the controller, data subjects and the Data Protection Authority. In addition, he or she should be responsible within the institution for the company's compliance with the rules provided by law and guide employees and contractors of the entity regarding the practices to be taken in relation to the protection of personal data. An initial reading of the LGPD allows to conclude that any entity that treats personal data must indicate a DPO, but the Data Protection Authority may establish complementary norms on the definition and the attributions of the person in charge, including hypotheses on which companies will not need to nominate a DPO.

- **Data Protection Impact Assessment (DPIA)**: considered as an impact assessment on the protection of personal data, it refers to the controller documentation that contains the description of data processing activities that may create risks to data subjects, as well as measures, safeguards and mitigation mechanisms implemented. The DPIA may be mandatory in situations already characterized as risky or, at the request of the Authority, where the processing of data is based on legitimate interest. The DPIA methodology is widely adopted by the GDPR and allows, in addition to risk mapping, an effective photograph of the entity's regulatory compliance status.

- **Record Data Processing Activities**: all personal data processing activities must be recorded, from their collection to their exclusion, indicating what types of personal data will be collected, the legal basis that authorizes their uses, their purposes, the retention time, the information security practices implemented in the storage and with whom the data can be eventually shared, methodology known as data mapping.

- **Information Security Standards**: both data controller and data processor should take appropriate technical, security and administrative measures to protect personal data. The Data Protection

Authority may provide for minimum technical standards, considering the nature of the data handled, the specific characteristics of the treatment and the current state of technology.

- **Privacy by Design and by Default**: it is mandatory to adopt from the design of services, products and business models the practice of guaranteeing privacy and data protection rights. The general principles of LGPD and safety standards should therefore be observed from conception to execution and offering of the product and service. Also, privacy controls, popularly accessible through dashboards in online platforms, should by default be the most protective, and it is up to the data subjects to make them flexible if they so wish.

- **Codes of Conduct and Certification Bodies**: The LGPD clearly encourages the adoption of industry codes of conduct and certifications bodies that can ensure compliance with the data protection rules. Certain sectors of society may create their own codes of conduct in the use of data, which may even be higher than the law. These must be previously authorized by the Authority and provide methods that demonstrate compliance. Furthermore, entities may qualify before the Authority to certify that other institutions are in compliance with the general law.

- **International Data Transfers**: LGPD brings a series of legal instruments that allow for the international transfer of personal data, even to countries that are not considered to have an adequate level of protection. It will be possible to internationally transfer personal data based on the specific and express consent of the data subject, which must be prior and separated from the other purposes and requisitions of consent. It will also be possible to carry out the transfer if there is a guarantee, by the controller, through contractual instruments, such as binding corporate rules and standard clauses, that it will comply with the principles, data subject rights and the data protection regime provided by law. Like the GDPR, the law allows for transfer by means

of the adoption of seals, certificates and codes of conduct issued and authorized by the Data Protection Authority.

- **Liability**: the different agents involved in the data processing - the controller and the processor - can be jointly and severally liable for information security incidents and / or improper and unauthorized use of the data, or for non-compliance with the law. However, the liability of the processor, that is who practices data processing on behalf of the controller, may be limited to its contractual and information security obligations if it does not violate the rules imposed by the LGPD. It is therefore important to define whether a company should be viewed as a controller or a processor, or both, to set the limits of its liability.

- **Mandatory Data Breach Notification**: data breach notifications to the Data Protection Authority becomes mandatory, and it must be performed within a reasonable time frame, which may, based on the severity of the case, determine the notification to all data subjects involved and the widespread publicity of the incident, which can have a huge reputational impact on the institution's image, and even lead to its devaluation in the market and loss of consumer confidence.

- **Penalties**: administrative sanctions may be applied by Authority in case of violation of LGPD. Among the sanctions, there are notices, fines, or even the total or partial prohibition of activities related to data processing. Fines may vary from 2% of the company's, group's or conglomerate's turnover in Brazil in its last fiscal year, limited in total to R$ 50,000,000.00 (fifty million reais) per infraction. There is also the possibility of daily fine to compel the entity to cease violations.

- **Transition and adaptation period**: the LGPD will enter into force 18 months after its publication. That is, public and private entities will have this period to adapt. In addition, the National Authority may establish rules on the progressive adaptation of databases created up to the date of entry into force of the Law, considering the complexity of the processing operations and the nature of the data.

Next steps

The LGPD now goes for presidential sanction. The Presidency can either abide by the law, deny it completely or veto certain parts. Much has been said about the possibility of vetoing the creation of the National Data Protection Authority, based on several arguments, both legal, political and budgetary. However, to enact a general data protection law without an autonomous and independent authority may have an undesirable impact on its effectiveness, and even render the law incomplete, since its text makes 56 references to Authority, and certain parts simply will not make sense without its existence.

Following the publication of the law, entities will have 18 months to adapt. It can be a difficult and costly task, especially for those who may decide to start adapting by the end of the transition period, practice that has been widely seen in the context of GDPR.

In short, the LGPD will have an impact on society as few laws have had before, since, today, practically every practice of the society deals with the use of personal data. Companies from all sectors will have to adapt and a new culture about the appropriate use of data must be formed, something difficult to achieve considering that Brazil, unlike other regions of the world, mainly in Europe, is still in its infancy regarding this topic.

In this sense, the protection of personal data should and can be seen not as a cost, but as a competitive advantage, a market differential. In a time of major information leaks and scandals over misuse of data, complying with clear, transparent and harmonic rules can restore or increase consumer confidence in companies and the marketplace. Therefore, companies need to conform to today's rules and understand that anticipating future regulation is an investment and a competitive advantage.