Personal data processing in Brazil: A new scenario to come

By Carla do Couto Hellu Battilana, CIPP/E, and Shin Jae Kim, CCEP

Carla do Couto Hellu Battilana (ccouto@tozzinifreire.com.br) is a Partner in the Privacy and Information Technology practice, and Shin Jae Kim (skim@tozzinifreire.com.br) is a Partner in the Compliance practice at TozziniFreire Advogados in São Paulo, Brazil.

The data privacy legal framework is going through important modifications in Brazil: the Brazilian General Data Protection Law—Law 13.709/2018 (LGPD)—that regulates the treatment of personal data in public and private sectors was enacted in August 2018. The law was inspired by international guidelines, especially those provided by the European Union’s General Data Protection Regulation (GDPR), and is supposed to come into force in August 2020.

The aim of this article is to provide an analysis of the innovations brought to the Brazilian data privacy scenario by the publication of the LGPD and the effects that it may have on different types of businesses.

An overview on current Brazilian data protection legislation

There are several pieces of legislation in Brazil dealing with different scopes of privacy and data protection, such as intimacy, private life, honor, image and secrecy of correspondence, bank operations, and communications. Such pieces of legislation include the Federal Constitution, the Civil Code, the Consumer Protection and Defense Code, the Brazilian Internet Act, and the Criminal Code.

Accordingly, although online treatment of personal data is governed by the Brazilian Internet Act and treatment of consumer personal data is governed by the Consumer Protection and Defense Code, online treatment of consumer personal data is governed by both pieces of legislation.

The LGPD does not replace the current legislation, but supplements it. Therefore, as of August 2020, personal data protection in Brazil is going to rely mainly on the LGPD, but the other pieces of legislation will continue to be valid and effective for specific matters.

As an additional remark, note that the Brazilian National Data Protection Authority was vetoed in the promulgation of LGPD for an alleged breach of legislative initiative. In December 2018, however, Provisional Measure 869/2018 (MP) created such authority and modified the vacatio legis period of LGPD from 18 months as of its publication to 24 months (August 2020). In order to gain definitive effectiveness, the MP must be converted into law by the National Congress.

As of when this paper was submitted, the MP was not converted; therefore, it is not possible to confirm when the LGPD will come into force.

The LGPD

The LGPD addresses the processing of personal data in both public and private sectors. It was based on international standards and is applicable to the processing of personal data carried out in the Brazilian territory, or the processing of personal data that has been collected in the Brazilian territory.

The definitions of “personal data” and “processing” are similar to the ones set forth in the GDPR, which means that the scope of application of the law is broad, because personal data means any data related to an identified or
identifiable individual, and processing is basically any operation carried out with the data, such as collection, reception, storage, use, transfer, access, communication, etc.

Similarly to the GDPR, the LGPD ensures several data subject rights that may be exercised at the request of the data subject, as follows: (1) right to information, (2) right to access, (3) right to rectification, (4) right to data elimination, (5) right of opposition, (6) right of portability, and (7) right to review automated decisions.

Whereas the current Brazilian legislation only permits data processing pursuant to data subjects’ prior and express consent, the LGPD modifies this rule and expands the situations in which personal data may be processed.

In addition to consent, data processing is also allowed in the following hypothesis: (1) due to a legal or regulatory obligation; (2) by the public administration as required for the enforcement of public policies; (3) by research bodies, whenever the anonymization of the personal data is possible, and limited to the minimum necessary to achieve the purpose of the research; (4) whenever necessary for the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject; (5) for the regular exercise of rights, including in lawsuits, administrative, or arbitration proceedings; (6) for protection of life or physical safety of the data subject or of third parties, as well as in a procedure carried out by health professionals or by sanitary entities; (7) for the controller’s legitimate interest; and (8) for purposes of credit protection.

Data subjects shall have clear, accurate, and easily accessible information about who is processing their personal data. Therefore, if the controller that obtained the consent from a data subject intends to communicate or share personal data with other controllers, it must obtain a specific consent from the data subject for this purpose as well.

One of the most important steps for compliance with the LGPD is mapping the data flows and processing activities. Once companies identify the personal data collected, how the processing is carried out, and for which purposes the data is processed, it will be possible to assess whether the intended data treatment can be framed into one of the possible lawful bases for processing. This is the reason why mapping is essential for companies to comply with the law: They must understand what they do with the data and then adjust practices as needed.

Until August 2020, consent remains as the central key of the Brazilian data protection legislation, but one must keep in mind that different business sectors have specific rules that may enable, oblige, or forbid personal data processing.

The “real” consent and its characteristics

Generally, in Brazil, data subjects currently must provide their prior and express consent to data treatment. Whereas consent is basically the sole basis for data processing today, once the LGPD comes into force, consent will be placed together with nine other scenarios where personal data processing is legally allowed.

Although the importance of consent remains significant, several changes in the structure are implemented by the LGPD to increase data subjects’ control and, consequently, hamper the controller’s obtainment of consent.

All purposes of the processing will have to be communicated in a clear, detailed, and individual way, and the controller is going to have the burden of proving that consent was provided in accordance with the law. In other words, companies will have to create technological means to store consent evidence, as well as ensure that all data subjects’ rights are being followed and respected.

The LGPD defines consent as the “free, informed and unequivocal manifestation” by means of which the data subject agrees with the processing of the personal data for a determined purpose.

A “freely given” consent is directly related to the data subject’s bargaining power[1] and the ability to provide a granulated consent,[2] where a data subject can agree to some aspects of the data processing and decline others.
According to Bruno Bioni, the “informed” aspect of the consent is associated with the information provided to the data subject. Once the data subject is provided with original and unpredictable information that protects from information asymmetry, the data subject is capable of truly understanding the nature of the consent granted and, therefore, providing a well-informed consent.

Finally, when data controllers provide mechanisms to ensure that the data subject had information and bargaining power to provide a freely given and informed consent, this consent can be considered unequivocal. The unequivocal aspect, therefore, concerns the conclusive behavior of consenting with data processing that the data subject acknowledges and understands.

However, even if data controllers do provide all the material needed to provide a lawful consent, it is difficult to ensure that data subjects did access, analyze, acknowledge, and understand it before consenting. Therefore, controllers must demonstrate that they put forth their best efforts to increase data subjects’ control and improve the quality of their consent.

As mentioned above, once the LGPD is in force, consent will no longer be the sole legal basis to allow data processing. Compliance with legal or regulatory obligations and the controllers’ legitimate interest are two other possibilities that can be explored by companies prior to the data processing.

**Compliance with legal obligations and legitimate interest**

Highly regulated sectors have specific rules that authorize, oblige, or forbid personal data processing. It is important that companies map these rules and identify all the legal obligations they are subject to, because it is a way of dismissing the need for consent in specific situations.

However, data that is collected for the purpose of compliance with legal or regulatory obligations cannot be processed for other purposes (e.g., statistics and marketing), which means that companies can either identify another lawful basis for processing or will need to obtain new consent.

The LGPD also foresees legitimate interest as a hypothesis for data processing “whenever necessary to serve the legitimate interests of the controller or of third parties, except in the event of prevalence of fundamental rights and liberties of the data subject, which requires protection of the personal data.” However, the legitimate interest must be narrowly interpreted and carries several additional obligations.

For example, whenever the treatment is based on the legitimate interest of the controller, only the personal data strictly required for the desired purpose may be processed. Although companies may rely on legitimate interest as a basis for treatment of personal data, it is not possible to ensure how it will be interpreted and enforced once the LGPD comes into effect. Although the wording of the specific section of the law that refers to legitimate interest may be interpreted in a broad way, the entire context and principles of the law may lead to a narrow and more conservative interpretation, so authorities may have different views on this issue.

Below are some examples of regulated sectors and legal obligations that enable data treatment in those scenarios.

**Financial market**

The Brazilian financial market is highly regulated by governmental bodies such as the Brazilian Central Bank (BACEN), the Federal Securities Commission (CVM), and the National Monetary Council (CMN), among others. In addition to the federal laws that regulate bank secrecy, transfer of personal financial data to authorities, and the creation of databases with credit history, the authorities mentioned above also regulate what information must be provided when a client is opening a bank account, for how long this personal data must be stored, and other specific rules for the sector.

In a scenario in which it may be harder to obtain data subject’s consent, financial institutions can rely on legal obligations as a justification to process personal data (provided that the referred processing is limited to the
mandatory rule).

It is also worth noting that Brazilian scholars tend to understand that the monitoring of transactions in order to prevent insider trading, fraud, collusion, market manipulation, and other illicit conduct would be acceptable justification for the legitimate interest treatment.

**Life sciences and healthcare**

Law 13,787/2018 rules on the digitization and use of automatized systems for the storage and handling of medical records. This matter had already been regulated by the Medical Federal Council, which issued Resolution CFM number 1,821/2007 and entered into a covenant with the Brazilian Society of Medical Informatics (SBIS). With the mentioned law in force, the digital copies must contain the exact information of the original digital files (art. 2, §1 of Law 13,787/2018 and Resolution CFM 1,821/2017), and the medical records can be deleted after 20 years of its last update (art. 6 of Law 13,787/2018 and article 8 of Resolution CFM 1.821/2007).

Additionally, Resolution 466/12 has been enacted by Brazilian National Counsel of Health (CNS) and is deemed one of the main regulations on the conduct of clinical research in Brazil and provides for confidentiality and privacy standards for participation of individuals during all stages of clinical research, among other provisions.

Ordinance 1.271/14 from the Ministry of Health establishes the Brazilian National List of Compulsory Notification of diseases, injuries, and public health events in public and private health services throughout the National territory, among other provisions.

These regulations on the healthcare and pharmaceutical sectors need to be analyzed carefully and will need to be interpreted jointly with the new law, especially considering that the LGPD brings stricter standards and conditions for the processing of sensitive personal data. Therefore, this detailed and comprehensive analysis is essential when it comes to personal data related to health.

**Insurance**

The Brazilian insurance system is based on the ordinances and regulations from the Brazilian Superintendence of Private Insurance (SUSEP). The calculation of risks and injuries, definition of awards, the transfer of insurance, and the request for surrender values are all regulated by SUSEP’s rules.

The submission of personal data to SUSEP is an example of a situation that would not need the data subject’s consent depending on the specific regulation—such an act by the data controller would correspond to the compliance with a legal obligation.

**Retail business**

Considering the Brazilian data protection background, it is possible to observe a direct relation to consumer protection. Although the LGPD is not in force, the Brazilian Consumer Defense Code is taken as a relevant law that establishes limits and obligations to companies (suppliers) in many scenarios, such as when collecting its consumers’ information to create databases and registering consumers in positive or negative credit enrollments.

There are also sectorial rules on telemarketing and e-commerce, among others.

Due to the relevance of consumer legislation in data privacy, while the National Data Protection Authority is not created, federal and state consumer authorities have been active in investigating and imposing penalties in relation to data protection matters involving consumers’ personal information.

**Reporting mechanism**
Specifically regarding compliance, the law will certainly affect internal investigations, background checks, and whistleblowing programs. It is a common practice to proceed with background checks on existing and new employees, especially after recognizing that unethical employees may cause data incidents and corruption schemes. Assuming that background checks can operate on a range of levels (from checking a person’s status on social networks to verifying their past criminal activity), it is important to identify the boundaries between legal obligations and breach of employees’ privacy rights.

According to Eduardo Ustaran, whistleblowing programs are relevant to companies because employees are usually the first to observe illegal or improper activities. They can help stop misconduct by reporting such activities to the company’s authorities. With respect to reporting mechanisms, in addition to a non-retaliation policy, companies must also ensure employees are aware of clear and detailed privacy policies.

Therefore, during the data mapping process, companies should also evaluate these procedures to ensure that they comply with the law. In these cases, the main lawful basis used for data processing will probably be framed as either compliance with legal obligation or legitimate interest.

**Conclusion**

The LGPD represents a change in the Brazilian data privacy paradigm and requires an effective organizational transformation in companies. Considering the main steps for compliance with the LGPD, it is possible to:

1. Map and evaluate how data is collected and for what purposes;
2. Analyze and review agreements and procedures in connection with the processing;
3. Adjust internal and external policies; and
4. Engage and involve all the sectors of the company through training, workshops, and awareness to ensure a change in the corporation’s DNA.

The privacy by design and privacy by default techniques should be implemented to ensure personal data protection from the development of services and products by companies.

One cannot ignore the complexity of the Brazilian data protection legal regime and the interconnection of several pieces of legislation when determining the best strategy to adapt the company to this new reality. It is essential to have a multidisciplinary view, because each sector has its own applicable rules, and they must all be covered and respected to assure an actual corporate compliance.

**Acknowledgments**

We thank Maria Eugênia Geve de Moraes Lacerda for her contributions to this article. Maria (melacerda@tozzinifreire.com.br) is a junior associate at TozziniFreire Advogados.

**Takeaways**

- The Brazilian General Data Protection Law (LGPD) is expected to enter into force in August 2020, and it does not replace the current legislation, but supplements it.
- LGPD was inspired by international guidelines, especially the European Union’s General Data Protection Regulation.
- Currently Brazilian data privacy legislation is based on the data subjects’ prior and express consent to data processing.
- When LGPD is in force, compliance with legal or regulatory obligations will be a relevant base for data processing.
processing, especially in highly regulated sectors.

- LGPD represents a change in the Brazilian data privacy paradigm and requires a multidisciplinary view to promote an organizational transformation in companies.

8 Idem.