COSMOS
Navigate the Compliance Universe

CEP Magazine - June 2019
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.[3] Once the data subject is provided with original and unpredictable information[4] that protects from information asymmetry,[5] 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.[6]

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.