KILPATRICK TOWNSEND

January 14, 2019

GDPR-Inspired Data Protection Heads to South America: Brazil's New Data Protection Law Updated to Authorize an Enforcement Authority

by Amanda M. Witt , John M. Brigagliano

On July 10, 2018, the Brazilian Federal Senate approved a General Data Protection Regulation[1] ("Lei Geral de Proteção de Dados" or "LGPD"). The bill, was largely inspired by the European General Data Protection Regulation ("GDPR"). Although several LGPD provisions were vetoed by Brazil's president in August 2018, a December 2018 executive order reinstated many of the vetoed provisions.[2] Most significantly, the executive order reinstated sections establishing an agency tasked with enforcing Brazil's data protection laws. [3]

This post summarizes the key provisions of the bill and addresses its applicability to US-based clients.

Territorial Scope and Definition of Personal Data

In a similar way to the GDPR, the LGPD defines "personal data" as any information relating to an identified or identifiable natural person.[4] Additionally, in order to prevent the use of personal data for discriminatory practices, the LGPD establishes additional restrictions applicable to the processing of sensitive data.[5] Article 5, II defines "sensitive data" as any data pertaining to racial or ethnic origin, religious beliefs, political opinions, membership of syndicates or religious, philosophical or political organizations, data relating to health or sexual life, and genetic or biometric data when linked to a natural person.

The LGPD applies broadly to any data processing operation occurring in Brazil, regardless of the location of the entity conducting the operation or holding the data.[6] Further, the LGPD aims to broadly protect personal data, whether obtained by electronic or physical means, or by the public or private sector.[7]

Under the LGPD, there are situations where anonymized data may be considered to be personal data. Specifically, when the anonymization process to which the data has been submitted is reversible by the use of "reasonable efforts", the data will be deemed personal data and thus subject to the LGPD rules. [8] Similarly, if anonymized data is used for the purposes of establishing behavior profiles, the LGPD will also apply.

Consent and Rights of Data Subjects

Article 7 of the LGPD sets forth a limited number of situations where the processing of personal data is allowed. Notably, the LGPD provides that the collection, use or processing of personal data may be conditioned upon first obtaining the explicit consent of the data subject.

Further, consent must be given in writing, in a clear and separate provision from other contractual provisions, or by "any other means that demonstrate the data subject's consent." [9] The data processor or controller bears the burden of proof of showing that consent was given according to the terms of the LGPD.[10] Additionally, any generic, blanket authorization regarding the use of personal data is expressly prohibited.[11] Similarly, data subjects may revoke their consent at any time, making consent a less reliable basis for processing.[12]

The LGPD confers extended rights upon data subjects.[13] Specifically, pursuant to the LGPD, data subjects have the right to access, rectify, cancel or exclude their data. Further, data subjects may also oppose the processing of their data. The LGPD also sets forth a right to data portability, pursuant to which an individual may request a copy of his or her data in a transferable format. Individuals may then opt to transfer their data to other service providers of their choice.

Legal Bases for Processing and Transfer

Similarly to the GDPR, organizations must identify a specific legal basis for any data processing. As mentioned above, the LGPD provides several legal bases in addition to consent, some of the more significant of which include:

1. Performance of a contract;
2. Fulfillment a legal or regulatory obligation;
3. Fulfillment the controller's legitimate interests, or the legitimate interests of a third party; or
4. For research purposes, but the personal data should be anonymized.[14]

The LGPD also restricts cross border transfers. Companies must ensure that personal data receives adequate protection when transferred. Therefore, data transfers are allowed under a number of circumstances, including if any of the following bases are met, the specifics of which will be further developed by the regulator:

1. transfers to countries offering adequate protection;
2. transfers pursuant to specific contractual clauses for a given transfer; standard contractual clauses; and global corporate rules;
3. where the regulator specifically approves the transfer; or
4. after obtaining the specific consent of the data subject.[15]

Data Protection Officers (DPO)

The LGPD requires companies to appoint a DPO seemingly without exception. The law also mandates that the DPO perform the following duties: accepting complaints and communications from data subjects; providing explanations and adopting measures; receiving communications from the national authority and adopting new measures; training the entity's employees and contractors regarding best practices; and carrying out other duties as determined by the controller or set forth in complementary rules.[16] Unlike in the GDPR, the DPO does not have to be a natural person and can be performed by a third party, which means that the DPO role may be outsourced to a third party legal entity or individual.[17] Therefore, entities such as companies or working groups can fulfill the DPO's responsibilities.

Civil Liability and Administrative Sanctions

Pursuant to the LGPD, the processor and the controller may be held jointly and severally liable for any damage resulting from a violation of the terms of the LGPD.[18] The processor may also be held liable for failure to comply with the controller's clear and legal instructions.

In addition to civil liability, failure to comply with the LGPD may also result in administrative penalties. Article 52 of the LGPD sets forth a number of penalties, which include warnings, fines, suspension or even prohibition of the activity related to the data processing. Fines are calculated based on a company's annual net revenue, and are limited to a total amount of fifty million Brazilian reais (R$ 50,000,000), nearly thirteen million dollars (US$ 13,000,000). It must be noted that the fines are applied separately to each violation, resulting in a significant risk to data controllers and processors in the event of non-compliance.

The National Data Protection Authority

Article 55 of the LGPD establishes the creation of an independent federal agency named Autoridade Nacional de Proteção de Dados ("ANPD"). The ANPD will be responsible for the regulation of all matters related to data protection and for monitoring and enforcing the LGPD. Although initially vetoed by the Brazilian President, the ANPD was reinstated by executive order in December 2018.[19] However, in order to remain effective, that executive order must be converted into law by the Brazilian congress in 2019.[20] The ANPD does not have the power to audit companies, but may request information pursuant to an investigation.[21]

Conclusion

The LGPD will come into effect 24 months following the original publication of the law.[22] Therefore, enforcement is now set to begin in August 2020.23Accordingly, US-based clients with operations in Brazil must plan to comply with the new regulation. Initial compliance steps include:

- Identify to which data the LGPD applies;
- Establish and document legal bases for processing;
- Review data subject rights and establish processes for meeting those rights, including data subject requests;
- Establish and document legal bases for international data transfers; and
- Appoint a data protection officer.

Footnotes

[1] Bill 53/2018 of the Brazilian Congress on the protection of personal data, amending Law No. 12,965 dated 04/23/2014 (LGPD).

[2] Provisional Measure No. 869 of December 27, 2018.

[3] *Id*. at art. 55.

[4] LGPD at art. 5, I.

[5] *Id*. at art. 11.

[6] *Id*. at art. 3.

[7] *Id*.

[8] *Id*. at art. 12.

[9] *Id*. at art. 8.

[10] *Id*. at art. 8, §2.

[11] *Id*. at art. 8, §3.

[12] *Id*. at art. 8, §4.

[13] *Id*. at art. 18.

[14] *Id*. at art. 7.

[15] *Id*. at art. 33.

[16] *Id*. at art. 41.

[17] Measure No. 869 at art. 5 VIII.

[18] *Id*. at art. 42.

[19] Measure No. 869 art. 55.

[20] Renato Leite Monteiro, Changes to Brazil's new data protection law and the establishment of the DPA, IAPP, https://iapp.org/news/a/changes-to-brazils-data-protection-law-and-the-establishment-of-the-dpa/.

[21] Measure No. 869 at art. 29.

[22] LGPD at art. 65.

[23] Measure No. 869 art. 65.