ARTIGO 24.08.2018

BRAZILIAN GENERAL DATA PROTECTION ACT (GDPA) SANCTIONED BY PRESIDENT OF BRAZIL MICHEL TEMER ON AUGUST 14

POR: RAPHAEL DE CUNTO, BEATRIZ LANDI LATERZA FIGUEIREDO,

The act will come into force eighteen months after the date of its publication in the Official Gazette of the Federal Executive, which happened on August 15. This means that the companies must adapt to the new legal requirements by February 2020.

The text originally approved by Congress created a national data protection authority reporting to the Ministry of Justice, but the President of Brazil vetoed the corresponding articles for unconstitutionality in the legislative process (since the creation of public administration bodies is solely incumbent on the Executive). The President is expected to enact a provisional measure or submit a new bill to Congress before the GDPA takes effect.

Privacy has been always protected by the Federal Constitution and several other statutory rules,[1] which have since served as a guidepost to define the practices permissible or not for companies as regards people's data, but the GDPA has now set detailed rules, rights and obligations for these practices.

Adapting to the GDPA, in practice, will be certainly a challenge to companies and will demand efforts and time, the reason why companies should organize themselves reasonably in advance.

How to keep up with the new rules? Here are some steps to become compliant.

The first step to conform with the GDPA is to make a general mapping of each company's personal data collection, processing, storage and erasure practices. Companies actually need to know which data they collect, where they store them, what they do with them, how they protect them, which employees have access to which databases, to be then able to identify which of these practices must be adjusted. It is important, for example, to identify to which countries data would be transferred and for which purpose, since the GDPA has restrictions and obligations related to cross-border transfers. Once the companies identify which are the cross-border transfers made in their operational routines, they will be able to implement the necessary actions to adapt each of them to legal standards.

A second important step will be the internal allocation of responsibilities involving data processing. For larger-sized companies, with a greater volume, relevance and/or sensitivity of operations involving data processing, this can mean the creation of a specific department and budget. In other cases, the duties and costs related to the matter may be assigned to existing departments and/or collaborators. In any case, all companies should designate a person in charge of the data processing practices, who will act as a liaison between the company, data subjects and the national authority, besides being responsible for instructing the company's staff on data processing practices. The identity and contact data of this data protection officer must be publicly disclosed in a clear and objective manner, preferably on the company's website. The national authority may detail in the future the circumstances in which there will be no need to designate a data protection officer.

Other necessary actions will involve the implementation of controlled processes to ensure data subjects' legal rights, such as the rights to access, correction, anonymization, blocking, erasure and portability of their data. To that end, companies will need to put channels and routines in place to inform and satisfy the data subjects' demands. The GDPA sets out that data subjects may exercise their rights upon express request to the companies, and companies will need to implement the necessary tools to receive and meet any such requirements. Moreover, the companies will need to be able to immediately inform the other companies with which they have shared data about any requirements received from the respective data subjects, so that the latter may also implement the requested measures. This means not only that they will need to maintain strict controls over which data are shared with which companies, but also that they will need to stipulate contractual obligations with those companies to ensure that the data subjects' demands can be satisfied.

Contractual obligations with all companies with which data is shared will be key to set limits on their use. The GDPA recognizes that a violation of data subject rights in the context of consumer relations remains subject to liability rules sets out in the relevant law, which could mean that companies should be considered jointly and

liability rules sets out in the relevant law, which could mean that companies should be considered jointly and severally liable for damage caused to consumers. The revision and any necessary amendment to agreements with companies with which there is data sharing is recommended.

Companies will also need to run processes to obtain and check parental consent when dealing with children and teenagers data.

When adapting to the GDPA, companies will need to ensure the adoption of technical and administrative security measures to protect personal data from unauthorized access and from accidental or unlawful events of destruction, loss, change, communication or any form of unlawful or improper processing. A company that fails to adopt the security measures prescribed by law or the minimum standards later established by the national authority will be held liable for the damage arising from security incidents. Companies should also implement security incident response procedures. Under the GDPA incidents that may cause significant risk or damage to data subjects should be informed both to the national authority and to the data subjects.

Finally, according to the GDPA, companies may formulate good practice and governance rules (such as privacy governance programs); these rules are not mandatory, but their existence will be taken into account as a mitigating circumstance if administrative sanctions are imposed. These rules can include organization conditions, procedures, technical standards, obligations for several processing players, educational actions, and internal mechanisms to monitor and mitigate risks, among others.

Besides adopting several practices, as those mentioned above, companies will need to produce a series of documents, such as:

- Privacy policy: companies should provide data subjects with clear, complete and straightforward information on the collected data, the form and duration of processing and the respective specific purposes, as well as on its sharing with third parties, responsibilities of the company and of third parties and data subjects' rights, among others. Changes in the data processing purpose should be informed, and data cannot be processed for purposes other than those informed.

- Informed consent for processing of data on employees and job applicants: like the privacy policy, it should contain clear, complete and straightforward information on the data collection and processing in this context.

- Internal codes and manuals related to data processing practices and routines, including policies on retention and erasure of data, data access policies, among others.

- Agreements with data operators.

- Standard contractual clauses applying to companies with which the company shares data.

- Documents supporting cross-border transfers to countries that do not attribute an adequate degree of protection to personal data.

- Data protection impact assessment report: a document that may be requested by the national authority describing personal data processing activities that may pose risks to data subjects, as well as measures, safeguards and mechanisms adopted to mitigate such risks.