
PUBLICATIONS

ALERT 05.30.2018

HOUSE OF REPRESENTATIVES GIVES GREEN LIGHT TO THE BRAZILIAN GENERAL DATA PROTECTION ACT

BY:

RAPHAEL DE CUNTO, LARISSA MARIA GALIMBERTI AFONSO, ANDRÉ ZONARO GIACCHETTA, CIRO TORRES FREITAS,
JOSÉ MAURO DECOUSSAU MACHADO,

In plenary session held on May 29, 2018, the House of Representatives gave its green light to Bill No. 4,060 of 2012 (Bill), which sets out the Brazilian General Data Protection Act (Act).

Congressional efforts have gained momentum in the wake of the EU General Data Protection Regulation (GDPR), which became enforceable on May 25. This thumbs-up given by the House of Representatives is an important step to a more robust regulation on use of personal data in Brazil by way of a general law on the matter, as it already happens in over 100 countries.

Below are some highlights of the Bill as approved:

- Scope of application

The Act is to apply to the processing of personal data by individuals and private or public legal entities, no matter the country where these are headquartered or where the data will be hosted, provided that such processing (i) takes place within the Brazilian territory, or (ii) is intended to offer or provide goods or services within the Brazilian territory, or else (iii) the personal data in point have been collected from data subjects located in Brazil at the time of such collection. However, the Act will not apply if the data originate from a country offering the same level of protection envisaged in the Act and are not intended for disclosure; for sharing with Brazilian processing agents; or for cross-border transfer to a third country. Processing of personal data solely for journalistic, artistic, academic, public security, national defense and security, criminal investigation and law enforcement purposes is also excluded. Data processing by individuals solely for personal purposes is not subject to the Act either.

- Rights of data subjects

Data subjects will have the right to obtain from the person responsible for processing (the 'controller'), at any time and upon request, (i) a confirmation as to the existence of personal data processing; (ii) access to his or her own personal data; (iii) correction of incomplete, inaccurate or outdated data; (iv) anonymization, blocking or removal of unnecessary, excessive or noncompliant data; (v) portability of such personal data to another service or product vendor; (vi) receipt of information on third parties with which his or her data have been shared; (vii) cancellation of his or her consent; and (viii) the data subject's review of unfavorable decisions that have solely relied on automated processing of his or her personal data.

- Processing requirements

Processing of personal data will only be possible (i) upon the data subject's written consent or by any other means expressly stating his or her informed consent; (ii) for enforcement of statutory or regulatory requirements by the controller; (iii) if necessary for closing of a contract or transaction to which the data subject is a party, at the latter's request; (iv) for ordinary exercise of rights in a court, administrative or arbitration proceeding; (v) to protect the life or physical integrity of the data subject or others; (vi) for attainment of healthcare objectives by healthcare professionals or public health entities; (vii) when so required to meet the lawful interests of the data subject or others; (viii) for credit protection purposes; (ix) for the conduction of studies by research bodies; or (x) by the public administration to the extent required for enforcement of public policies.

- Cross-border transfer

Transfer of personal data to third countries may occur, among others: (i) to third countries or international organizations that accord adequate protection to personal data vis-à-vis the levels established in the Act; (ii) when the controller can offer and ensure that safeguards are in place in terms of observance of the principles, data subject rights and protection systems prescribed in the Act; (iii) when such transfer is necessary for international legal cooperation among government bodies; (iv) when the competent body authorizes such transfer; (v) upon specific consent from the data subject based on prior, conspicuous disclosure of the cross-border status of the intended transfer, clearing distinguishing the latter from other purposes.

- Civil liability and penalties

The Bill lays down the liability of data processing agents (controller and processor) for ensuing damage, on very similar terms to those of the Brazilian Consumer Protection Code. The Bill even provides for exoneration from civil liability of controllers and processors – when the data subject or a third person are solely to blame for the damage, among other events. Besides, the following administrative

sanctions are imputable to collectors and processors for breach of any provisions in the Act: (i) warning; (ii) a fine capped at R\$ 50 million per offense; (iii) disclosure of the offense; (iv) blocking of personal data; (v) erasure of personal data; (vi) suspension of database operations; (vii) suspension of personal data processing activities; and (viii) prohibition against engaging in personal data processing activities.

- Supervisory authority

The National Data Protection Authority will be tasked with exercising a supervisory and enforcement role as an entity of the indirect federal public administration (acting as a special independent government entity reporting to the Brazilian Ministry of Justice).

- Reporting requirement

The Bill introduces in the Brazilian legal system the duty of informing the competent authority and personal data subject about any security incidents that may pose significant risks or damage to the latter. This reporting must be made by the controller within a reasonable period (to be defined by the competent authority) and contain (i) a description of the type of personal data then affected; (ii) information on the data subjects involved; (iii) an indication of the technical and security measures adopted for data protection purposes; (iv) the risks underlying the incident; (v) the reasons for delay (unless the reporting is promptly made); and (vi) the past and future measures to reverse or mitigate the effects of any such incident.

The Bill has clearly drawn on the GDPR, but has some specific characteristics that may translate into hurdles to the transfers of personal data between Brazil and the UE. Under the Bill, for instance, no consent is required for processing of any personal data that are manifestly made public by the data subject – which differs from the EU rule (where this waiver is not contemplated at such an extent).

Some provisions of the Bill, if eventually passed into law, will represent a real challenge to those involved in personal data processing. For instance, the Bill establishes that a child's personal data can only be processed upon clear, specific consent given by one of the child's parents or by the holder of parental responsibility over the child; the processor will be required to endeavor all efforts necessary to make sure that such condition has been satisfied, taking into consideration available technology.

As yet another aspect worthy of note, there is a potential risk of conflict between the Act and other statutory provisions in Brazil. The Bill has not adequately addressed the provisions in the Civil Rights Framework for the Internet (Law No. 12,965 of 2014), which lays down the conditions for processing of personal data from internet service users. This will undoubtedly cast doubt on whether personal data from internet users can be processed without their consent under the other circumstances envisaged in the Act (for instance, to meet lawful interests of the processor, or to protect the life and physical integrity of the data subject or others).

The Bill will soon be sent over to the Federal Senate, where Bill No. 330 of 2013 dealing with this same matter is already underway. Both bills are likely to be consolidated and then move forward jointly, when adjustments could be made so that the future Act may serve as an effective tool to improve the protection of data subjects and their personal data, without posing any unwanted obstacles to the economic activities of processing industry players or to innovation.