DATA PROTECTION LAW OF PANAMA

Mauricio Paris
Partner @ECIJA

On March 26, 2019, the National Assembly of Panama, through Law No. 81, approved the much-awaited Data Protection Law, which was published in the official daily on Friday, March 29, 2019. Despite the long wait, the law won't take effect until March 26, 2021, two years after its promulgation.

In this case, like all regulations on data protection in Latin America, Panama was noticeably influenced by the European regulatory model, with the peculiarity that, having been approved after the approval in 2016 of the **General Data Protection Regulation (GDPR)**, it includes several of its innovations.

Regarding the **scope of the law's application**, it will apply to databases that are 1) located in Panamanian territory and store or contain personal data of nationals or foreigners and 2) are administered by a person domiciled in Panama.

It is an evident omission that the Panamanian law does not apply to personal data processing done within Panamanian territory by a person not domiciled in Panama, such as a database like "the cloud," which is located outside of Panamanian territory.

Article 3 establishes five cases in which the law will not be applied, some of which are also included in Article 2 of the GDPR. For example, the law does not apply to the processing of personal data by individuals for personal or domestic purposes. However, it is noticeable that processing for *financial intelligence analysis* is excluded from the scope of application. It is astonishing that Panama, a country with highly developed financial services, would allow the exclusion of a considerable amount of personal data processing from the protection standards that this legislation intends to guarantee, particularly given the indeterminate and broad nature of the concept of financial intelligence.

Article 6 of the law regulates the legal bases that legitimize the processing of personal data:
1) Consent,
2) Performance of a contractual obligation,
3) Fulfillment of a legal obligation,
4) Processing authorized by law or regulations that develop them.

This legislation follows the standards of the GDPR and is important because it is a significant paradigm shift from processing based solely on consent. It also includes - although in article 8 - other processing bases contemplated in the GDPR, such as processing to protect vital interests (medical or health emergency) or the legitimate interest, after considering the interests involved.

The new law recognizes **ARCO Rights**, already recognized in the majority of data protection regulations. It concerns access, rectification, cancellation (now called erasure in the GDPR), and opposition, which are guaranteed and granted inalienable character. The **right to data portability** is also regulated and is also new to the GDPR.

The law includes the right of the data subject not to be subjected to a decision based solely on **automated processing**, similar to that contained in Recital 71 and Article 22 of the GDPR. This right is intended to ensure that people are not subjected to decisions based solely on the automated processing of their personal data, which produces negative legal effects. This is, for example, common in the practice of profiling consumers.

The law also requires, although unclearly, those responsible for and custodians of databases to keep **records of processing activities**. They must record all transfers of personal data to third parties (Article 31). This record of processing activities (which is not limited to transfers of personal data) is a novelty of the GDPR that left in effect the obligation established by Directive 95/46 to communicate to the corresponding authorities the existence of databases, an obligation that continues in Costa Rican legislation, for example, a clear influence of Spanish legislation from before the approval of the GDPR.

One area where the Panamanian legislation seems unnecessarily complicated, as a result of a conceptual error, relates to the **processor of personal data**. The person in charge of personal data, who performs the processing of such data on behalf of the data controller, is not regulated, whether individual or legal entity (even a public entity). A controller-processor relationship very frequently exists in service contracts; hence adequate regulation of it is essential for any law.

Notwithstanding the foregoing, Panamanian law defines the **custodian of the database**, denoting it as an individual or legal entity, public or private, lucrative or not, who acts on behalf of the data controller and is responsible for the custody and conservation of the database. This definition is limited to two operations of processing, custody and conservation, and the person in charge can perform not only this processing but others such as gathering, enquiries, removal, corrections, etc.

Article 10 regulates the so-called **processing of personal data by mandate**, stipulating that the agent must respect the conditions of the legal mandate in fulfillment of the command. The question remains, under Panamanian law, as to whether the assignment of the processing of personal data should then be structured as a mandate contract or a service agreement, although Article 14 itself speaks of the duty of care of the agent "by order or mandate" of the person in charge.

The regulatory authority that will assume the supervision of personal data processing is the already-existing National Authority of Transparency and Access to Information (ANTAI, according to its initials in Spanish). The aforementioned authority has functional independence, by resolving all complaints filed until its last resource. The law also contemplates the creation of a Council for the Protection of Personal Data, which will perform an advisory function to ANTAI and also prepare public policies.

The Panamanian legislation undoubtedly did not follow the GDPR in terms of fixing the fines derived from breach of its provisions. While in Europe these fines can reach twenty million euros, or 4% of the annual income of a company, in Panama **the maximum fine is ten thousand balboas** (equivalent to the US dollar).

Although the economic realities in Panama and the European Union are significant, such low fines discourage compliance, as has happened in Costa Rica, where it is cheaper for many companies to include in their budgets the cost of paying fines rather than take all the necessary measures to comply with the law.

Regarding degree of infractions, the law provides a list: minor error, serious error and very serious error. Also, those responsible for the processing of personal data who violate the law will have to compensate victims for any **pecuniary losses and/or moral damages** caused

by the improper processing of personal data, enforceable through court action. The current legislation does not limit such compensation to the owner of the personal data.

In Central America, legislation regarding data protection is still pending in Guatemala, El Salvador and Honduras.