/Carey

August 12, 2024

LEGAL ALERT

Legitimization of databases prior to the entry into force of the new data protection law

One of the structural principles of the new data protection law is the principle of lawfulness and fairness, which requires that all processing has an appropriate legal basis. Those responsible for managing databases that have been organized prior to the entry into force of the new Data Protection Law will face a great challenge: the adaptation of their databases to the new regulation, which will clearly mean a race against time.

What is meant by a database

The new Personal Data Protection Law defines "**personal databases**" as an organized set of personal data, whatever the purpose, form or modality of their creation, storage, organization and access, which allows the data to be related to each other, as well as to carry out their processing.

This means that, whether the data is in an elaborate spreadsheet or in a simple notebook, if it allows data to be related and processed, they are considered databases.

The new law will apply, in general, to all processing of personal data carried out by a natural or legal person, including the collection and storage of personal data in databases.

Challenge for controllers: adapting their databases to new requirements

One of the structural principles of the new Personal Data Protection Law is that of lawfulness and fairness. This implies that each data processing must have an appropriate legal basis.

This poses a significant challenge for data controllers who manage databases whose collection and processing began prior to the entry into force of the new law.

In short, it will be necessary for those controllers to seriously evaluate

whether their databases have an adequate and relevant legal basis that allows them to continue processing data on these databases.

For example, in those cases in which data controllers carry out data processing under the legal basis of consent, they must reevaluate whether such consent granted under the standard of prior legislation complies with the new requirements of the new Data Protection Law, which imposes ostensibly higher conditions. Thus, in many cases it could be concluded that these databases do not have the corresponding legal basis, and a new legal basis is necessary to continue with the processing.

How much time will data controllers have to identify an appropriate legal basis for their database?

The bill presented in 2017 contained a transitory article that established a period of forty-eight months for existing databases to adapt to the terms of the new law. However, this article was discarded, not prospering in the final proposal of the new law.

As a result, data controllers must have their databases regularized when the law comes into force. It is important to note that the new law contemplates a vacancy period of 24 months from its publication in the Official Gazette. Although this period is not short, similar experiences show that in some cases it may not be a long time, so the call is to carry out these evaluations of the databases as soon as possible.

What legal basis are there?

The new Data Protection Law establishes that consent is the general rule for lawful data processing. However, it also considers the processing of personal data without the consent of the owner to be lawful in certain cases, such as in the execution of a contract, compliance with a legal obligation, the satisfaction of legitimate interests, among others.

If the data controller is unable to link its processing with one of the other legal basis, it will face the challenge of requesting the consent of each of the data subjects in its database, considering that the consent must meet certain requirements: be prior to processing, express, free, specific in terms of purposes, informed and unequivocal.

What happens if the controller does not adapt a database to any of the legal basis established in the law?

The controller is exposed to a serious penalty, whose fine could amount to up to UTM 10,000 (USD 705,000 app.).

In the event of a recidivism, the Personal Data Protection Agency could apply fines of up to UTM 30,000 (USD 2,114,470 app.), or up to the amount corresponding to 2% of the annual income from sales and services and other activities of the line of business in the last calendar year.

While adapting databases in a short window of time is a major challenge, it is also an opportunity to improve data handling practices and ensure the protection of individuals in relation to their personal data.

Authors: José Ignacio Mercado; Iván Meleda; Gabriela García