ECIJA

Torre Mural. Av. Insurgentes Sur 1605 piso 10
Col. San José Insurgentes, C.P. 03900,
Ciudad de México, México
Tel: (+52) 5556626840
www.ecija.com

Legal memo

Mexico City, Mexico, December 7, 2022

5 Principles for a Data Privacy Compliance Program

The regulations on personal data protection establish a series of complex obligations to be observed by companies that process personal data.

Fines imposed in 2021 by the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) for violations of personal data protection legislation exceeded 90 million pesos (Approx. US$45 million).

The regulations on personal data protection establish a series of complex obligations that must be observed by companies that process personal data within the framework of their operations. Each of these obligations entails a series of activities that are easy to overlook when the company is unaware of the relevance, scope, and consequences of the issue.

In terms of Article 28 of the Regulations of the Federal Law for the Protection of Personal Data in Possession of Individuals, companies must adopt measures to guarantee the proper treatment of personal data, giving priority to the interests and reasonable expectations of privacy of the owners.

Among the measures contemplated in the legislation is the development of mandatory and enforceable privacy policies and programs within the organization of the companies. These policies and programs are a set of guidelines issued by companies to promote, monitor, and ensure compliance with applicable legislation. Therefore, allowing them to mitigate situations that could expose them to some type of risk or liability, as well as to demonstrate due diligence in the development of their functions.

In our experience, to ensure the correct design, implementation and operation of a privacy and personal data protection compliance program, the following steps should be followed:

1. Directory of data processing. It is essential to evaluate the different processes of the company to identify the processing of the personal data it carries out (profiles of owners, data processed, purposes of processing, transfers, among others).

2. Diagnosis of compliance. It is necessary to identify the existing compliance mechanisms or those that still need to be implemented to comply with the principles and duties established in the regulations (information, consent, purpose, proportionality, responsibility, loyalty, and quality).

3. Design of compliance program. Compliance mechanisms must be suitable and in line with the company's operations (privacy notices, cookie policies, mechanisms for obtaining consent, catalog of functions and obligations of personnel, clauses or agreements with clients and suppliers involved in the processing of personal data, among others).

4. Implementation of compliance program. It is necessary to carry out awareness and training actions for personnel involved in the processing of personal data, to ensure the proper implementation and compliance with the program (e.g., officer, delegate, or committee for the protection of personal data).

5. Periodic reviews. The program should be evaluated periodically to measure its level of compliance, as well as to identify any updates that may be necessary due to legislative or operational changes in the company (internal or external audits).

In this way it is possible to close possible non-compliance gaps that could expose companies to fines of up to 320,000 times the value of the Unidad de Medida y Actualización (approximately $30 million pesos, approx. US$1.5M), which could be increased by an equal amount in cases of repetition and doubled in the case of violations involving the processing of sensitive data.

TMT and Compliance Area of ECIJA Mexico
Socios.mexico@ecija.com