MEXICO DATA PROTECTION LAW

As of 2009 protection of personal data is recognized in the Mexican Constitution as a fundamental right. While some legal protection existed previously for personal data in the possession of the federal government, it wasn't until the enactment of the Federal Personal Data Protection Law (*Ley Federal de Protección de Datos Personales*) (the "Data Protection Law") on July 5, 2010 that there was a law regulating the use of personal data in the hands of private parties. The Data Protection Law applies primarily to companies located in Mexico, but in some cases also applies to non-Mexican companies doing business with its employees, customers, and suppliers in Mexico.

WHAT IS REGULATED?

The Data Protection Law regulates the processing and use of "personal data," which is defined by the law as any information concerning an identified or identifiable individual. Among the regulation of "personal data" there is a subset of stricter regulations regarding "sensitive personal data," which encompass data that may reveal (i) racial or ethnic origin; (ii) medical information; (iii) genetic information; (iv) religious, philosophical, and moral beliefs; (v) union membership; (vi) political views; and (vii) sexual preference.

The processing of personal data includes the retrieval, use, disclosure, or storage of personal data by any means. The use of personal data includes any action related to its access, management, commercial use, transfer, or disposal.

The Data Protection Law applies to all private parties that use or process personal data in Mexico, with certain exceptions (*e.g.*, non-commercial personal use).

HOW IS IT REGULATED?

Obligations are imposed on private parties to ensure the personal data is processed and used properly. The Data Protection Law is enforced by the Federal Institute for Access to Public Information and Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) ("INAI").

The processing and use of personal data is subject to certain basic principles set out in the Data Protection Law:

- Legality: Personal data must be gathered, processed, and used lawfully.
- Consent: Consent from the individual must be obtained, either express or implied.

- Information: Individuals must be informed of the terms of how their personal data will be used and processed by means of a privacy notice.
- Finality: Information must be used only for its intended purpose and destroyed once the purpose of its collection and processing has been achieved.
- Loyalty: Gathering of personal data must not be done through deceptive or fraudulent means.
- Proportionality: Only request information that is appropriate and necessary to accomplish the purpose indicated in the privacy notice.
- Responsibility: Ensure that the principles established in the law are fulfilled by adopting all necessary measures.

Generally, consent is implied by making available to the individual the applicable privacy notice. However, for sensitive and financial information an express consent is required in writing.

Databases containing sensitive information cannot be created unless their creation can be justified by purposes that are legitimate, concrete, and consistent with the explicit objectives or activities pursued by the data controller. When processing sensitive data, the data controller must make reasonable efforts to keep the processing period to a minimum.

RIGHTS OF THE INDIVIDUAL

When personal data is to be collected, individuals must be provided with a privacy notice that must contain at minimum the following information:

- The identity and address of the data controller.
- The purposes of the processing of the personal data.
- The available options and resources that the data controller can offer to the individual to limit the use or the dissemination of the personal data.
- Details of any transfers of personal data that have been carried out (if applicable).
- The procedure and resources through which the data controller can communicate to the individual any changes in the privacy notice.

The individuals would then have the right to access, correct, oppose the processing or use of, and cancel/delete their personal data, except as otherwise established by law.

DATA PROTECTION SAFEGUARDS

Data controllers must establish and maintain administrative, technical, and physical security measures that allow personal data to be protected from damage, loss, alteration, destruction, or unauthorized use, access, or treatment. Additionally, the Data Protection Law establishes that data controllers must not adopt security measures with respect to personal data of third parties that are less secure than the measures adopted to conserve or protect their own information.

The data controller must immediately inform the data subject if a breach or violation of security has occurred that could affect the moral and economic rights of the individual affected.

THIRD-PARTY PROCESSING

Personal data can be processed by a third party at the request of the data controller upon the execution of an agreement between the parties. The third party must then:

- Follow the instructions provided by the data controller for its processing.
- Refrain from using the personal data for purposes different from those instructed by the data controller.
- Implement security measures as per applicable laws.
- Maintain confidentiality regarding the processed personal data.
- Destroy the personal data when the relationship with the data controller is finalized, or as requested by the data controller (unless there is a legal provision requiring its conservation).
- Refrain from transferring the personal data, unless instructed to do so by the data controller.

SANCTIONS

Non-compliance with the provisions of the Data Protection Law can be sanctioned by the INAI. The sanctions range from warnings instructing the data controller to carry out the actions requested by the data subject (in relation to the data subject's right of access, correction, cancellation, and opposition), to fines equal to 100 to 320,000 days of the minimum wage[1] applicable in Mexico City for each instance of breach. If the data controller has committed the same offense previously, an additional fine is imposed. For violations committed when processing sensitive personal data, the sanctions can be doubled.

[1] On January 27, 2016, Mexico's Congress published an amendment to Mexico's Federal Constitution which included the creation of a new reference unit to replace the minimum wage, called UMA, for *Unidad de Medida y Actualización* which is currently in effect, notwithstanding that certain laws have not been amended to include the mention of this new reference unit. The initial value for the UMA was set to the then in effect minimum wage applicable to all of Mexico, which was $73.04 Mexican Pesos. At this value and current exchange rates, the maximum fine is approximately US $2.6 million per breach.

The Data Protection Law also provides for criminal sanctions in certain scenarios:

- Up to a three-year jail sentence when data controllers cause a security breach with the aim of obtaining an economic benefit.
- Up to a five-year jail sentence for fraudulently processing personal data.
- When dealing with sensitive personal data, the abovementioned criminal sanctions are doubled.

Civil claims can be initiated by the data subject if the data controller's violation has caused damage to him. However, the data subject is required to obtain a final administrative decision by the INAI before the civil claim can commence.

RECOMMENDATIONS

Companies subject to the Data Protection Law should take the following steps:

- Identify aspects of your business that might be subject to the law.
- Adopt or revise privacy policies, implement supervisory systems, and train personnel about compliance with the Data Protection Law.
- Review third-party agreements with regard to data protection issues and responsibility for compliance with the law.

If you have additional questions, please do not hesitate to contact the Thompson & Knight attorney with whom you regularly work or one of the attorneys listed below.

CONTACTS:

Alejandro A. Sánchez-Mújica A.
+52.81.8215.7729
Alejandro.SanchezMujica@tklaw.com

Michael C. Titens
+1.214.969.1437
Michael.Titens@tklaw.com