MEXICO

LAW


The Executive Branch has also issued:

- The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (the Regulations), which entered into force on December 22, 2011
- The Privacy Notice Guidelines (the Guidelines), which entered into force on April 18, 2013
- The Recommendations on Personal Data Security, on November 30, 2013
- The Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014
- The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados), which entered into force on January 27, 2017


The Regulations apply to all personal data processing when:

- Processed in a facility of the data controller located in Mexican territory
- Processed by a data processor, regardless of its location, if the processing is performed on behalf of a Mexican data controller
- Where the Mexican legislation is applicable as a consequence of Mexico’s adherence to an international convention or the execution of a contract (even where the data controller is not located in Mexico), or
- Where the data controller is not located in Mexican territory, but uses means located in Mexico to process personal data, unless such means are used only for transit purposes

The Law only applies to private individuals or legal entities that process personal data, and not to the government, credit reporting companies governed by the Law Regulating Credit Reporting Companies or persons carrying out the collection and storage of personal data exclusively for personal use where it is not disclosed for commercial use.

DEFINITIONS

Definition of personal data

‘Personal Data’ is any information concerning an identified or identifiable individual.
Definition of sensitive personal data

'Sensitive Personal Data' is personal data that affects the most intimate areas of the data subject’s life, which if misused, may lead to discrimination or entail a serious risk to the data subject. In particular, the definition includes data that may reveal any of the following:

- Racial or ethnic origin
- Past or present health conditions
- Genetic information
- Religious, philosophical or moral beliefs
- Union affiliation
- Political views
- Sexual orientation
- Pictures and videos
- Fingerprints
- Geolocation
- Banking information
- Signature

NATIONAL DATA PROTECTION AUTHORITY

The National Institute of Transparency for Access to Information and Personal Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) (INAI) and the Ministry of Economy (Secretaría de Economía) serve as Mexico’s data protection authorities.

REGISTRATION

Mexican law does not require registration with a data protection authority or other regulator in relation to the use of personal data.

DATA PROTECTION OFFICERS

All data controllers are required to designate a personal data officer or department (each, a Data Protection Officer) to handle requests from data subjects exercising their ARCO Rights (as defined in ‘Collection and Processing’) under the Law. Data Protection Officers are also responsible for enhancing the protection of personal data within their organizations.

COLLECTION & PROCESSING

The term 'processing' is broadly defined to include the collection, use, communication or storage of personal data by any means. Use includes all access, management, procurement, transfer and disposal of personal data.

In processing personal data, data controllers must observe the principles of legality, information, consent, notice, quality, purpose, loyalty, proportionality and accountability.

Personal data must be:
- Collected and processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed
- Accurate and, if necessary, updated; every reasonable step must be taken to ensure that data that is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified, and
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed

Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data. In addition, personal data must be processed as agreed upon by the parties (in a privacy notice or otherwise) and in compliance with the Law.

To legally process personal data, data controllers must provide a privacy notice (Aviso de Privacidad) (the Privacy Notice), which must be made available to a data subject prior to the processing of his or her personal data. The Privacy Notice may be provided to data subjects in printed, digital, visual or audio formats, or any other technology.

A comprehensive Privacy Notice must at least contain:

- The identity and domicile of the data controller collecting the data
- The purposes of the data processing
- The options and means offered by the data controller to data subjects to limit the use or disclosure of their data
- The means for exercising rights of access, rectification, cancellation or objection (ARCO rights) in accordance with the provisions of the Law
- Where appropriate, the types of data transfers to be made
- The procedure and means by which the data controller will notify the data subjects of changes to the Privacy Notice, and
- Identification of any sensitive personal data that will be processed

The Guidelines permit the following three forms of privacy notice: comprehensive, simplified and short form, depending on whether the personal data is obtained directly or indirectly from the data subject, and the context and space in which the personal data is collected. Each of these forms must meet specific disclosure requirements.

The data controller has the burden of proof to show that the Privacy Notice was provided to the data subject prior to the processing of his or her personal data.

Some form of consent is required for all processing of personal data, except as otherwise provided by the Law. Implicit consent (notice and opt-out) applies to the processing of personal data generally; express consent (notice and opt-in) applies to the processing of financial or asset data; and express and written consent applies to the processing of sensitive personal data. Consent may be communicated verbally, in writing, or via any technology, or by any other unmistakable indication. Express written consent may be obtained through the data subject’s written signature, electronic signature, or any other authentication mechanism.

Consent from the data subject will not be required for the processing of personal data in any of the following apply:

- Any law so provides
- The data is contained in publicly available sources
- The identity of the data subject has been disassociated from the data
- Processing has the purpose of fulfilling obligations under a legal relationship between the data subject and the data controller
- There is an emergency situation that could potentially harm an individual with regard to his or her person or property
- Processing is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data subject is unable to give consent in the manner established by the General Health
Data Protection Laws of the World

Mexico

Law (Ley General de Salud) and other applicable laws, and said processing is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or

- Pursuant to a resolution issued by a competent authority

TRANSFER

Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide the third parties with the Privacy Notice provided to the data subject and the purposes to which the data subject has limited the data processing.

Data processing must be consistent with what was agreed in the Privacy Notice, which shall contain a clause indicating whether or not the data subject agrees to the transfer of his or her data. The third party recipient assumes the same obligations as the data controller who has transferred the data.

Domestic or international transfers of personal data may be carried out without the consent of the data subject where the transfer is:

- Pursuant to a law or treaty to which Mexico is party
- Necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management
- Made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies as the data controller
- Necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject
- Necessary or legally required to safeguard public interest or for the administration of justice
- Necessary for the recognition, exercise or defense of a right in a judicial proceeding, or
- Necessary to maintain or comply with an obligation resulting from a legal relationship between the data controller and the data subject.

The Regulations establish that communications or transmissions of personal data to data processors do not need to be informed nor consented by the data subject. However, the data processor must do all of the following:

- Process personal data only according to the instructions of the data controller
- Not process personal data for a purpose other than as instructed by the data controller
- Implement the security measures required by the Law, the Regulations and other applicable laws and regulations
- Maintain the confidentiality of the personal data subject to processing
- Delete personal data that were processed after the legal relationship with the data controller ends or when instructed by the data controller, unless there is a legal requirement for the preservation of the personal data
- Not transfer personal data unless instructed by the data controller, the communication arises from subcontracting, or if so required by a competent authority

SECURITY

All data controllers must establish and maintain physical, technical and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. They may not adopt security
measures that are inferior to those they have in place to manage their own information.

The risk involved, potential consequences for the data subjects, sensitivity of the data and technological development must be taken into account when establishing security measures.

**BREACH NOTIFICATION**

Security breaches occurring at any stage of the processing that materially affect the property or moral rights of the data subject must be promptly reported by the data controller to the data subject.

The Regulations provide that breach notification must include at least the following information:

- The nature of the breach
- The personal data compromised
- Recommendations to the data subject concerning measures that he or she can adopt to protect his or her interests
- Corrective actions implemented immediately, and
- The means by which the data subject may obtain more information in regard to the data breach

**ENFORCEMENT**

Data subjects can enforce their ARCO Rights, when no response is obtained from the data controller via INAI and ultimately the court system.

If any breach of the Law or its Regulations is alleged, INAI may perform an on-site inspection at the data controller’s facilities to verify compliance with the Law.

Violations of the Law may result in monetary penalties or imprisonment, including the following:

- INAI may impose monetary sanctions in the range of 100 to 320,000 times the Mexico City minimum wage (currently, MX$88.36, updated every year). Sanctions may be increased up to double the above amounts for violations involving sensitive personal data.
- Three months to three years of imprisonment may be imposed on any person authorized to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties will be doubled if sensitive personal data is involved.
- Six months to five years of imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorized to process such data. Penalties will be doubled if sensitive personal data is involved.

**ELECTRONIC MARKETING**

Email marketing constitutes personal data processing and is subject to the Law, including applicable notice and consent requirements.

**ONLINE PRIVACY**

The Regulations and Guidelines that address the use of cookies, web beacons and other analogous technologies, require that when a data controller uses online tracking mechanisms that permit the automatic collection of personal data, it provides prominent notice of the use of such technologies; the fact that personal data is being collected the type of personal data collected and the purpose of the collection and the options to disable such technologies.

An IP address alone may be considered personal data, however, there has not been a resolution or decision issued by the
compeénént authority on this point.

**KEY CONTACTS**

**Gabriela Alaña**  
Partner  
T + 52 55 5261.1817  
gabriela.alana@dlapiper.com

**Ana Kuri**  
Associate  
T + 52 55 5261.1847  
ana.kuri@dlapiper.com

**Paola Aguilar**  
Law Clerk  
T +1 555.261.1818  
maria.aguilar@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization’s level of data protection maturity.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.