DATA PROTECTION LAWS OF THE WORLD

Mexico

MEXICO

Last modified 28 January 2024

LAW

The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) ("the Law") entered into force on July 6, 2010.

Subsequently, the Executive Branch has also issued the following (collectively, with the Law, referred to herein as "Mexican Privacy Laws"):

- 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 Protecció n de Datos Personales en Posesión de Sujetos Obligados), which entered into force on January 27, 2017

On June 12, 2018, a decree was published in the Official Gazette of the Federation approving two important documents:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dated January 28, 1981, and its
- Additional Protocol regarding supervisory authorities and trans-border data flows dated November 8, 2001.

Mexican Privacy Laws apply to all personal data processing under any of the following circumstances:

- Processing carried out by a data controller established in Mexican territory
- Processing carried out by a data processor, regardless of its location, if the processing is performed on behalf of a data controller established in Mexico
- Processing by or on behalf of a data controller not located in Mexico, where Mexican legislation is applicable pursuant to the execution of an agreement or Mexico’s adherence to an international convention or
- Processing carried out within Mexican territory, on behalf of a data controller not established in Mexican territory, unless such processing is 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. Further, Mexican Privacy Law also does not generally apply to business-to-business data, including:

- Data of legal entities.

- Data of individuals acting as merchants or professionals.
- Data of natural persons acting on behalf of a business (e.g., their employer), where the personal data processed is (a) limited to first and last names, title, position and functions performed, and business contact data, such as mailing or physical address, email address, telephone number and fax number, and (b) the personal data is processed solely for the purpose of representing the business or administering the business relationship (i.e., fulfilling orders, providing services, carrying out transactions between the business entities)

Additionally, the INAI has issued several documents and guidelines for the private sector regarding the processing of personal data, including the following:

- 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
- Recommendations for the Designation of the Data Protection Officer or the Data Protection Department
- Guideline to Implement Compensatory Measures
- Guideline for the orientation of the due processing of personal data in the activity of extrajudicial collection
- Guideline for the Secure Deletion of Personal Data
- Suggested minimum criteria for contracting cloud computing services that involve the processing of personal data
- Guideline for the Processing of Biometric Data.

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

Other key definitions

'ARCO Rights' refer to the access, ratification, cancelation and opposition rights of data subjects, with respect to their personal data.

'Controller' or 'data controller' means the individual or private entity makes decisions regarding the processing of personal data.

'Data subject' means the individual to which the personal data belongs.

'Guidelines' means the guidelines issued by INAI, regarding the compliance with the principles and duties of the Data Privacy Law.

'INAI' refers to the National Institute of Transparency, Access to Information and Protection of Personal Data (***Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales***).

'Privacy notice' means the physical or electronic document, or document generated in any other form by the controller and made available to data subjects, prior to the processing of their personal data. There are three forms of a privacy notice: comprehensive or full-form, simplified, and short.

'Processing' means any collection, use, disclosure or storage of personal data made through any means, including any access, handling, exploitation, transfer or disposal of personal data.

'Processor' or 'data processor' means the individual or entity that separately or jointly with others processes personal data on behalf of the controller.

'Remittance' any communication of personal data carried out between the controller and the processor, within or outside Mexican territory.

'Third Party' means an individual or entity, whether national or foreigner, that is not the data subject, the controller or the processor of the personal data.

'Transfer' means any communication of personal data carried out between the controller and any third party.

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 overseeing and advising on the protection of personal data within their organizations.

COLLECTION & PROCESSING

Principles and obligations

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

Pursuant to these principles:

- Personal data must be collected and processed fairly (and not through deceptive or fraudulent means) and lawfully
- Personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes.
- Consent must be obtained, unless an exception applies.
- Processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected. or further processed

- Personal data must be 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
- Personal data must be 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.
- A privacy notice (Aviso de Privacidad) must be made available to data subjects prior to the processing of their personal data.

Required information for privacy notices

To legally process personal data, data controllers must provide a privacy notice (Aviso de Privacidad), 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.

Controllers are required to notify data subjects of the main characteristics of the processing to which their personal data will be subject. This obligation is complied with through the privacy notice. Therefore, any data controller is required to prepare and make available to data subjects the relevant privacy notice(s) corresponding to their personal data. Controllers will have to make available distinct privacy notices for different categories of data subjects, such as personnel and customers.

The Guidelines permit the following three forms of privacy notice, 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:

- **Comprehensive privacy notice**: required to be provided when the personal data is obtained in-person from the data subject, for example, in a face-to-face interview.
- **Simplified privacy notice**: required to be provided when the data is obtained directly from the data subject, for example, when registering for an account on website or during a customer service call.
- **Short form privacy notice**: may be provided when the space for the privacy notice is limited and the Personal Data collected is minimum, for example, at an ATM, in a SMS, on a raffle ticket

Each of these forms must meet specific disclosure requirements, as described below, and the simplified and short-form notices must link to, or provide information about how to obtain, the comprehensive notice.

A **comprehensive privacy notice** must at least contain:

- The identity and address of the data controller
- A description of the personal data that will be processed
- Identification of any sensitive personal data that will be processed, and an affirmative statement that such data will be processed (if applicable)
- The purposes of the data processing, including the primary and any secondary purposes
- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes
- The means by which data subjects can revoke their consent
- The means for exercising rights of access, rectification, cancellation or objection (ARCO rights)
- Where appropriate, the types of data transfers to be made, including the purposes of such transfers and the identification of any third parties (not including processors) to whom personal data is transferred
- 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

A **simplified privacy notice** must include, at least, the following information:

- The identity and address of the Controller
- The purposes of the data processing, including the primary and any secondary purposes

- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes
- How to access or obtain the comprehensive privacy notice

The **short form privacy notice** must include, at least, the following information:

- The identity and address of the Controller
- The purposes of the data processing, without distinguishing any secondary purposes
- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes

In addition to the required information, a privacy notice must be clear and in a comprehensible language, and with an easy structure and design, which means it should among other things, the privacy notice should not use inappropriate, ambiguous, or vague sentences, or refer to texts and documents that are not available for the data subject to review.

The data controller has the burden of proof to show that the privacy notice was provided to the data subjects prior to the processing of their personal data (unless an exception applies). However, controllers are not required to provide a privacy notice where:

- personal data is obtained indirectly and it is intended for historical, statistical, or scientific purposes
- where the personal data collected is not subject to Mexican Privacy Laws (*eg*, certain business-to-business data as described previously)

Consent to processing

Except as otherwise provided by the Law, some form of consent is required for all processing of personal data; depending upon the circumstances consent may be implicit, express, or express and written:

Implicit (or tacit) consent applies to the processing of personal data generally, except where the Law requires express or express written consent (or where consent is not required):

- Implicit consent is obtained where the data subject has been informed of the privacy notice and has not objected to or refused the processing of personal data as described in the privacy notice.
- Express consent (notice and opt-in) is required for o the processing of financial or asset data.
- Express consent may be obtained verbally, in writing, or via any technology or other unmistakable indication. Express and written consent is required for the processing of sensitive personal data. Express written consent may be obtained through the data subject’s written signature, electronic signature, or any other authentication mechanism.

In addition to the above, express or express written consent must be obtained where otherwise specifically required pursuant to an applicable law.

On the other hand, consent from the data subject is not required (but a privacy notice must still be made available) for the processing of personal data where any of the following apply:

- The processing is required pursuant to an applicable Mexican law
- The data is contained in publicly available sources
- The identity of the data subject has been disassociated from the data (*ie*, the data subject is no longer identifiable)
- Where the processing is for the purpose of fulfilling obligations pursuant to 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 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

Mexican privacy laws distinguish between 'transfers' of personal data (to third parties) and transmissions of personal data (to processors). Under Mexican Privacy Laws, a 'transfer' is any communication or transmission of personal data by or on behalf of the Controller to a third party (not including a processor). Where the data controller intends to transfer personal data to domestic or foreign third parties other than a 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. In addition, the controller must notify data subjects in the privacy notice of the transfer, including:

- that the transfer may be made, as well as to whom and for what purposes the personal data may be transferred.
- where consent to the transfer is required, that the data subject consents and how the data subject can refuse to consent to the relevant transfer(s).

The purpose of the transfer must be limited to the purpose and conditions informed in the privacy notice and consented to by the data subject (as applicable).

The third-party recipient must assume the same obligations as the data controller who has transferred the data.

Domestic and 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 (provided they will comply with principles of Mexican Privacy Laws, the privacy notice provided to data subjects and the other applicable internal policies regarding data protection)
- 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 processors do not need to be notified or consented to 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, and more care should be taken in the collection and process of sensitive personal data.

The Controller also has the obligation to train its personnel on the proper handling of personal data in order to ensure compliance with the Mexican Privacy Laws. Per the Guidelines, a controller must also establish, document and follow security policies and procedures, including:

- Maintaining an inventory of personal data and the relevant processing systems, and update this at least once per year with respect to sensitive personal data
- Identifying the duties and obligations of persons that processing personal data on behalf of the controller
- Conducting appropriate risk analyses to identify dangers and estimate risk of harm to personal data
- Establishing security measures applicable and confirm they are effectively implemented
- Assessing and improving security on an ongoing basis
- Establishing a roadmap to implement any missing security measures identified pursuant to a security breach (as necessary to prevent a recurrence of such breach)
- Performing reviews or audits of security program
- Maintaining records of the storage means for personal data

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.

Under Mexican Privacy Laws, a security breach of personal data includes any unauthorized:

- loss or destruction of personal data
- theft, loss or copying of personal data
- use, access or processing of personal data
- damage or alteration of personal data

If there is a breach of personal data, the controller must first analyze the causes of such breach; and then take steps to implement any corrective, preventive, improvement actions necessary to prevent the breach from recurring.

If a breach significantly affects the property or moral rights of the data subjects, the controller must immediately notify the affected data subjects, as soon as it confirms that the breach has occurred, so that the affected Data Subjects can take the corresponding measures.

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
- Immediate corrective actions implemented in response to the breach, 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.

In determining the appropriate sanctions, the INAI will consider:

- The nature of the data
- The notorious inadmissibility of the refusal of the Data Controller, to carry out the acts requested by the data subject, in terms of this Law
- The intentional or unintentional nature of the action or omission constituting the offense
- The economic capacity of the data controller, and
- Recidivism

The sanctions imposed by the INAI are without prejudice to any further civil or criminal liability.

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 competent authority on this point.

KEY CONTACTS

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