Chambers
GLOBAL PRACTICE GUIDE

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy

Mexico
Creel, García-Cuéllar, Aiza y Enríquez, S.C

chambers.com

2020

MEXICO

Law and Practice

Contributed by:
Begoña Cancino Garín
Creel, García-Cuéllar, Aiza y Enríquez, S.C see p.9

Contents

1. Basic National Regime

1.1 Laws

The Mexican legal framework for personal data (the "Mexican DP Legal Framework") is contained primarily in the Mexican Constitution, followed by the "Federal Law of Protection of Personal Data held by Private Parties" (*Ley Federal de Protección de Datos Personales en Posesión de Particulares* – FDPL), effective as of 6 July 2010, and the "Federal Law of Protection of Personal Data held by Authorities" (*Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados* – FDPLA) effective as of 26 January 2017, which generally governs how companies or individuals and/or authorities gather, use, store, protect and manage personal data internally, and also how and with whom they share such information. The National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) is the federal authority in charge of overseeing the due observance of both the FDPL and the FDLPA, and the provisions arising therefrom.

The Mexican DP Legal Framework also includes the Regulations to the FDPL and FDPLA (the "Regulations"), which set out the procedural rules and mechanisms to comply with legal provisions; the Privacy Notice Guidelines (the "Guidelines"), which entered into force on 18 April 2013; and other provisions intended to provide a set of best practices, such as the Parameters for Self-Regulation regarding personal data (the "Parameters"), which entered into force on 30 May 2014.

1.2 Regulators

The INAI is empowered to evaluate whether the incident that originated a data breach was caused by a failure of compliance or negligence. The INAI is in charge of guaranteeing people access to public government information, protecting personal data in the possession of the federal government and individuals, and resolving denials of access to information formulated by the dependencies or entities of the federal government.

Public prosecutors in Mexico are in charge of investigating and resolving cyber activities; a cyber police service has been created to follow up on crimes or unlawful activities committed through the internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account. In addition, the Federal Police has created a scientific division called the National Centre for Cyber-incidents Response, which is focused on assisting the victims or claimants of cyber threats and cyber attacks.

1.3 Administration and Enforcement Process

The procedure will be initiated by request from the data owner or his legal representative, clearly stating the content of his claim and the provisions of the law deemed violated. The data protection request must be submitted to the INAI within 15 days of the date on which the response from the data controller is communicated to the data owner. If the data owner does not receive a response from the data controller, the data protection request may be filed after the deadline for the data controller's response has passed. In this case, it will be sufficient for the data owner to accompany its data protection request with the document that proves the date on which he filed the request for access, rectification, cancellation or objection (ARCO).

The data protection request will also be allowed under the same terms when the data controller does not deliver the requested personal data to the data owner, or delivers it in an incomprehensible form or refuses to make changes or corrections to personal data, or where the data owner is not satisfied with the information delivered since he considers it to be incomplete or not matching the information requested. Upon receipt of the data protection request by the INAI, said request will be sent to the data controller for said controller to issue a response, provide any evidence it deems relevant and make its formal arguments in writing within 15 days. The INAI will admit any evidence it deems relevant and introduce it. It may also request any other evidence it deems necessary from the data controller. After the introduction of evidence, the INAI will notify the data controller of its right to present its arguments within five days of notification, if it considers this to be necessary. As required under the procedure, the INAI will issue a decision on the data protection request filed, after analysing the evidence and other elements of proof it deems appropriate, such as those that arise from the hearing(s) held with the parties.

1.4 Multilateral and Subnational Issues

On 12 June 2018, the Mexican Official Gazette published a notice that Mexico has adopted the Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and cross-border data flows. Both are binding international instruments that protect the individual against any abuse of the collection and processing of personal data, and at the same time seek to regulate the cross-border flow of personal data.

In general terms, Mexico has proper regulations on the protection of personal data, and Mexican law does not differ too much from the specific provisions set forth in the EU's General Data Protection Regulation; however, there are differences that should be considered carefully.

The applicable laws detailed in **1.1 Laws** are of a federal nature.

1.5 Major NGOs and Self-Regulatory Organisations

In order for parties to comply with their obligation of accountability, they may use standards, best international practices, corporate policies and any other mechanisms adequate to pursue such purpose, including self-regulation agreements. The Mexican regulator issues the parameters for self-regulation regarding personal data. In addition, in terms of the protection of personal data, Mexican law allows that agents from the private and public sectors (such as companies, consumers, organisations or public administrations) may organise – individually or collectively – the issuance of regulations on the subject through codes of good practices. In this regard, there are two types of model:

- pure self-regulation, where the regulation is left in the hands of the particular agent, without the slightest intervention by the State; and
- mixed self-regulation, where the law establishes minimum standards on personal data protection.

There is therefore legislation on the matter, but it allows individuals to develop and establish their own regulation based on those standards, as long as those minimums are met, and to move within that flexible framework.

The principal duty of individuals and corporate bodies who are accredited as certifiers is to certify that the privacy policies, programmes and procedures voluntarily put into place by data controllers are followed in practice, and to ensure proper processing and that the security measures adopted are adequate for their protection. For this purpose, certifiers may adopt mechanisms such as inspections and audits.

1.6 System Characteristics

The Federal Law on the Protection of Personal Data Held by Private Parties includes a data controller's obligation to notify immediately (instead of within a specific term, as in the GDPR) a breach to data subjects that may significantly affect their economic or moral rights, but no requirement to notify the federal regulator is set forth in the relevant law. In this regard, it will be up to data controllers to decide whether or not to notify data subjects; to that end, a data controller would consider the sensitivity of the personal data compromised in the breach and to what extent its misuse could affect data subjects from an economic and moral perspective.

1.7 Key Developments

There have been no key developments in law, regulatory activity, enforcement, litigation or public attention in the last 12 months.

1.8 Significant Pending Changes, Hot Topics and Issues

Reforms to the current privacy law are expected in the short term, to bring Mexican regulations in line with Convention 108 and ultimately with the GDPR.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The appointment of a data protection officer is mandatory; failure to do so is not specifically sanctioned by applicable law but may be interpreted as improper or illegal data processing.

Data controllers are accountable at every stage of personal data processing required for the conduct of the business, and have the following key legal obligations:

- to provide fair processing notice to all data subjects;
- to gather consents for processing personal data;
- to abide by the personal data principles while processing personal data (Legal Processing of PD); and
- to implement technical and organisational measures to protect personal data against damage, loss, alteration, destruction or unauthorised use (Security Measures).

Fair processing notice (drafting and delivery of a privacy notice to each data subject) is one of the key obligations imposed on data controllers under the law and must be drafted in three formats, depending on the delivery method:

- Full Privacy Notice (delivered personally to the data subject);
- Simplified Privacy Notice (delivered directly to data subjects, using remote mechanisms); and
- Abbreviated Privacy Notice (delivered to data subjects through written mechanisms).

Consent must be freely given, specific and informed. If customers' and employees' personal data may include health information, which is considered to be sensitive data under the law, express and written (opt-in) consent is required. The law provides that express and written consent may be granted by a handwritten signature or an electronic signature, or by any other authentication mechanism established for such purpose. On the other hand, if the personal data collected does not contain sensitive information but only financial information (such as credit card information), express (but not written) consent is required. Express consent may be granted verbally, in writing, by electronic or visual means, or any other technology, or by unequivocal signs. Regarding express consent, the law provides that it shall be given verbally "when the data subject externalises it in person or through the use of any technology that allows for verbal interlocution." Also, express consent must be unequivocal – ie, there must be elements that undoubtedly evidence that it has been granted. Finally, if only "standard" personal data is collected and does not include sensitive or financial information, implied (opt-out) consent would be sufficient. Under the law, consent is deemed implied when a data subject does not object to the processing of his or her personal data once a privacy notice has been furnished.

The terms "privacy by design" and "by default" are not specifically set forth in Mexican law.

The need to conduct privacy impact analyses is suggested in the applicable parameters and guidelines issued by the authority.

A data controller is allowed to comply with the accountability principle, but is not required to do so.

A data subject's rights provided by Mexican law refer only to the rights to access, rectify, erase/cancel and oppose to the processing of their personal data. Mexican law does not specifically provide for portability.

Mexican laws provide for dissociation, understood as the procedure through which personal data cannot be associated with the data owner nor allow identification thereof, by way of its structure, content or degree of disaggregation.

Mexican law provides for cloud computing, understood as a model for the external provision of computer services on demand that involves the supply of infrastructure, a platform or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared. Within the scope of their authority and assisting the INAI, regulatory agenciesshall issue guidelines for the proper processing of personal data in cloud computing.

According to Mexican law, "harm" refers to any damage suffered by data subjects to their property or rights, because of a misuse of their data or a breach of law.

2.2 Sectoral and Special Issues

The term "sensitive personal data" is defined as all personal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive data is considered to be that which may reveal items such as racial or ethnic origin; present and future health status; genetic information; religious, philosophical and moral beliefs; union membership; political views; and sexual preference.

Financial Data

In general terms, financial or asset data will require the express consent of the data owner for processing; however, it is not necessarily considered sensitive data.

Health Data

Health data is considered sensitive data.

Communications Data and Voice Telephony

The constitutional right of inviolability protects private communications, in some cases; private communications may contain personal data or sensitive personal data, the processing of which should also abide by the principles of the related privacy law. This also applies to text messaging. Guidelines applicable to the preparation of the Privacy Notice require data subjects to be informed of any technology that allows the automatic collection of PI simultaneously with the first contact with the individuals and the provision of mechanisms to collect consents through opt-in mechanisms, and how to deactivate said technology. There is no distinction in Mexican law between cookies, beacons and tracking technologies, all of which are included within the term "cloud computing".

Internet

Privacy policies are required and, according to Mexican consumer protection provisions, will be legally regulated under the provisions applicable to adhesion contracts.

Mexican law is silent about whether consent is required for behavioural advertising, but, in general, consent will be required for the processing of personal data related to behavioural advertising as long as such data could be linked to an identified or identifiable individual. This also applies to video and television advertising.

Social Media, Search Engines and Large Online Platforms

The previous comments provided in this section regarding the internet apply indistinctly to social media, search engines and large online platforms.

Mexican law provides for the right of erasure as an ARCO right.

In terms of hate speech, disinformation, abusive material and political manipulation, the speech is usually analysed by means of provisions addressing the constitutional right of expression.

Mexican law does not specifically address data portability.

Children's Privacy

The Mexican Privacy Law does not provide for children's rights on this topic, but some aspects might be found in the General

Law of Children's and Teenager's Rights. Mexico should also abide by international treaties intended to protect children.

Educational or school data is considered sensitive information if it can be linked to an identified or identifiable individual.

2.3 Online Marketing

Data privacy law provides that processing for marketing, advertising or commercial promotion purposes needs to be expressly and specifically included as one of the "purposes of processing" in the privacy notice.

The Federal Consumer Protection Law, on the other hand, provides for an opt-out system. It states the possibility for the consumer to demand that specific suppliers and companies that use their information for advertising purposes do not offer goods, products or services directly to their address, workplace or electronic address, or through any other means, nor send advertising. Likewise, the consumer may demand at all times that suppliers and companies that use their information for marketing or advertising purposes do not assign or transfer their information to third parties, except when such assignment or transfer is determined by a judicial authority.

Finally, the Federal Law to Protect and Defend Users of Financial Services provides that regulated financial institutions shall not contact their consumers for marketing or advertising purposes when they have expressly asked not to be contacted, or if they are registered with the specific registry of the National Commission for the Defense of Financial Consumers. This law also provides for an opt-out system.

See **2.2 Sectoral and Special Issues** regarding data processing within the internet environment.

2.4 Workplace Privacy

The special law regulating labour issues is the Federal Labor Law, which provides that the processing of personal data held by authorities will be subject to the provisions of the applicable privacy law.

Although there is no particular restraint on the employer's ability to monitor workplace communications on the labour side, such activities are restricted from the data privacy standpoint if the monitored communications contain information of identifiable individuals – eg, the image or portrait of identifiable individuals is considered personal data, and fair notice would be required in order to process it.

Whistle-blowing is not regulated under Mexican law, but it is a common and good practice within companies to implement this kind of procedure. From a labour law perspective, it is not necessary to notify employees about the processing of their personal information collected through a hotline. However, from a data privacy standpoint and in cases where the whistle-blower is required to identify himself, he has to be notified about the processing of his personal data so as to give his consent; such consent should be given after data controllers provide the parties involved with all specific information about the whistle-blowing process (usually through a "whistle-blowing privacy notice"). In general terms under Mexican law, all privacy notices should contain (at least) the following information:

- the identity and domicile of the data controller;
- the purpose of the data processing;
- the means to limit the disclosure of data;
- the means for exercising ARCO rights;
- the data transfers to be made (where applicable); and
- the procedure through which to notify data subjects about changes in the privacy notice.

If a whistle-blower decides to take the first option, they retain the rights to withdraw the consent at any time.

2.5 Enforcement and Litigation

When determining the amount of fines for violations of privacy laws, regulators shall consider the following factors:

- the nature of the personal data (ie, whether the data is sensitive personal data);
- whether the infringer had ignored the data subject's initial rejection for the collection and processing of the data;
- whether the infringement was intentional or caused by omission;
- the economic capacity of the infringer;
- whether the infringer has previously been found guilty of the same offence; and
- potential enforcement penalties.

Penalties vary from a warning notice to fines ranging from 100 to 320,000 days of the minimum daily wage in Mexico City, to imprisonment ranging from three months to five years. These penalties may be doubled in the case of sensitive personal data.

The adoption of a self-regulatory scheme under the Parameters for Mandatory Self-Regulation can be used as evidence of compliance with the applicable law and the regulation, and may help to reduce any sanctions should a breach occur.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

The laws applicable to law enforcement access to data for serious crimes are the Federal Constitution, the Federal Law of Protection of Personal Data held by Private Parties and its regulations, and the General Law for Transparency and Access to Public Information. The Transparency Law adds corruption, serious human rights violations, and crimes against humanity to the list of issues where information cannot be withheld.

Any authority, entity or organism connected with the Judicial, Executive or Legislative powers, either autonomous or not, as well trust funds and all parties exercising public funds and carrying out acts of authority, is entitled to classify or declassify information containing personal data. Also, access to personal data held by authorities could be obtained through out a judicial order.

There are physical, technical and administrative safeguards in place to protect privacy by law and in practice.

3.2 Laws and Standards for Access to Data for National Security Purposes

The laws applicable to government access to data for intelligence, anti-terrorism or other national security purposes are the same as those stated in **3.1 Laws and Standards for Access to Data for Serious Crimes**.

3.3 Invoking a Foreign Government

An organisation may not invoke a foreign government in a formal way, but the Federal Law for Protection of Personal Data held by Private Parties provides that it is a responsibility of the Federal Regulator (INAI) to co-operate with other domestic and international bodies and supervisory authorities, in order to assist in the area of data protection.

3.4 Key Privacy Issues, Conflicts and Public Debates

There is a public debate regarding the use of personal data by authorities enforcing criminal laws because of the illegal disclosure of photos from the victims of homicide in Mexico City or the illegal disclosure in the media of personal data from people involved in crimes. The debate focuses on the right to be informed and the presumption of innocence that applies in Mexico, along with the right of auto determining the use of personal data.

4. International Considerations

4.1 Restrictions on International Data Issues

A data controller has to comply with the following requisites before transferring data to a data processor:

- data controllers must obtain the consent of the data subjects to transfer their personal data;
- the data controller must communicate the privacy notice to the data processor; and
- the data processor must assume the same obligations that correspond to the data controller.

4.2 Mechanisms That Apply to International Data Transfers

Contractual provisions, corporate rules and consent are the key aspects to proceed with international data transfers, unless exceptions arise.

4.3 Government Notifications and Approvals

No government notifications or approvals are required in order to transfer data internationally in accordance with the Mexican Privacy Law, only those required to be obtained from data subjects.

4.4 Data Localisation Requirements

Cross-border data transfers can be performed without obtaining consent from data subjects if the reason to transfer the data internationally falls into the following cases:

- when the data relates to the parties of a private or administrative contract or partnership agreement and is necessary for its performance and enforcement;
- the law requires that the data shall be processed;
- such action hinders judicial or administrative proceedings relating to tax obligations, the investigation and prosecution of crimes, or the updating of administrative sanctions;
- it is necessary to protect the legal interests of the data owner;
- it is necessary to carry out an action in the public interest;
- it is necessary to fulfil an obligation legally undertaken by the data owner; or
- the data is subject to processing for medical diagnosis or prevention, or health services management, provided that such processing is done by a health professional subject to a duty of secrecy.

4.5 Sharing Technical Details

There is no legal requirement to share with the federal regulator on data privacy matters.

4.6 Limitations and Considerations

There is a particular obligation set forth in the FLPD on the Federal Regulator (INAI) to co-operate with domestic or international authorities when it comes to data privacy issues.

4.7 "Blocking" Statutes

See **4.4 Data Localisation Requirements**.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Mexican authorities have addressed biometric data through the issuance of guidelines intended to assist all parties (data collectors, processors and data subjects) to identify and process all biometric data accordingly. Mexican law is silent in such specific regard, but entitles the federal regulator to issue official guides to communicate its criteria on the matter.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Pursuant to the FDPL, individuals or corporate bodies may agree among themselves or with civil or government organisations – national or foreign – on binding self-regulation arrangements in matters of personal data protection, complementing the provisions of the Law, these Regulations, and the regulations issued by departments or agencies in this matter and within their jurisdiction. Furthermore, through such arrangements, the data controller may prove to the federal regulator that it complies with the obligations set forth in said regulations. This is in order to harmonise the processing carried out by those who become bound by the arrangements, and to facilitate the exercise of data subjects' rights.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

Based on the INAI's figures, fines imposed by such regulator for the misuse of personal data from 2012 to January 2019 amounted to circa MXN424,340,941, and 257 sanction procedures were generated for misusing people's data.

Companies dedicated to the financial and insurance services have been sanctioned the most by the INAI, with 78 procedures opened between 2012 and January 2019, whose fines reached MXN252,666,244, equivalent to 59.5% of the total amount of fines applied. They are followed by private organisations dedicated to the media, with 25 procedures opened, and fines reaching MXN54,660,607. In third place are those dedicated to the retail trade, with 41 procedures opened, and MXN33,356,032 in fines. The FDPL provides for 19 behaviours that will incur fines for private companies.

Chapter X of said law includes the following in the list of punishable activities: "transfer data to third parties without communicating to them the privacy notice that contains the limitations to which the holder subjected the disclosure of the same", or "carry[ing] out the transfer or transfer of personal data, outside of the cases in which it is permitted by law." The sanctions that apply range from 100 to 320,000 days of minimum wage in force in Mexico City (MXN10,268 to MXN32.8 million).

5.4 Due Diligence

Although there are no legal specifications in this regard, certain best practices are recommended to ensure data protection during a due diligence process. First, while populating a data room, it is advisable to redact personal information; provide model contracts rather than real contracts; avoid disclosure of sensitive personal information; ensure that all people accessing the data room are bound by confidentiality agreements; and – finally but importantly – choose a secure data room provider that complies with data protection laws. The value of personal data should be confirmed during the deal and reflected in the contract, especially those referring to compliance with privacy laws. Also, if it is an asset deal, then it should be confirmed whether the database containing personal data can be assigned or not, as this may have a direct impact on the structure of the deal.

5.5 Public Disclosure

There is no Mexican data protection law mandating disclosure of an organisation's cybersecurity risk profile or experience.

5.6 Other Significant Issues

Additional provisions are expected that will regulate, in a deeper sense, data privacy issues related to cloud computing. Under Mexican regulations, data controllers should only use services that ensure the proper protection of the personal data they gather.

Considering that cloud computing is a model for the external provision of computer services on demand that involves the supply of infrastructure, a platform or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared, a data controller should enter into service agreements with at least the following contractual conditions for the service provider:

- it shall use similar policies to protect personal data as those reflected in Mexican law;
- if the service provided involves subcontracting, such provisions should be transparent;
- it should not assume any ownership of the information about which the service is provided; and
- it should maintain confidentiality with respect to the personal data about which it provides the service.

In addition, the service provider should have mechanisms in place at least for:

- disclosing changes in its privacy policies and the services provided;
- permitting the data controller to limit the type of processing of personal data included in the service provided;
- establishing and maintaining adequate security measures to protect data included in the service provided;
- ensuring the suppression of data after the service has been provided;
- impeding access by those who do not have authorised access and informing the data controller if there is an official request for data from a competent authority; and
- informing the data controller about events of breach, immediately after their occurrence, and providing the data controller with all necessary information to assess the extent of the harm caused by the breach, in accordance with Mexican legal provisions.

Creel, García-Cuéllar, Aiza y Enríquez, S.C is a leading full-service corporate law firm, specialising in all practice areas, with an unwavering commitment to excellence. It has an established reputation for delivering creative, specialised and responsive legal advice on the most complex and innovative matters in Mexico for the most sophisticated and demanding clients. The practice is based on the philosophy that a client is best served by legal advice designed to anticipate and avoid problems, rather than respond to them. The firm's goal is to be the law firm of choice for clients with the most demanding transactions and projects and, in this endeavour, to become a strategic service-provider to them, by offering the type of legal advice that gives clients certainty and peace of mind.

Author

Begoña Cancino Garín is a partner and the head of department, practising in the areas of intellectual property, data privacy, regulatory and administrative litigation. Ms Cancino is a member of the International Trademark Association (INTA), the Mexican Bar Association and the Mexican Association for the Protection of Intellectual Property (AMPPI). She has contributed to several publications relating to the practice of Data Protection law.

Creel, García-Cuéllar, Aiza y Enríquez, S.C

Torre Virreyes
Pedregal 24, Piso 24
Col. Molino del Rey
Ciudad de México
Mexico 11040

Tel: +52 55 4748 0600
Fax: +52 55 4748 0670
Web: www.creel.mx

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ