Practical Law™
GLOBAL GUIDE 2015/16
DATA PROTECTION

Data protection in Mexico: overview

Begoña Cancino
Creel, García-Cuéllar, Aiza y Enriquez, SC

global.practicallaw.com/8-502-5162

REGULATION
Legislation

1. What national laws regulate the collection and use of personal data?

The protection of personal data is recognised in the Mexican Constitution (Constitution) as a fundamental right. Every individual has the right to the protection of their personal data and the right to access, rectify, oppose and cancel personal data under the terms specified by the federal laws (*Article 16, Constitution*).

In relation to the protection of personal data under the Constitution, Mexico has developed a strong system of data protection laws that have a specific scope of protection depending on the nature of the organisation or the individual responsible for gathering and treating the information or the data (data controller). Therefore, if personal data is gathered and treated by a government organisation or public servant of the Mexican Federal Government, those individuals and organisations must comply with the following laws:

- Federal Law of Transparency and Access to the Governmental Public Information (Federal Transparency Law) and its internal regulation. This applies to and regulates federal government organisations and their public servants in relation to how they should administer and treat information relating to the private life of individuals.
- Guidelines of the Federal Institute for Information Access and Data Protection, regarding Personal Data gathered and treated by the Public Federal Administration and their employees (Data Protection Guidelines). The Data Protection Guidelines specifically regulate the general politics and procedures the Federal Government and their public servants must observe in order to achieve the protections required by the Mexican Constitution and the Federal Transparency Law.

In addition, the Mexican Government recently issued a General Law of Transparency and Access to the Public Information (General Transparency Law), which came into force on 5 May 2015. The General Transparency Law provides general guidelines that will be adjusted to federal and local laws and which relate to:

- Transparency and access to public information.
- Data held by public individuals and organisations.

If personal data is gathered and treated by a private organisation or private individual, such parties will be required to comply with the Federal Law of Personal Data held by Private Parties (Federal Personal Data Law) and its internal regulation.

On 8 December 1997, Mexico subscribed to the Economic Partnership, Political Coordination and Cooperation Agreement with the EU in which "the parties agree to ensure a high standard of protection to the treatment of the personal data in accordance with the standards and provisions adopted by the international organisms and the EU" (*Article 51*). Through this agreement, Mexico has adopted Directive 95/46/EC on data protection (Data Protection Directive).

Scope of legislation

2. To whom do the laws apply?

The parties regulated under the Federal Personal Data Law are private parties, whether individuals or private legal entities that process personal data.

The Federal Transparency Law, the General Transparency Law and the Data Protection Guidelines are applicable to federal government organisations and their public servants (*see Question 1*).

3. What data is regulated?

"Personal data" is regulated. Personal data includes any information concerning an identified or identifiable individual. Mexican data protection laws also regulate a specific category of data known as "sensitive personal data" (that is, personal data touching on the most private areas of the data subject's life, or whose misuse might lead to discrimination or involve a serious risk). Sensitive data is considered to be data which may reveal the data subject's:

- Racial or ethnic origin.
- Present and future health status.
- Genetic information.
- Religious, philosophical and moral beliefs.
- Union membership.
- Political views.
- Sexual preference.

4. What acts are regulated?

The processing of personal data is regulated under Mexican data protection laws. The processing of personal data includes the retrieval, use, disclosure or storage of personal data by any means. Under the applicable laws, use of personal data includes any action of access, management, exploitation, transfer or disposal of personal data.

© Thomson Reuters 2016
This article was first published in the Data Protection Global Guide 2015/16 and is reproduced with the permission of the publisher, Thomson Reuters. The law is stated as at 1 October 2015.

5. What is the jurisdictional scope of the rules?

The Federal Personal Data Law applies to all private parties (whether individuals or legal entities) that process personal data in Mexico.

6. What are the main exemptions (if any)?

The following parties are exempt from the provisions of the Federal Personal Data Law:

- Credit information societies, provided the exemption is contemplated under the Law to Regulate the Credit Information Societies.
- Any individual that gathers and stores personal data for personal purposes and does so without the intention of commercially exploiting or using the data.

The following information in relation to individuals is also exempt from the provisions of the Federal Personal Data Law:

- Information from legal entities.
- Information from individuals in their capacity as professionals or merchants.
- Information from individuals providing services to individuals or legal entities if the information refers to their name, employment position, address, phone number (provided the information is used with the purpose of representing the employee or a contractor).

7. Is notification or registration required before processing data?

The Federal Personal Data Law does not require any notification or registration before the processing of the personal data.

The Federal Personal Data Law also provides that if the creation of a database containing sensitive personal data can be justified, notification is not necessary.

MAIN DATA PROTECTION RULES AND PRINCIPLES

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

Obligations are imposed on data controllers to ensure the personal data is processed properly. The obligations are set out in the Federal Personal Data Law, which establishes the following principles:

- **Legality principle.** Under this principle, personal data must be gathered and treated lawfully in accordance with the Federal Personal Data Law.
- **Consent principle.** Under this principle, consent from the owner must be obtained in order to gather and treat their personal data (*see also Question 9*).
- **Information principle.** Under this principle, the owner of personal data must be informed of the terms of how their personal data will be treated and processed. This is done by making a privacy notice available to the data subject (*see Question 12*).
- **Quality principle.** Under this principle, the data controller must verify that the personal data contained in the databases is correct and updated for the purposes for which it was gathered.
- **Finality principle.** Under this principle, the data controller must delete the personal data when the purpose for obtaining the information is achieved. In addition, the personal data that is gathered and treated by the data controller must only be treated for the purposes for which it was originally obtained.
- **Loyalty principle.** Under this principle, the gathering of personal data must not be done through deceptive or fraudulent means.
- **Proportionality principle.** Under this principle, the data controller is only allowed to gather personal data that is necessary, appropriate and relevant to accomplish the purpose established in the privacy notice.
- **Responsibility principle.** Under this principle, the data controller must ensure that the principles established in the Federal Personal Data Law are fulfilled, by adopting all necessary steps for the application.

9. Is the consent of data subjects required before processing personal data?

Under Mexican law, all processing of personal data is subject to the consent of the data subject. Express consent is provided when it is communicated verbally, in writing by electronic or optical means, or via any other technology. Financial or asset data and sensitive data require the express consent of the data subject.

It is generally understood that the data subject will provide his consent to his data being processed once the privacy notice has been made available to him and he does not provide his express objection. It must also be possible for consent to be revoked at any time without retroactive effects, and the data controller must establish the mechanism and procedure for such revocation in the privacy notice.

There are no particular rules regarding the consent of minors in the Federal Personal Data Law. In this regard, the general civil provisions in connection with capability are applicable.

10. If consent is not given, on what other grounds (if any) can processing be justified?

In the absence of consent, the data controller must rely on the exceptions set out in the Federal Personal Data Law. The exceptions are as follows:

- The personal data is already available in the public domain.
- The personal data is submitted to a process of dissociation (that is, when personal data is no longer associated with an identifiable data subject or person).
- The data processing is performed for the purpose of fulfilling an obligation which derives from a juridical relationship between the data subject and the data controller (for example, tax paying obligations of a company in Mexico where the employer must use personal data of employee to fulfill tax obligations such as social security).
- There is an emergency situation that could potentially affect the data subject (for example, either physical damage or damage to his possessions).

- The personal data is essential for medical purposes (for example, the attention or provision of healthcare services, diagnosis or prevention, medical treatment or management of health services) where:
  - the data subject is not in a physical or mental condition to grant consent under the terms of the General Health Law and other applicable regulations; and
  - the treatment of personal data is performed by an individual who has a legal obligation to keep the information secret or other equivalent obligations.
- The decision to process the data derives from a competent authority such as the Federal Institute for Access to Public Information and Data Protection.

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

To process sensitive personal data, the data subject must provide his express consent in written form. This can be validated through:

- The data subject's handwritten signature.
- Electronic signature.
- Other mechanisms of authentication.

Databases containing sensitive data 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 regulatory party. When processing sensitive data, the data controller must make reasonable efforts to keep the processing period to a minimum.

All penalties set out in the Federal Personal Data Law are doubled if the breach relates to sensitive personal data.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

When personal data is to be collected, the data subject must be provided with a privacy notice, which must contain at least the following information:

- The identity and address of the data controller.
- The purposes of the treatment of the personal data.
- The available options and resources that the data controller can offer to the data subject to limit the use or the dissemination of the personal data.
- The resources for enforcing the rights of access, rectification, cancellation or opposition to the processing in accordance with the Federal Personal Data Law.
- 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 data subject any changes in the privacy notice, in accordance with the Federal Personal Data Law.

13. What other specific rights are granted to data subjects?

The Federal Personal Data Law contemplates the following rights for the owners of personal data:

- The right to access the personal data.
- The right to rectify the personal data.
- The right to oppose the treatment of the personal data.
- The right to cancel/delete the personal data (*see Question 14*).

14. Do data subjects have a right to request the deletion of their data?

At all times the data subject has the right to request the cancellation of his personal data. The request for cancellation leads to a blocking period after which, the personal data is deleted. However, the data controller may retain data exclusively for purposes related to his responsibilities arising from processing. Once the data is cancelled, the data owner will be notified.

However, the data controller is not obligated to cancel personal data if:

- 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 the data to be processed.
- The deletion of the data will hinder:
  - judicial or administrative proceedings relating to tax obligations;
  - investigations and prosecution of crimes; or
  - the updating of administrative sanctions.
- The data is necessary to:
  - ensure the legally protected interests of the data subject;
  - carry out an action in the public interest; or
  - fulfil an obligation legally undertaken by the data subject.
- The data is subject to processing for the purposes of medical diagnosis or prevention, or health services management, provided the processing is performed by a healthcare professional subject to a duty of secrecy.

SECURITY REQUIREMENTS

15. What security requirements are imposed in relation to personal data?

Data controllers must establish and maintain administrative security measures, technical security measures and physical security measures that allow personal data to be protected from damage, loss, alteration, destruction or unauthorised use, access or treatment (*Federal Personal Data Law*).

In addition, the Federal Personal Data Law establishes that data controllers must not adopt security measures that are lesser than the measures implemented to conserve or protect their own information.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

The data controller must immediately inform the data subject if a breach or violation of security has been made to the data controller's security measures that could affect the moral and economic rights of the data subject.

The internal regulation of the Federal Personal Data Law defines the following conduct as a security breach or violation of security:

- Loss or unauthorised destruction of personal data.
- Stealing or making an unauthorised copy of personal data.
- Unauthorised use, access and treatment of personal data.
- Damage, alteration or unauthorised modification of personal data.

PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

According to the Federal Personal Data Law and its internal regulation, personal data can be processed by a third party at the request of the data controller. However, it is necessary for such a relationship to be established under an agreement.

To treat personal data on behalf of the data controller, third parties must:

- Treat the personal data according to the instructions of the data controller.
- Refrain from treating the personal data for purposes different to those commanded by the data controller.
- Implement security measurements according to the Federal Personal Data Law, its internal regulation and with regard to the related and applicable laws.
- Maintain confidentiality regarding the treated personal data.
- Remove the personal data being treated when the relationship with the data controller is finalised (or requested by instruction from the data controller), unless there is a legal provision demanding the conservation of the personal data.
- Refrain from transferring the personal data, unless instructed to do so by the data controller.

ELECTRONIC COMMUNICATIONS

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The Federal Personal Data Law is silent in relation to the storage of cookies or equivalent devices on the data subject's terminal equipment.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The Federal Personal Data Law is silent in relation to unsolicited electronic commercial communications (spam). However, consumers can directly demand specific suppliers and companies which use their information for marketing or advertising purposes to (*Federal Law on Consumer Protection*):

- Not bother them via their personal address, workplace, email account or any other means when being offered goods, products or services.
- Not send advertising.

Consumers can also at any time demand suppliers and companies using their information for marketing or advertising purposes to not assign or transfer their information to third parties (unless the assignment or transfer is determined by a judicial authority).

The Consumer Protection Agency maintains a public registry of consumers who do not wish that their information be used for marketing or advertising purposes. Consumers can be listed in this public registry free of charge.

Infringement of these provisions is punishable with fines ranging from about MXN7,010 to MXN22 million (these amounts are determined according to the current minimum wage).

INTERNATIONAL TRANSFER OF DATA

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

Domestic or cross-border transfers of data are allowed and can be performed without prior authorisation from the Federal Institute for Access to Public Information and Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*).

An intra-group cross-border transfer of data does not require consent from the data subject. However, in such a scenario, the data controller is responsible for ensuring the recipient of the data abides by the same principles to those set out in the privacy policy. This can be accomplished through:

- The execution of data transfer agreements (although at present, no standard model clauses have been approved or issued by the relevant regulator).
- The implementation of enterprise-wide enforceable policies that comply with applicable requirements under Mexican law (although no regulatory approval would be required for such policies and there are no geographic transfer restrictions under the applicable laws).

Domestic and international transfers of data can also be carried out without the consent of the data owner 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.
- Necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party.
- Necessary or legally required to safeguard public interest or for the administration of justice.
- Necessary for the recognition, exercise or defence of a right in a judicial proceeding.
- Necessary to maintain or fulfil a legal relationship between the data controller and the data subject.

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

The only requirement to store certain types of personal data relates to the storage of sensitive information, as the data controller must:

- Justify the creation of the database.
- Make reasonable efforts to keep the period of processing the data to a minimum.

Data transfer agreements

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Data transfer agreements are contemplated in Mexican data protection laws.

No standard forms or precedents have been approved for data transfer agreements by the national authorities. However, it is possible to submit such agreements to and obtain the opinion of the Federal Institute for Access to Public Information and Data Protection. The Institute will then confirm whether such an agreement is suitable and meets the applicable requirements.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

A data transfer agreement is not sufficient to legitimise the transfer, as the agreement must include an express reference that the data can be transferred and specify the intended purposes for being transferred. Therefore, the information contained in the privacy notice is crucial to legitimise the transfer.

24. Does the relevant national regulator need to approve the data transfer agreement?

There is no legal requirement for the Federal Institute for Access to Public Information and Data Protection to approve the data transfer agreement.

ENFORCEMENT AND SANCTIONS

25. What are the enforcement powers of the national regulator?

The Federal Institute for Access to Public Information and Data Protection has the following powers of enforcement:

- The power to resolve data protection disputes.
- The power to conduct verification procedures.
- The power to enforce penalty application proceedings and impose sanctions for infringements of the Federal Personal Data Law.

26. What are the sanctions and remedies for non-compliance with data protection laws?

Infringements of the Federal Personal Data Law are sanctioned by the Federal Institute for Access to Public Information and Data Protection (INAI) with:

- 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, rectification, cancellation and opposition (*see Question 13*)).
- Fines ranging from 100 to 320,000 days of the Mexico City minimum wage. If the data controller has committed the same offence previously (recidivism), an additional fine is imposed. For violations committed when processing sensitive personal data, the sanctions can be increased up to double the established amounts.

When calculating the amount of fine to impose, the INAI takes the following into consideration:

- The nature of the personal data (that is, whether the data is sensitive personal data).
- Whether the infringer had ignored the data subject's initial rejection for 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.

On the other hand, the Federal Personal Data Law only provides for criminal sanctions when:

- Data controllers using the personal data with the aim making an economical profit provoke a security breach to a database under their control. This is punishable by three months to three years' imprisonment.
- Data controllers using the personal data with the aim making an undue profit treat personal data by cheating (for example, taking advantage of an error which enabled the data controller to obtain the data from the data subject). This is punishable by six months to five years' imprisonment.

For criminal conduct committed when the treatment or violation relates to sensitive personal data, the sanctions can be increased up to double the established amounts.

Finally, 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 the final decision of the INAI at the initial infringement proceeding before the civil claim can commence.

REGULATORY AUTHORITY

National Institute for Transparency, Information Access and Personal Data Protection held by Individuals

W http://inicio.ifai.org.mx/SitePages/ifai.asp

Main areas of responsibility. Ensuring compliance with data protection laws, enforcement of data protection, verification and sanctions procedures, development, promotion and diffusion of analysis, and studies and investigations in personal data protection.

ONLINE RESOURCES

National Institute for Transparency, Information Access and Personal Data Protection held by Individuals

W http://inicio.ifai.org.mx/SitePages/ifai.aspx

Description. Official website of the highest data protection authority in Mexico. Website is available in English.

Practical Law Contributor profiles

Begoña Cancino, Partner

Creel, García-Cuéllar, Aiza y Enriquez, SC
T +52 (55) 4748 0679
F +52 (55) 4748 0690
E begona.cancino@creel.mx
W www.creel.mx

Professional qualifications. Mexico, Lawyer,

Areas of practice. Intellectual property and entertainment.

Non-professional qualifications. Universidad La Salle, Mexico, 2001; post-graduate diplomas in IP, Universidad de Buenos Aires (UBA), Universidad Nacional Autónoma de México (UNAM) and Ilustre Nacional Colegio de Abogados

Recent transactions

- Counsel to a multinational alcoholic beverages company in several transactions intended to grow its tequila segment including the acquisition of two premium brands in Mexico.
- Counsel to a multinational dairy and food corporation in the acquisition of a brand of dairy products in Mexico.
- Counsel to several clients in litigious actions with the Administrative Authorities and Federal Courts.
- Counsel to several clients on data privacy matters in order to align their legal structure to the specific provisions of the recently enacted Mexican Data Privacy Law.

Languages. Spanish, English

Professional associations/memberships. International Trademark Association (INTA); Mexican Association for the Protection of Intellectual Property (AMPPI).

Publications. *MCI can look but not touch, World Intellectual Property Review, July/August, 2013*, article on amendments to the Mexican Copyright Law.