Mexico

Gustavo A Alcocer and Abraham Díaz Arceo
Olivares

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legal framework for PII protection is found in article 6 of the Mexican Constitution; and in the Federal Law for the Protection of Personal Data Held by Private Parties, published in July 2010, its Regulations, published in December 2011, the Privacy Notice Rules, published in January 2013, the Binding Self-Regulation Parameters, also published in January 2013 and May 2014, and the General Law for the Protection of Personal Data Held by Public Governmental Entities, published in January 2017. Mexican PII protection law is not based exclusively on an international instrument on data protection, but instead follows international correlative laws, directives and statutes, and thus has similar principles, regulation scope and provisions.

The Federal Law for the Protection of Personal Data (the Law) regulates the collection, storage, use and transfer of PII and protects individual data subjects (individuals); it is a federal law of public order, which makes its provisions applicable and enforceable at a federal level across the country and is not waivable under any agreement or covenant between parties, since it is considered to be a human right. This Law regulates the use and processing given to the PII by PII data controllers (PII controllers) and PII processors, thus providing several rights to individuals and obligations to PII controllers and PII processors, in order to ensure the privacy and confidentiality of such information. The Privacy Notice Rules comprise the requirements for such notices, whereas the Binding Self-Regulation Parameters contain the requirements and eligibility parameters to be considered by the authority for approval, supervision and control of self-regulation schemes, and authorisation and revocation of certifying entities as approved certifiers.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is the authority responsible for overseeing the Law. Its main purpose is the disclosure of governmental activities, budgets and overall public information, as well as the protection of personal data and individuals' right to privacy. The INAI has the authority to conduct investigations, review and sanction PII controllers and PII processors, and authorise, oversee and revoke certifying entities.

The Ministry of Economy is responsible for informing and educating on the obligations regarding the protection of personal data between national and international corporations with commercial activities in Mexican territory. Among other responsibilities, it must issue the relevant guidelines for the content and scope of the privacy notice in cooperation with the INAI.

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Administrative sanctions are provided for violations to the Law from 100 to 320,000 times the minimum general daily wage applicable in Mexico City (MGDW) for PII controllers and PII processors, depending on the seriousness of the breach and specific behaviour and conduct that may lead to criminal penalties is sanctioned from three months' and up to five years' imprisonment, depending on the seriousness of the breach (profit-making with PII or the methods used to get consent for the use of the PII) and the nature of the PII (penalties are doubled if the personal data is considered by law as sensitive personal data).

In addition, related conduct may be sanctioned under the Criminal Code, such as professional secrecy breaches and illegal access to media systems and equipment.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Law applies to non-public individuals and entities that handle PII. In addition, the following non-public persons and entities are excluded from the application of the Law:

- credit information bureaux or companies, where such companies are specially regulated by the Law for the Regulation of Credit Information Companies; and
- persons who handle and store PII exclusively for personal use and without any commercial or disclosure purposes.

Also, from January 2017, the Law for the Protection of Personal Data Held by Public Governmental Entities applies to any authority, entity, body or organism of the executive, legislative and judicial powers of the government, autonomous entities, political parties, trusts and public funds, at federal, state and municipal levels.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Law covers PII regardless of the means or media where such data is stored, processed or organised (whether physical or electronic); however, there is no regulation regarding the unauthorised interception of communication (as it would relate to surveillance or espionage), electronic marketing or surveillance of individuals. In this regard, such matters as illegal access to media, systems and equipment could be covered by criminal law.

- Article 166-bis of the Federal Criminal Code sanctions with imprisonment from three months to up to three years the person who in virtue of his or her position in a telecommunications company,

unlawfully provides information regarding people using the said telecommunication services.
- Article 177 of the Federal Criminal Code sanctions with imprisonment from six to 12 years, and a fine up to 600 MGDW, the person who intervenes in any private communication without a judicial order issued by a competent authority.
- Article 211-bis of the Federal Criminal Code sanctions with imprisonment from six to 12 years, and a fine up to 600 MGDW, the person who reveals, divulges or improperly uses any information or images obtained from the intervention of a private communication.
- Article 36 of the Federal Law for Consumers' Protection sanctions the publication in any mass media of any notice addressed undoubtedly to one or various specific consumers, with the aim of collecting a debt from them, or having them comply with an agreement.
- Article 76-bis of the Federal Law for Consumers' Protection recognises as a consumer's right in transactions effected through electronic, optic or other technologic means, that the supplier of a commodity or service uses the information provided by the consumer in a confidential manner, and consequently said information cannot be transmitted to other different suppliers, unless consented by the consumer or ordered by competent authorities.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Along with other laws already pointed out herein, such as the Criminal Code, the Law for the Regulation of Credit Information Companies and the Law for the Protection of Personal Data Held by Public Governmental Entities, there is additional legislation covering specific data protection rules, such as the Civil Code and the Code of Commerce.

7 PII formats

What forms of PII are covered by the law?

As previously noted, the Law covers PII regardless of the means or media used for its storage, process or organisation. Such means or formats include:
- digital environment (hardware, software, web, media, applications, services or any other information-related technology that allows data exchange or processing; among these formats, the Law specifically includes PII stored in the cloud);
- electronic support (storage that can be accessed only by the use of electronic equipment that processes its contents in order to examine, modify or store the PII, including microfilm); and
- physical support (storage medium that does not require any device to process its content in order to examine, modify or store the PII or any plain sight intelligible storage medium).

8 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Mexican PII protection laws are not limited to PII controllers established or operating in Mexican territory. Although the Law does not provide a specific reach or scope of its applicability, the Regulations to the Law do. In this regard, such regulations (and, therefore, the Law), in addition to being applicable to companies established or operating under Mexican law (whether or not located in Mexican territory) apply to companies not established under Mexican law that are subject to Mexican legislation derived from the execution of a contract or under the terms of international law.

Additionally, Mexican regulations on PII protection apply: to company establishments located in Mexican territory; to persons or entities not established in Mexican territory but using means located in such territory, unless such means are used merely for transition purposes that do not imply a processing or handling of PII; and when the PII controller is not established in Mexican territory but the person designated as the party in charge of the control and management of its PII (a service provider) is.

In the case of individuals, the establishment will mean the location of the main place of business or location customarily used to perform their activities or their home.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?

Yes, all processing or use of PII is covered by the Mexican legal framework.

Mexican PII protection law makes a distinction between PII controllers and those who provide services to owners, where the latter are independent third parties who may be engaged by the PII controller in order to be the parties responsible for the PII processing and handling. While it is not mandatory to have this third-party service provider, should a company (PII controller) engage such services, it shall have a written agreement stating all the third party's responsibilities and limitations in connection with the PII.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The law provides eight main standards for the processing of PII:
- legality: PII controllers must always handle PII in accordance with the law. All personal data shall be lawfully collected and processed, and its collection shall not be made through unlawful or deceitful means;
- consent: PII controllers must obtain consent from individuals for the processing and disclosure of their PII. In this regard, consent of individuals shall not be required if:
  - PII is contained in publicly available sources;
  - PII cannot be associated with the individual, or if by way its structure or content cannot by associated with the individual;
  - PII processing is intended to fulfil obligations under a legal relationship between the PII controllers and individuals;
  - there exists an emergency situation in which the individual or its properties may be potentially damaged;
  - PII is essential for certain medical or health matters where the individual is unable to provide consent under applicable laws; or
  - a resolution is issued by a competent authority to process and disclose PII, without the required consent;
- information: PII controllers must notify the individual of the existence and main characteristics of the processing that will be given to the PII;
- quality: PII handled must be exact, complete, pertinent, correct and up to date for the purposes for which it has been collected;
- purpose ('finality principle'): PII may only be processed in order to fulfil the purpose or purposes stated in the privacy notice provided to the individual;
- loyalty: PII controllers must protect individuals' interests when handling their PII;
- proportionality: PII controllers may only handle the PII necessary for the purpose of the processing; and
- responsibility: PII controllers are responsible for the processing of the PII under their possession.

11 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

The law makes a distinction regarding 'sensitive' PII. This information is deemed the most personal of the individual, and if mistreated, could lead to discrimination or to general risk to the individual (i.e., racial or ethnic origin, present or future health status, genetic information, religion, political opinions, union membership or sexual orientation).

In view of this, the Law provides more stringent rules for the processing of this sensitive PII, such as the obligation for PII controllers to always get written and express consent from individuals for the

processing of their sensitive PII. Likewise, PII controllers may not hold sensitive PII without justified cause pursuant to the purpose of the processing.

Several additional limitations apply to the general handling of this type of information (eg, PII controllers must use their best efforts to limit the processing term of sensitive PII, the privacy notice must expressly point out the nature of such information when required; and, as previously pointed out, when it comes to penalties for the breach or mistreatment of PII, these may double when processing sensitive PII).

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The PII Controller must have a privacy notice available for all individuals whose data is in their possession or collected for use and processing. According to the Law and its Regulations, there are three types of privacy notices: an integral privacy notice; a simplified privacy notice; and a short privacy notice. The privacy notice must include, at least, the following information:

- the identity and address of the PII controller;
- PII that would be subject to processing;
- the purpose of the processing;
- the mechanisms provided by the PII controller to the individuals to limit the use or disclosure of the information;
- the means for individuals to exercise their rights to access, rectify, cancel or oppose the processing of their PII;
- any transfer of the PII to be made, if applicable;
- the procedure and vehicles in which the PII controller will notify individuals about modifications to the privacy notice;
- the procedure and means by which the PII controller should notify the individuals of any modification in such privacy notice; and
- regarding sensitive PII, the privacy notice shall expressly state that the information is of a sensitive nature.

In addition and pursuant to the privacy notice rules, the notice must take into account the following characteristics:

- inaccurate, ambiguous or vague phrases must not be used;
- the individual's profile must be taken into account;
- if an individual's consent is granted through tick marks in text boxes, these must not be pre-ticked; and
- reference to texts or documents not available to individuals must be omitted.

13 Exemption from notification

When is notice not required?

A privacy notice is not necessary when:

- exemption is available in a specific provision of applicable law;
- the data is available in public sources;
- PII data is subject to a prior dissociation procedure (anonymised data);
- there is an existing legal relationship between the individual and the PII controller;
- there is an emergency situation that could potentially harm an individual or his or her property;
- it is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the individual is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation; or
- a resolution is issued by a competent authority.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The Law provides individuals with 'ARCO' rights: to access (the right to know what information is being held and handled by the PII controller), rectify (the right to request at any time that the PII controller correct the PII that is incorrect or inaccurate), cancel (the right to request the PII controller to stop treating their PII) or oppose (the right to refuse) the processing of their PII.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

As discussed in question 10, PII has to fulfil the standard of quality (PII should be exact, complete, pertinent, correct and up to date).

Quality is presumed when PII is provided directly by the individual, and remains such until the individual does not express and prove otherwise, or if the PII controller has objective evidence to prove otherwise.

When personal data has not been obtained directly from the individual, the PII controller must take reasonable means to ensure the quality standard is maintained.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The Law provides a 'need to hold basis'; PII controllers must not hold PII any longer than the time required to fulfil its purpose (as stated in the privacy notice). After the purpose or purposes have been achieved, a PII controller must delete the data in its collection after blocking them for subsequent suppression.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

As discussed in question 10, the Law does provide a 'finality principle', whereby a PII controller is restricted to using the PII only in order to fulfil the purpose or purposes stated in the privacy notice provided to the individual, the purpose of which must comply with the legality standard. If the PII controller intends to process data for other purposes that are not compatible with, or similar to, the purposes set out in the privacy notice, an individual's consent must be collected again for such purposes.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The PII controller is not allowed to use PII for any purposes other than that authorised or notified to the individual, unless such new purpose is authorised by or notified to (in such cases where express authorisation is not required) the individual, or unless such use is explicitly authorised by law or regulation.

Security

19 Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

PII controllers or entities in charge of processing PII must take and observe various security measures for the protection of the PII, including administrative, physical and technical measures.

Administrative measures must be taken, such as actions and mechanisms for the management, support and review of the security in the information on an organisational level, the identification and classification of the information, as well as the formation and training of the personnel, in matters of PII.

In addition, certain physical measures such as actions and mechanisms – technological or otherwise – designed to prevent unauthorised access, damage or interference to the physical facilities, organisational critical areas equipment and information, or to protect mobile, portable or easy to remove equipment within or outside the facilities.

Technological measures must also be taken, including controls or mechanisms, with measurable results, that ensure that:

- access to the databases or to the information is by authorised personnel only;
- the aforementioned access is only in compliance with authorised personnel's required activities in accordance with his or her duties;
- actions are included to acquire, handle, develop and maintain safety on the systems; and
- there is correct administration on the communications and transactions of the technology resources used for the processing of PII.

Other actions that must be taken include:
- making an inventory on the PII and the systems used for its in processing;
- determining the duties and obligations of the people involved in the processing;
- conducting a personal data risk analysis (assessing possible hazards and risks to the PII of the company);
- establishing security measures applicable to PII;
- conducting an analysis for the identification of security measures already applied and those missing;
- making a work plan for the implementation of any security measures missing as a result of the aforementioned analysis;
- carrying out revisions and audits;
- training to the personnel in charge of the processing of PII; and
- maintaining a register of the PII databases.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

In accordance with the Law, PII controllers must notify individuals if any of their personal data is breached. Such notice must include:
- the nature of the incident;
- the personal data compromised;
- details to the individual of the measures that the PII controller may take to protect his or her interests;
- any corrective actions taking place immediately; and
- any means by which the individual may find more information on the subject.

In the case of a violation of PII, the PII controllers must analyse the causes of its occurrence and implement the corrective, preventive and improving actions to adapt the corresponding security measures to avoid the repetition of the violation.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

It is mandatory for the PII controller (or manager) to appoint an officer (person or department) in charge of the PII, who will be in charge of attending to and taking care of individual requests in order to exercise any of their rights provided by the Law. Likewise, this officer must promote the protection of PII within the company.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Although the Law does not specify record keeping as a mandatory requirement, as previously mentioned, it is recommended that PII controllers have a PII database, as well as a register on the means and systems used for the storage of those databases, in order to provide the maximum security for the PII under their possession or control.

Registration and notification

23 Registration

Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?

There is no need for PII controllers or processors to register with the INAI; however, the INAI has the authority to request a surprise inspection to monitor that PII controllers are complying with the Law and Regulations.

24 Formalities

What are the formalities for registration?

Not applicable.

25 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

27 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

In order to explain the regulations on transfer of PII, it must first be understood that the Law defines transfer of PII as the communication of PII to third parties, whether inside or outside Mexico, other than from the PII controller, the officer in charge or the service provider (PII controlling company), in which the third party has to comply with the provisions set forth in the privacy notice of the PII controller.

Transfer of PII to entities that provide PII processing services is not construed as a transfer of PII per se; therefore, any such transfer of PII will be the responsibility of the PII controller and, thus, the PII controller will be liable for any risk or breach in the PII information.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Any transfer of PII (as defined by the Law) must be made with the individual's consent, unless otherwise provided by Law (certain exceptions to consent apply). PII disclosure to other recipients must be made under the same conditions as it was received by the PII controller, so, in the case of such disclosure, the PII controller will be able to demonstrate that it was communicated under the conditions as the individual provided such PII. The original PII Controller always has that burden of proof in these cases.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The following transfers are allowed without restrictions:
- where the transfer is made pursuant to a law or treaty to which Mexico is party;

- where the transfer is necessary for medical diagnosis or prevention, healthcare delivery, medical treatment or health services management;
- where the transfer is made to holding companies, subsidiaries or affiliates under common control of the PII controller or to a parent company or any company of the same group as the PII controller operating under the same internal processes and policies;
- where the transfer is necessary pursuant to an agreement executed or to be executed in the interest of the individual between the PII controller and a third party;
- where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
- where the transfer is necessary for the recognition, exercise or defence of rights in a judicial process; and
- where the transfer is necessary to maintain or to comply with a legal relationship between the PII controller and the individual.

32 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

There is no mandatory notification or authorisation required from supervising authority. The Law only provides that the PII controller may, if it deems necessary, request an opinion from the INAI regarding the compliance of any international PII transfer with the Law.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Not applicable. Transfers outside the jurisdiction are not subject to restriction or authorisation.

Rights of individuals

34 Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Among the main rights of individuals (ARCO rights – see question 35) is the right to access a copy of the information being held and treated by the PII controller. This right may be limited for national security reasons, regulations on public order, public security and health or for the protection of third-party rights, and with the limitations provided in the applicable laws, or through a resolution of a competent authority.

35 Other rights

Do individuals have other substantive rights?

In addition to the right of access, as previously pointed out, the Law provides individuals with their ARCO rights: right to access, rectify, cancel (request the PII to stop treating their PII) or oppose (eg, refuse) the processing of their PII.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The INAI is entitled to declare neither damages nor compensations in favour of any individuals. Therefore the breach of any PII law does not automatically grant monetary damages or compensations to any PII owner.

It is important to mention that under Mexican legislation damages must be claimed and proven through a civil law action. In addition, injury to feelings can also be claimed as moral damage, but moral damages must also be claimed through a civil action before Mexican civil courts. This means that any PII owner has to prosecute first an administrative action before the INAI in order to prove the breach of the law, and after that, to initiate an independent civil law action, before civil courts, in order to collect any damages, or loses, or to claim any compensation derived from any moral damage.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights are exercisable by the INAI. The process is initiated either by a filing by an affected individual or directly by the INAI as a result of any anomalies found during a verification procedure.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Aside from the limitations and exclusions already described herein, the Law does not include any additional derogations, exclusions or limitations.

Supervision

39 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes. Since the INAI is an administrative authority, any of its resolutions can be challenged through a nullity trial before the Federal Court for Tax and Administrative Affairs, and later on through a Constitutional rights action known as Amparo suit.

Specific data processing

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The Law specifically refers to the use of PII in the cloud; the Law provides a list of requirements with which the third party providing these types of storage service must comply in order to ensure the safety of the PII to be uploaded therein.

Furthermore, when PII controllers use remote or local means of electronic communication, optical or other technology mechanisms, which allow them to collect PII automatically and simultaneously at the same time that individuals have contact with such PII, the individuals must be informed, through a communication or warning duly placed in a conspicuous location, with regard to the use of these technologies and the fact that PII has been collected, as well as the process to disable such access, except when the technology is required for technical purposes.

41 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The Law does not provide any specific rules on marketing by email, fax or telephone; nonetheless, any such contact with individuals is treated as PII and any marketing through those media will, therefore, be regulated in accordance with the Law.

42 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

Mexican law regulates the processing of PII in services, applications, and infrastructure in cloud computing. That is, the external provision of computer services on demand that involves the supply of infrastructure, platform, or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared. For these purposes, the data controller may resort to cloud computing by general contractual conditions or clauses.

These services may only be used when the provider:

- complies at least with the following:
  - has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;
  - makes transparent subcontracting that involves information about the service that is provided;
  - abstains from including conditions in providing the service that authorises or permits it to assume the ownership of the information about which the service is provided; and
  - maintains confidentiality with respect to the personal data for which it provides the service; and
- has mechanisms at least for:
  - disclosing changes in its privacy policies or conditions of the service it provides;
  - permitting the data controller to limit the type of processing of personal data for which it provides the service;
  - establishing and maintaining adequate security measures to protect the personal data for which it provides the service;
  - ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it; and
  - impeding access to personal data by those who do not have proper authority for access or in the event of a request duly made by a competent authority and informing data controller. In any case, the data controller may not use services that do not ensure the proper protection of PII.

The guidelines have not been issued yet to regulate the processing of PII in cloud computing.

Gustavo A Alcocer **gustavo.alcocer@olivares.mx**
Abraham Díaz Arceo **abraham.diaz@olivares.mx**

Pedro Luis Ogazón 17
Col. San Angel
01000 Mexico City
Mexico

Tel: +52 55 53 22 30 00
Fax: +52 55 53 22 30 01
www.olivares.com.mx