by Gustavo Alcocer and Paulina Villaseñor

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The legal framework for PII protection is found in the Federal Law for the Protection of Personal Data in Possession of Third Parties, published in July 2010, its Regulations, published in November 2011, the Privacy Notice Rules, published in January 2013, and the Binding Self-Regulation Parameters, also published in January 2013. Mexican PII protection law follows international correlative laws, directives and statutes, and thus has similar principles, regulation scope and provisions.

Mexican PII protection law (the Law) regulates the recollection, storage and use 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. This Law regulates the use and processing given to the PII by PII data controllers (PII owners), thus providing several rights to individuals and obligations to PII owners 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 powers of the authority.

The Federal Institute of Access to Information and Data Protection 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 the Individuals' right to privacy. The Data Protection Institute (IFAI) has the authority to conduct investigations, review and sanction PII owners, and authorise, oversee and revoke certifying entities.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

Although uncommon, the Law does provide certain serious breaches or behaviour and conduct type that may lead to criminal penalties from three months' up to 10 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 found penalised under the Criminal Code such as secret disclosure 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 only to non-public persons and entities that handle PII. In addition, the following non-public persons and entities are excluded from the application of the Law:

- credit information bureaus 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.

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 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.

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 and the Law for the Regulation of Credit Information Companies, there are 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 only accesses to by the use of electronic equipment that processes its contents in order to examine, modify or store the PII, including microfilms); and

- physical support (any plain sight intelligible storage medium).

8 Extraterritoriality

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

Mexican PII protection laws are not limited to PII owners 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: (i) 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 (ii) when the PII owner is not established in Mexican territory but the person designated as the party in charge of the control and management of its PII (service providers) is.

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 services to owners?

Mexican PII protection law makes a distinction between PII owners and those who provide services to owners, where this latter are independent third parties who may be engaged by the PII owner in order to be the parties responsible of the PII processing and handling. While it is not mandatory to have this third party service provider, should a company (PII owner) 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? Give details.

The law provides eight main standards for the processing of PII:

- Legality: PII owners must always handle PII in accordance with the law.

- Consent: PII owners must obtain consent from individuals for the processing of their PII (this standard has some exceptions).

- Information: PII owners 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.

- 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 owners must protect individuals' interests when handling their PII.

- Proportionality: PII owners may only handle the PII necessary for the purpose of the processing.

- Responsibility. PII owners are responsible for the processing of the PII under its possession.

11 Legitimate processing – types of data

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

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 (ie, present of future health issues or illnesses, genetic information, religion, political opinions or sexual orientation).

In view of this, the Law provides more stringent rules for the processing of these sensitive PII, such as the obligation for PII owners to always get written and express consent from individuals for the processing of their sensitive PII. Likewise, PII owners 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 owners 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 data they hold? What must the notice contain and when must it be provided?

The PII owner must have a privacy notice available for all individuals whose data is in their possession or collected for use and processing.

The privacy notice should contain at least the following information:

- the identity and address of PII owner;

- the purpose of the processing;

- the mechanisms provided by the PII owner in order for the individuals to limit the use or disclosure of the information;

- means for individuals to exercise their rights to access, rectify, cancel or oppose to the processing of their PII;

- any transfer of the PII to be made, if applicable;

- the procedure and means by which the PII owner should notify the individuals any modification in such privacy notice.

In addition and pursuant to the new Privacy Notice Rules, the notice must take into account the following characteristics:

- inaccurate, ambiguous or vague phrases must not be used;

- the individuals' profile must be taken into account;

- if an individuals' consent is granted through check marks in text boxes, these must not be pre-checked; and

- reference to texts or documents not available to individuals must be omitted.

13 Exemption from notification

When is notice not required (for example, where to give notice would be disproportionate or would undermine another public interest)?

A privacy notice is always required, but the law does provide certain compensatory means of mass communication for the notification to those individuals whose PII was treated prior to the enactment of the Law, and whose

personal notification may not be possible or would represent a disproportionate effort due to the number of individuals and the age of the information.

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: access (the right to know what information is being held and handled by the PII owner), rectify, cancel (the right to request the PII to stop treating their PII) or oppose (the right to refuse the processing of their PII) to the processing of their PII.

15 Data accuracy

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

As previously pointed out 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 owner has objective evidence to prove otherwise.

When personal data has not been obtained directly from the individual, the PII owner must take reasonably 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 owners must not hold PII any longer than the time required to fulfil its purpose (as pointed out in the privacy notice).

17 Finality principle

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

As pointed out in question 10, the Law does provide a 'finality principle', whereby a PII owner 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.

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 owner 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 obligations

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

PII owners 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.

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 the information is by authorised personnel only;
- the aforementioned access is only in compliance to 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 security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

PII owners 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 owner 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.

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

There is no need for PII owners or processors to register with the supervisor authority (IFAI); however, IFAI has the authority to request a surprise inspection to monitor that the PII owners 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 data owner or processor 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 owner, the officer in charge or the service provider (PII controlling company).

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 owner and, thus, the PII owner 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 owner, so in case of such disclosure, the PII owner will be able to demonstrate that it was communicated under the conditions as the individual provided such PII. The original PII owner always has that burden of proof in these cases.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Cross-border PII transfer is allowed as long as such transfer is made by written agreement (or similar) detailing all the conditions under which the PII owner received the PII, as well as a description of each party's obligations and the purpose of the transfer. The receiving party will be considered as the new PII owner.

32 Notification of transfer

Does 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 owner may, if it deems necessary, request an opinion from IFAI 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 see a copy of their personal information held by PII owners? Describe 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 owner. 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, law provides individuals with the ARCO rights: right to access, rectify, cancel (request the PII to stop treating their PII) or oppose (ie, 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?

Compensation for individuals is regulated in the Law, however, individuals could claim any damages on a case-by-case basis.

It is important to mention that under Mexican legislation damages must be proven; in addition, injury to feelings could be claimed as moral damage, but these cases are very difficult to prove.

37 Enforcement

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

The rights are exercisable by IFAI. The process is initiated either by a filing by an affected individual or directly by IFAI 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 data owners appeal against orders of the supervisory authority to the courts?

Any recourse or appeal against the supervisory authority's resolutions, are exercisable through the judicial system.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

When a person authorised to treat PII breaches the safety of the PII databases

under its charge in pursuit of profits, he or she is liable for between three months' and three years' imprisonment. When a person seeking unlawful profit treats PII in a deceitful manner, taking advantage of an error or mistake by the individual or the person authorised to transfer the PII, he or she is liable for between six months and five years in prison.

These penalties are doubled in case of sensitive PII.

41 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 with in order to ensure the safety of the PII to be uploaded therein.

Furthermore, when PII owners 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 this 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.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

The law does not provide any specific rules on marketing by e-mail, 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.

Source Getting the Deal Through: Data Protection & Privacy 2014