Mexico

Abraham Diaz, Gustavo A Alcocer and Carla Huitrón
OLIVARES

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legal framework for PI protection is found in:

- article 6 of the Mexican Constitution:
- the Federal Law for the Protection of Personal Information Held by Private Entities, published in July 2010, and its Regulations published in December 2011;
- the Privacy Notice Rules, published in January 2013;
- the Binding Self-Regulation Parameters, 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 PI 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 PI and protects individual data subjects' (individuals) rights. It is a federal law of public order that makes its provisions applicable and enforceable at the 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. The Law regulates the use and processing given to the PI by PI data controllers (PI controllers) and PI processors, thus providing several rights to individuals and obligations to PI controllers and PI processors, to ensure privacy, security 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. Since June 2018, Mexico has been a member of the Convention for the Protection of Individuals Concerning the Automated Processing of Personal Data, and its Protocol (Convention 108).

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is the data protection authority responsible for overseeing the Law. Its main purpose is the disclosure of government 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 PI controllers and PI 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.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Since the Federal Law for the Protection of Personal Information Held by Private Entities proposed a centralised model of protection of PI instead of a sectorial model, the INAI is the only data protection authority in charge of the protection of personal information.

Further, section VII of article 38 of the Federal Law for the Protection of Personal Information Held by Private Entities sets forth as a general obligation of the INAI: 'To cooperate with other supervising authorities and national and international entities, to help in the protection of personal information.'

Likewise, article 40 of the Federal Law for the Protection of Personal Information Held by Private Entities makes clear that this law constitutes the legal framework that any other authorities must observe when issuing any regulations that may imply the processing of PI, and said regulations must be issued in coordination with the INAI. This obligation is also included in articles 77 and 78 of the Regulations of the Federal Law for the Protection of Personal Information Held by Private Entities.

Breaches of data protection law

4 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 for PI controllers and PI processors. Depending on the seriousness of the breach and specific behaviour and conduct (profit-making with PI or the methods used to get consent for the use of PI), it may lead to criminal penalties, which are sanctioned with between three months and five years of imprisonment. This also depends on the nature of the PI (penalties are doubled if the personal data is considered by law as sensitive personal data).

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

1.5 Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

Yes, as this is an administrative procedure, PI owners have two options to appeal an order issued by the data protection authority:

- A remedy claim: this is filed before the same authority that issued the order.
- A nullity trial: this is filed before the Federal Court of Administrative Affairs (FCA), whether appealing the first order issued by the data protection authority or the resolution of the remedy claim. If the resolution issued by the FCA is not satisfactory, it can further be challenged by starting a procedure with the federal circuit courts by the affected party, through an *amparo* lawsuit (a constitutional legal remedy).

SCOPE

Exempt sectors and institutions

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

The Federal Law for the Protection of Personal Data (the Law) applies to non-public individuals and entities that handle PI. Also, the following non-public persons and entities are excluded from the application of the Law:

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

Also, as from January 2017, the General 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.

Interception of communications and surveillance laws

7 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Law covers PI 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 communications (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, including:

- article 166-bis of the Federal Criminal Code sanctions with imprisonment from three months to up to three years, for 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 the minimum general daily wage (MGDW), for 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, for the person who reveals, divulges or improperly uses any information or images obtained from the intervention of 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, to collect a debt from them or have them comply with an agreement; and
- 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 confidentially provided by the consumer, and consequently said information cannot be transmitted to other different suppliers unless consented by the consumer or ordered by competent authorities.

Other laws

8 | Are there 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. However, to date, Mexico does not count on specific and express rules for data protection in connection with employee monitoring, e-health records or the use of social media.

In the case of e-health records, there are some specific regulations for the creation and handling thereof. However, concerning the protection of PI, there is a referral to the rules outlined in the Federal Law for the Protection of Personal Information Held by Private Parties, its Regulations, and the General Law for the Protection of Personal Data Held by Public Governmental Entities (the latter in the case of e-health records for the public sector).

Additionally, in January 2021, an amendment to the Federal Labour Law was published and set into force, establishing a general law framework for the regulation of telework. Although this law framework refers to the rules set forth in the Federal Law for the Protection of Personal Information Held by Private Entities, it introduces some rules that must be observed by employers and employees, when operating in telework mode.

PI formats

9 | What categories and types of PI are covered by the law?

The Law covers all types of PI; however, for clarity purposes, the authority divides the PI into the following categories:

- PI:
  - identification data;
  - academic data;
  - transit data and migratory movements;
  - labour data;
  - patrimonial data; and
  - data on administrative and/or judicial procedures; and
- sensitive PI:
  - data on people's health;
  - electronic data;
  - ideological data;
  - biometric data;
  - sexual Life data; and

- ethnic data.

Likewise, the Law covers PI regardless of the means or media used for its storage, process or organisation. Such means or formats include:

- digital formats (eg, 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 PI stored in the cloud);
- electronic support (ie, storage that can be accessed only by the use of electronic equipment that processes its contents to examine, modify or store the PI, including microfilm); and
- physical support (ie, storage media that does not require any device to process its content to examine, modify or store the PI or any plain sight intelligible storage medium).

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors of physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Mexican PI protection laws are not limited to PI 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 applying 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 PI protection apply:

- to companies' 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 PI; and
- when the PI controller is not established in Mexican territory, but the person designated as the party in charge of the control and management of its PI (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.

Covered uses of PI

11 | Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

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

By virtue of this obligation of PI controllers to execute an agreement with any PI processor they use, the duties acquired by the PI processor must be the same as those imposed by the Law on the PI controller.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 | Does the law require that the processing of PI 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 PI:

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

Legitimate processing – types of PI

13 | Does the law impose more stringent rules for processing specific categories and types of PI?

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

Given this, the Federal Law for the Protection of Personal Data provides more stringent rules for the processing of this sensitive PI, such as the obligation for PI controllers to always get written and express consent from individuals for the processing of their sensitive PI. Likewise, PI controllers may not hold sensitive PI without justified cause pursuant to the purpose of the processing.

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

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 | Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The PI 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 Federal Law for the Protection of Personal Data (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 PI controller;
- PI that would be subject to processing;
- the purpose of the processing;
- the mechanisms provided by the PI 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 PI;
- any transfer of the PI to be made, if applicable;
- the procedure and vehicles in which the PI controller will notify individuals about modifications to the privacy notice;
- the procedure and means by which the PI controller should notify the individuals of any modification in such privacy notice; and
- regarding sensitive PI, the privacy notice must 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.

Exemptions from transparency obligations

15 | When is notice not required?

A privacy notice is not necessary when:

- the exemption is available in a specific provision of applicable law;
- the data is available in public sources;
- PI data is subject to a prior dissociation procedure (anonymised data);
- there is an existing legal relationship between the individual and the PI 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.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PI?

Personal information has to fulfil the standard of quality (PI should be exact, complete, pertinent, correct and up to date).

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

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

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

Yes, in accordance with the regulation of the Law, only the PI that is necessary, appropriate, relevant and non-excessive in connection with the purposes for which they were obtained may be processed. Therefore, the PI controller must take reasonable efforts to limit the PI processed to the minimum necessary.

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

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

Purpose limitation

19 | Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the Law does provide a 'finality principle', whereby a PI controller is restricted to using the PI only to fulfil the purpose or purposes stated in the privacy notice provided to the individuals, the purpose of which must comply with the legality standard. If the PI 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 additional purposes.

The PI controller is not allowed to use PI 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.

Automated decision-making

20 | Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

When PI is processed as part of a decision-making process without the intervention of an individual, the PI controller must inform the data subject of this prior to carrying out the process.

Furthermore, as a good practice, the privacy notice may inform the data subject that their PI will be treated as part of an automated decision-making process, explaining the characteristics of the respective process.

SECURITY

Security obligations

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

PI controllers or entities in charge of processing PI must take and observe various security measures for the protection of the PI, 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 PI.

Also, certain physical measures such as actions and mechanisms – technological or otherwise – are 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 with authorised personnel's required activities according to 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 PI.

Other actions that must be taken include:

- making an inventory of the PI and the systems used for its 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 PI of the company);
- establishing security measures applicable to PI;
- analysing 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 PI; and
- maintaining a register of the PI databases.

Notification of data breach

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

A data breach occurs when data subjects suffer harm or damage to their property or rights because of the PI controller's or processor's non-compliance with any of the provisions stated in the Federal Law for the Protection of Personal Data (the Law).

Under the Law, PI 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 on the actions that the individual may adopt to protect his or her interests;
- any corrective actions taking place immediately; and
- any means by which the individuals may find more information on the subject.

In the case of a violation of PI, the PI 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.

However, to date, Mexican law does not include an obligation for private PI controllers to notify the supervisory authority. Although not required by law, the Mexican data protection authority does, however, recommend the issuing of notices in the event of any data breaches.

Government agencies are obliged to notify the National Institute of Transparency, Access to Information and Personal Data Protection of any data breaches.

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Yes, all responsible parties that process PI must establish and maintain physical and technical administrative security measures designed to protect PI from damage, loss, alteration, destruction or unauthorised use, access or processing. They must not adopt security measures inferior to those they keep managing their own information. Moreover, factors such as the risk involved, potential consequences for the data subjects, sensitivity of the data and technological development should be considered.

Administrative security measures

A set of actions and mechanisms should be established to manage, support and review information security at an organisational level, to identify and classify information, and to raise awareness for, educate and train personnel in the protection of PI.

Physical security measures

These include a set of actions and mechanisms, whether they use the technology, intended to protect the PI collected.

Technical security measures

These include a set of activities, controls or mechanisms, which produce measurable results, that use technology to ensure the protection of the PI collected.

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There are no criteria stated in the Law that require the appointment of a data protection officer. However, as good practice, the controller should always look to appoint a certified data protection officer who has a certain level of knowledge in PI matters and establish any other desired criteria in the agreement that they will execute.

It is mandatory for the PI controller (or manager) to appoint an officer (person or department) in charge of the PI, who will be in charge of attending to and taking care of individuals' requests to exercise any of their rights provided by the Federal Law for the Protection of Personal

Data (the Law). Likewise, this officer must promote the protection of PI within the company.

Record-keeping

25 | Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Although the Law does not specify record keeping as a mandatory requirement, it is recommended that PI controllers have a PI database, as well as a register on the means and systems used for the storage of those databases to provide the maximum security for the PI under their possession or control. Likewise, it is suggested to keep records as to the consents obtained from individuals for the collecting and processing of their PI.

Risk assessment

26 | Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

No, the Law does not impose owners or processors of PI to carry out a risk assessment in relation to the use of certain PI. However, PI controllers must carry out privacy impact assessments to determine the security measures to be adopted, as outlined in articles 60 and 61 of the Regulations of the Federal Law for the Protection of Personal Information Held by Private Entities.

Design of PI processing systems

27 | Are there any obligations in relation to how PI processing systems must be designed?

No, the Law does not yet include obligations on how PI processing systems must be designed.

REGISTRATION AND NOTIFICATION

Registration

28 | Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no need for PI controllers or processors to register with the National Institute of Transparency, Access to Information and Personal Data Protection (INAI); however, the INAI has the authority to request a surprise inspection to monitor that PI controllers are complying with the Federal Law for the Protection of Personal Data and Regulations.

Registration with the Mexican data protection authorities is neither required by law nor mandatory.

Other transparency duties

29 | Are there any other public transparency duties?

No other public transparency duties are imposed on PI controllers.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

To explain the regulations on transfer of PI, it must first be understood that the Federal Law for the Protection of Personal Data (the Law) defines the transfer of PI as the communication of PI to third parties, whether they are located in Mexico or abroad, other than the PI controller (PI controlling company), in which the third party has to comply with the provisions outlined in the privacy notice of the PI controller.

The transfer of PI to entities that provide PI processing services is not construed as a transfer of PI per se; therefore, any such transfer of PI will be the responsibility of the PI controller and, thus, the PI controller will be liable for any risk or breach in the PI information, which is why it is mandatory to regulate business relationships with PI processors and vendors through the execution of agreements, under which PI processors acquire the same obligations and duties as PI controllers.

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

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

As the Law expressly provides that the collecting or processing of any PI has to be through lawful means, the selling or purchasing of PI (marketing lists for advertising purposes), including any PI not collected in accordance with Mexican law, would be deemed illegal. If the marketing list includes only business contact information or publicly available information, then it can be used, and it is always recommended to provide recipients of emails sent for marketing purposes with a mechanism that allows easy opting out from the marketing service.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

The following transfers outside the jurisdiction are allowed without restrictions:

- where the transfer is made pursuant to a law or treaty to which Mexico is a 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 PI controller or to a parent company or any company of the same group as the PI 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 PI 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 PI controller and the individual.

Further transfer

33 | 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 neither subject to restriction nor authorisation.

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no express provision in Mexican law ordering that a copy of PI be retained in the Mexican jurisdiction when such PI is transferred outside the country; however, the controller who transfers such PI outside the jurisdiction may keep the PI exclusively for the purposes of the responsibilities regarding their treatment.

RIGHTS OF INDIVIDUALS

Access

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

Among the main rights of individuals (the right of access, rectification, cancellation and opposition) of the holders on their personal data rights (the rights to access, rectify cancel (request the PI to stop treating their PI) or oppose (ie, refuse) the processing of their PI) is the right to access a copy of the information being held and treated by the PI 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.

Other rights

36 Do individuals have other substantive rights?

At any time, the data owner may withdraw his or her consent for the treatment of his or her PI. The controller must establish simple and free mechanisms that allow data subjects to withdraw their consent at least by the same means by which they granted it.

Compensation

37 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 National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is entitled to declare neither damages nor compensations in favour of any individuals. Therefore, the breach of any PI law does not automatically grant monetary damages or compensation to any PI owner.

Under Mexican legislation, damages must be claimed and proven through a civil law action. Also, injury to feelings can be claimed as moral damage, but moral damages must also be claimed through a civil action before Mexican civil courts. This means that any PI owner has to prosecute first an administrative action before the INAI to prove the breach of the law, and after obtaining a final decision declaring the administrative infringement, it may initiate an independent civil law action, before civil courts to collect any damages, or loses, or to claim any compensation derived from any moral damage.

Enforcement

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

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

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 Does the law include any derogations, exclusions or limitations other than those already described?

Aside from the limitations and exclusions already described herein, the Federal Law for the Protection of Personal Data does not include any additional derogations, exclusions or limitations.

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 Are there any rules on the use of 'cookies' or equivalent technology?

The Federal Law for the Protection of Personal Data (the Law) specifically refers to the use of PI in the cloud; the Law provides a list of requirements any third party providing these types of storage service must comply with to ensure the safety of the PI to be uploaded therein.

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

Electronic communications marketing

41 Are there any rules on marketing by email, fax telephone or other electronic channels?

The Law does not provide any specific rules on marketing by email, fax, telephone or other electronic channels; nonetheless, any such contact with individuals is treated as PI and any marketing through those media will, therefore, be regulated according to the Law.

Targeted advertising

42 Are there any rules on targeted online advertising?

All advertising that is directed to consumers in Mexico is governed by the Federal Consumer Protection Law;, there are no specific regulations for targeted online advertising (online behavioural advertising), but the Federal Bureau for Consumer Protection operates a call-blocking registry, covering landlines and mobile phone numbers, which gives suppliers making advertising calls and sending advertising messages 30 days to stop disturbing the consumer at his or her registered address or electronic address or by any other means.

Likewise, all the advertising purposes must be specified clearly in the privacy notice, and the owner's consent is required.

Sensitive personal information

43 Are there any rules on the processing of 'sensitive' categories of personal information?

The Law describes as sensitive PI any PI that may affect the most intimate sphere of an individual, or that which, if misused, may lead to discrimination or carry a serious risk to the individual. In particular,

sensitive personal information is considered that which may reveal information such as ethnic or racial origin, a present or future medical condition, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions and sexual preference.

Express and written consent is required from the PI's owner for its treatment. No database with sensitive PI may be created without a legitimate justification, and they must be created in accordance with the explicit purposes of the controller.

Databases containing sensitive PI may only be created if:

- they obey to a legal mandate;
- it is justified for national security matters, public order, public security and public health, as well as to protect the rights of third parties; or
- the controller requires it for legitimate, concrete purposes and in accordance with his or her explicit purposes.

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules on individual profiling; however, if such automated processing results in personal data or information that may identify an individual, such activity will be subject to the Law, in which case the controller will be responsible under the Law.

Further, such advertising purpose will have to be clearly specified in the privacy notice, and the owner's consent will be required.

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Mexican law regulates the processing of PI 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 flexibly, 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;
- maintains confidentiality concerning 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 authorisation 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 PI.

No guidelines have yet been issued to regulate the processing of PI in cloud computing.

OLIVARES®
we know
MEXICO

Abraham Díaz Arceo
abraham.diaz@olivares.mx

Gustavo A Alcocer
gustavo.alcocer@olivares.mx

Carla Huitrón
Carla.huitron@olivares.mx

Pedro Luis Ogazón 17
San Angel
01000
Mexico City
Mexico
Tel: +52 55 5322 3000
Fax: +52 55 5322 3001
www.olivares.com.mx

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

On 16 April 2021, an amendment to the Federal Telecommunications and Broadcasting Law was published in the Official Gazette, aimed at the creation of a national registry of mobile phone users, through which it is intended to create a database with information on individuals or legal entities who own mobile phones.

The registration of mobile phone numbers, including all of the aforementioned requirements, was mandatory for all users of mobile phones in Mexico, and the telecommunications concessionaires would be responsible for collecting and updating or modifying the users' information, which will be available for Mexican competent authorities.

This reform caused alarm among specialists in the field, as well as among users in general, due to the lack of security observed in the past in the handling of personal data by the government, as well as the disproportionate demands it places on mobile phone users, forcing them to reveal sensitive data such as biometric data, in contravention to international trends.

The Mexican data protection authority (the National Institute of Transparency, Access to Information and Personal Data Protection (INAI)) filed a legal action denouncing the unconstitutionality and illegality of this amendment and, in May 2022, the Mexican Supreme Court of Justice ruled that the action filed by INAI was legally grounded, thus declaring as illegal the creation of the above-mentioned registry. This decision is final.

As to initiatives aimed at the proper management of PI during the covid-19 pandemic, there was no emergency legislation in Mexico,

and the relief programmes observed in the Mexican government were focused on enhancing the awareness of the value of PI among PI owners, so that they were more careful when sharing their PI, amidst a very relevant booming in the use of e-commerce platforms. INAI was very active in spreading official communications teaching PI owners as to how to safeguard one's PI. Likewise, INAI was heavily focused on enhancing its technological tools so that PI owners could exercise its rights though electronic means and data controllers and data processors could receive any legal assessment and consultation from INAI through such electronic means.

Finally, INAI was very active in keeping surveillance on the proper collecting and processing of PI by data controllers and data processors, and initiated a relevant number of proceedings and imposed a significant number of relevant sanctions against private and public entities who were found in default of the obligations set forth in Mexican law.