This country-specific Q&A provides an overview of data protection & cyber security law laws and regulations applicable in Mexico.

For a full list of jurisdictional Q&As visit legal500.com/guides
1. Please provide an overview of the legal and regulatory framework governing data protection and privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

In Mexico, the protection of personal data is a fundamental right recognized by the Federal Constitution (articles 6 paragraphs II, and 16 paragraph II).

In the public sector, the law that governs the protection of personal data in Mexico is the General Law on Protection of Personal Data held by Obliged Subjects (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados), published in the Official Gazette on January 26, 2017, as well as local laws addressing the subject within each state of the Mexican Republic.

In the private sector, the law that governs the protection of personal data in Mexico is the Federal Law on Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (‘the Law’) – which was published in the Official Gazette on July 5, 2010. Secondary legislation supplements the Law. This includes the Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (‘the Regulations’), and the Guidelines of the Privacy Notice (Lineamientos del Aviso de Privacidad) (the Guidelines), which were published in the Federal Official Gazette on December 21, 2011, and January 17, 2013, respectively. All individuals and legal entities in the private sector that are involved in the processing of personal data are governed by the aforementioned legislation. However, credit reporting companies and individuals who collect and process personal data exclusively for personal use are exempt from these rules.

The authority in charge of data protection enforcement is the National Institute for Access to Public Information and Personal Data Protection (‘INAI’). The INAI is an autonomous body responsible for promoting and disseminating the right to access public information, and the right to data protection within governmental agencies and private parties. This body is committed to working with other federal, state and municipal authorities in order to promote data protection in different industries and sectors, such as the financial, educational and health sectors.

This article will focus on the legislation applicable in the private sector.

In the Congress, there are several bills to amend the Law, however it is uncertain when they will be discussed and approved.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

No, there are no licensing requirements for entities covered by the Data Protection Law.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?
4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII only be kept for a certain period? Please outline any such principles or “fair information practice principles” in detail.

- Legality: this means that all processing of personal data must be carried out in compliance with all applicable laws.
- Consent: processing of personal data requires the data subject’s consent, unless such processing falls under one of the exceptions specifically established in the Law. Some of the exceptions to consent are a) where the personal data is contained in publicly available sources; b) where the personal data is anonymized; c) where the personal data is processed for the purpose of fulfilling obligations under a legal relationship between the data subject and the data controller; among others.
- Information: the data controller must communicate to the data subject, through the privacy notice, information related to the main characteristics of the data processing.
- Data Quality: personal data being processed must be correct, complete, relevant and up to date, in order to achieve the purposes for which it is being processed.
- Purpose Specification: personal data may only be processed in connection with clearly defined and legitimate objectives, as mentioned in the privacy notice made available to data subjects.
- Loyalty: the data controller must protect the interests of the data subject and his/her reasonable expectation of privacy. Misleading or deceptive means must never be used to collect and process personal data.
- Proportionality: Processing of personal data is only permissible where it is necessary, appropriate, relevant and not excessive in connection with the purposes for which personal data was obtained. In addition, a data controller is obliged to make reasonable efforts to limit the personal data being processed to the minimum necessary.
- Accountability: The data controller is responsible for verifying that any processing of personal data both where it is held directly, and where it has been communicated to a data processor, is conducted fully in accordance with the applicable regulations.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

As stated above, the general rule is that consent is necessary to process personal data, unless one of the exceptions provided by the Law applies.

6. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing?
operations)?

Implicit consent will be considered valid, however in certain circumstances, the Law does require explicit or explicit and written consent. Explicit consent is required where the data being processed is of a financial or economic nature. Any information relating to economic assessment of an individual such as, tax information, credit history, income and expenses, bank accounts, insurance, bonds, credit card numbers, security numbers and real property is viewed as financial or economic data.

Verbal and written communication is sufficient to constitute explicit consent, as are communications by electronic or optical means or via any other technology or by unmistakable indications. Explicit written consent is required for the processing of sensitive personal data, and may be obtained through the data subject’s signature, electronic signature or any authentication mechanism established for such purpose. The data controller will always be responsible for producing evidence showing that the required consent was obtained.

In practice, consent when it is express and written consent required it is usually collected in the same document as the relevant Privacy Notice.

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

To process personal data, it is necessary to obtain explicit written consent (see details above). The data controller must make reasonable efforts to limit the period of processing to the minimum necessary.

8. How do the laws in your jurisdiction address children's personal data or PII?

The Law does not include specific provisions addressing children’s personal data. However, following provisions of the Civil Code, parental consent is required to process personal data from children under 18 years.

The General Law on Children’s and Adolescent’s Rights address the need to protect these groups’ personal data, especially on media.

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

As mentioned above, the Law does not apply to credit reporting companies and individuals who collect and process personal data exclusively for personal use.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

Article 48 paragraph V of the Regulations determine that the data controller must adopt measures to guarantee the proper processing of personal data, giving priority to the interests of the data subject and the reasonable expectation of privacy. The measures that may be adopted by the data controller include the implementation of a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies, and business models, as well as to mitigate them.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

In accordance with the Data Protection Law, all Companies (data controllers) processing personal data must adopt and maintain physical, technical, and administrative security measures which have been designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. Data controllers must also adopt security measures that are at least equivalent to those adopted in the management of their own information. In adopting such security measures, the data controller must consider the risks involved, any potential consequences to the data subjects if there is a security breach, the nature of the data and technological development.

The Provisions suggests establishing, among others, the following security measures: (i) prepare an inventory of the personal data being processed, the means for storing such data and the systems used for its processing; (ii) determine the functions and obligations,
in relation to the protection of the personal data, of each of the persons involved in their processing; (iii) train people involved in the processing of the personal data transferred; (iv) perform a risk assessment; (v) identify missing security measures; (vi) perform regular reviews or audits; (vii) record the means of storing personal data; (viii) elaborate a document regarding the security measures established; and (ix) establish measures for the traceability of personal data (i.e., actions, measures and technical procedures that allow tracking the personal data during its processing).

The data controller must also keep the security measures under constant review, specifically updating them when the following events occur:

- The security measures or processes are modified for their continuous improvement, derived from the revisions to the security policy of the data controller;
- Substantial modifications are produced in the data processing that derive in a change of the risk level;
- The data processing systems are violated, or
- There is an affection to the personal data different to the previous ones.

Have incident response plan, identify the security measures violated, have an improvement plan and update these measures.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

The data protection law, under the accountability principle, mentioned previously, it is necessary to have in place policies and procedures necessary for ensuring the correct and legal data processing, among those could be the data retention and disposal policies; however, the law does not specify on each of the policy that a data controller must have. The Data protection authority has issued guidelines in this regard.

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

It is not required to consult with data privacy regulators.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

According to the Regulations, the data controller should consider conducting risk assessments to identify threats and estimate risks to the personal data. The Regulations do not specify under which circumstances it is recommended to conduct risk assessments.

The INAI has published different guidelines and recommendations on security measures, risk analysis, etc:

Recommendations for recognizing the main threats to personal data based on risk assessment. Available only in Spanish here.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

Yes, it is required to appoint a data protection officer. The data protection officer must be in charge, mainly, of promoting the protection of personal data within the organization and responding to the requests of the data subjects related to their Access, Rectification, Cancellation and Opposition (“ARCO”) rights.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

Data controllers or processors with personal data processing among the security measures they must adopt to protect that personal from misusage, alteration etc... are the necessary and adequate administrative measures. These measures include the training of staff or personal with responsibilities connected with the personal data must, courses on raise awareness. However as previously stated the Law does not specify on the training requirements.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice
requirements (e.g., posting an online privacy notice).

It is necessary to provide a privacy notice, complying with the Law, to the data subjects prior to the collection of their personal data. If the personal data is collected through a data transfer or public source (i.e. indirectly), the data subjects must be provided with a privacy notice at the first contact or before using the personal data.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data, and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

Data controllers are defined as the individuals or legal entities that decide on the processing of personal data. On the other hand, data processors are individuals or legal entities which alone or jointly with others process personal data on behalf of the data controller. The Law governs the processing of personal data by controllers, and only imposes a few obligations on processors, such as the obligation to process the data under the instructions of the controller and establish security measures, among others. It is possible to impose other obligations on processors, but this shall be done on a contractual basis.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

It is required to execute a data processing agreement complying with the Law.

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

**Monitoring.** In general, video surveillance or monitoring is permitted in the workplace if it complies with the Federal Constitution principles, and with labour and data protection laws, also some States has specific laws regulating video surveillance as well in certain workplaces.

CCTV monitoring should be done under previous notice, for specific purposes, like safety or prevention and prosecution of criminal acts or of administrative infractions, in compliance with fundamental right to data protection. Cameras should be placed in public spaces and consider the principles of proportionality, suitability and minimum intervention; the video surveillance system cannot be used to take pictures and sounds inside private properties, unless consented by the data subject or with judicial authorization.

The INAI in 2013 published practical recommendations for those who perform or want to perform monitoring, considering balance between the right of honour, data protection and privacy, but also the rights of companies to protect their information against cyberattacks, money laundering or anti-corruption practices.

In 2015, there was an approach to regulate this matter in a federal level, but the initiative was withdrawn in 2018.

Criminal courts issued a mandatory criterion about continuous monitoring (reasonable span) of public security cameras in order to prove the commission of a crime in flagrance, and that it is not an arbitrary action nor violates individuals right.

**Profiling.** Article 112 of the Regulations address that if personal data is used in decision-making without human intervention, the data controller must so inform the data subject. In addition, the data subject may exercise his right of access in order to discover the personal data used as part of the decision-making process, and as the case may be, his right to rectification, when he considers that some of the personal data used are incorrect or incomplete so that, in accordance with the mechanisms implemented by the data controller for this purpose, he can request a reconsideration of the decision made.

Finally, in this regard it is relevant to consider that the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Plus, among the objectives of the new version of Convention 108 is to include as a right for individuals: not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.

This Modernisation of Convention 108 was opened for signature in October 2018[1]: it has 35 state signatures and only 3 ratifications, the Mexican State is not part of
this update yet.

**Cookies.** Although in Mexico there are no specific guidelines on cookies and similar technologies, provisions on these can nevertheless be found in the Privacy Notice Guidelines (only available in Spanish here) (‘the Privacy Guidelines’) issued by the INAI

Cookies are defined in the Privacy Guidelines as a data file that is stored on the hard drive of the computer or device of electronic communications of a user when browsing a specific internet site, which allows the exchange of status information between said site and the user’s browser. The status information may reveal means of session identification, authentication, or preferences of the user, as well as any data stored by the browser regarding the website.

The above applies to remote or local means of electronic communication, optics, or other technology, that allow for the collection of personal data automatically and simultaneously while the data subject contacts them.

Tacit consent (opt-out) is the general rule: when the controller intends to collect the personal data directly or personally from the data subject, he must make the privacy notice available to him prior to such collection, which must contain a mechanism so that, where appropriate, the data subject can express his refusal to the treatment of his personal data for purposes that are different from those that are necessary and that underline the legal relationship between the controller and the data subject.

Under Mexican data protection regulations, cookies do not fall within the definition of ‘Personal Data.’ However, through the use of cookies, personal data such as, inter alia, internet protocol (IP) addresses, personal preferences, content personalisation, may be collected. In this sense, Mexican data protection regulations oblige controllers, in a broad way, to notify of any use of cookies or other tracking devices in the relevant privacy notice, and to provide a means of disabling them.

In that sense, the controller must include the use of cookies and other tracking devices (features and purposes) in the relevant privacy notice. Furthermore, and in addition to the privacy notice, banners or pop ups informing about the use of cookies or tracking devices may be employed.

Reference


21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

Personal Data Processing must comply with all the general data principles, specifically in this case “purpose specific” and consent. That means all purpose for which PII will be used must be objective, determined and justified; and the consent principle establishes that each consent must be informed, free and specific. In this context cross-contextual behavioral advertising could be performed to the extent it is clearly and unmistakable informed in the relevant privacy notices.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is “sale” or related terms defined and what restrictions are imposed, if any?

There is no law in this regard.

23. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Laws in Mexico addressing email communication or direct marketing, are as follow:

- **The Federal Law on Protection of Personal Data held by Private Parties (processing of personal data for marketing purposes)**
- **Regulations of the Federal Law on Protection of Personal Data held by Private Parties (processing of personal data for marketing purposes)**
- **Guidelines by the Mexican DPA on the processing of personal data in debt collection activities** (not mandatory; guidance for debt collectors)
- **The Federal Consumer Protection Law** (direct marketing, do not call lists)
- **Regulations of the Federal Law on Consumer Protection** (direct marketing, in particular sections I and III).
- **Commerce Code** (particularly second Title, section I)
- **Mexican Official Standard NMX-COE-001-SCFI-2019 15/21 for e-commerce**, of voluntary compliance
Regarding specific protection to consumer’s due to marketing practices, Data Controllers must comply with Privacy Notice Guideline 30 in relation to Article 16 (III) of the Data Protection Law, since it provides that data controllers must inform data subjects of the options and means open to them to limit the use and disclosure of their data, other than the exercise of ARCO rights, or to revoke their consent.

In this sense the relevant Privacy Notice should include that one of the purposes of using the consumer’s personal data, is to manage newsletters and communications, either with commercial information and promotions about products and services, or for work purposes, as appropriate, and should also provide specific mechanisms for the consumer to say no, among these mechanisms is the Public Register for Avoiding Advertising (‘REPEP’) or it can be an email, or a tick box.

In addition to providing consumers with the privacy notice the treatment of personal data and pursuant the Law, the principles and duties shall be observed.


PROFECO has a public registry to avoid advertisement (‘REPEP’ for its acronym in Spanish). This registry is fed by consumers that have chosen not to receive advertising calls either in landline or mobile number, text messages, and/or their contact information to be used for telemarketing activities. Suppliers and telemarketing companies paying certain governmental fees obtain and updated registry every 15 days and could use it to filter out the contact information of consumers that had opt out to receive calls. Telemarketing to consumers could be made directly by suppliers or by sourced to telemarketing companies.

Among others, the following provisions and restrictions of FCPL are applicable to marketing activities:

i. The information regarding consumers could not be used for purposes different than marketing or advertising purposes.

ii. The information provided by consumer should be treated on confidential basis, and shall not be disclosed to other unrelated suppliers or other third parties except express authorization consumer, or on demand of an authority with competent jurisdiction.

iii. Consumers may demand not to be bothered in his/her address, workplace, and electronic address or through any other mean to be offered goods or services, as well as not to receive advertising.

iv. Suppliers and companies using consumers’ information are bound to inform free of charge: (a) if it keeps any information of consumer, if so, to make it available, and/or (b) provide a report of the information disclosed to third parties.

v. Suppliers are jointly liable for the use of consumers information when marketing is made by third parties.

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

Laws in Mexico addressing biometrics, understanding biometrics as personal data when appropriate, will be the Law and its Regulations. They are applicable to the photographs/images of identifiable individuals since such images are considered personal data. In general terms, biometric data are not considered sensitive personal data but only under some circumstances whereby the use of such data may lead to discrimination or a serious risk to the data subject.

Biometric data are defined in the Guide for the Processing of Biometric Data, issued by INAI, 2018: measurable physical, physiological, behavioral and personality characteristics attributable to a single person.

Under the Law when processing biometrics personal data, implicit consent (‘opt-out’) suffices, unless financial or sensitive data is processed. Implicit consent is obtained when the individual is provided with a privacy notice and he/she does not object the processing of his/her personal data. The privacy notice shall be provided to the individuals, and their consent must be collected before collecting the biometric data. Verbal and written communication is enough to constitute explicit consent, as are communications by electronic or optical means or via any other technology or by unmistakable indications. It is always suggested to keep evidence of the provision of the privacy notice and the collection of the individual’s consent.

Under the Law, article 8 et al., the data subject must have the right to withdraw his/her consent at any time, in a manner which means it is as easy to withdraw as to give consent.
Guide for the Processing of Biometric Data, INAI, 2018. In this Guide, the INAI makes a summary of the principal obligations for data controllers regarding the processing of personal data and provides some recommendations to comply with these obligations. Some of the recommendations included in the mentioned guide are the following:

- To expressly inform in the privacy notice that biometric data will be collected, specifying the type (e.g., facial recognition).
- Describe the purposes for which the data collected will be processed (e.g. recognize data subjects).
- Collect and process the minimum number of data (including biometric data) necessary for the intended purposes.
- Do not keep the biometric data for a period longer than necessary to fulfill the purposes described.
- Establish administrative, physical and technical security measures necessary to ensure that data is protected from unauthorized access, processing, deletion, loss or use, like: employing encryption, secure deletion techniques. Training employees on privacy and data protection matters is a security measure that helps to mitigate risks.
- Do not disseminate data without the consent of the data subject and clearly define the authorized personnel to access and process information of this type.
- Delete unnecessary links between the database with other systems or databases that may inadvertently lead to an unauthorized transfer.
- Implement procedures to assess and address risk from the implementation of technologies and business models that involve the treatment of biometric data.
- Constantly supervise the activities carried out by external providers that offer services that involve the treatment of biometric data.
- Develop Internal policies to verify privacy programs compliance.
- Data controller should be plenty aware that biometric data (e.g., facial recognition) to be necessary to achieve its purpose, and that there it cannot be supplied by no biometric data.
- It is advisable to collect data with the best possible quality to decrease the number of biometric data required for fulfill the corresponding purpose.
- Store, organize and manage biometric data in a way that allows the attention of requests for the exercise of Access, Rectification, Cancellation and Opposition (ARCO) and revocation of consent rights on time. Data subject should be able to withdraw consent for facial recognition at any time.

25. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

International transfers of personal data or PII according to Law and its Regulations, must meet certain requirements to ensure standards of personal data protection, generally must be written in an agreement or clauses, requires the consent of the data subject and must provide the privacy notice.

In addition, international transfers are possible when the recipient assumes the same obligations as those of the data controller who transferred the personal data.

The Law defines transfer as any communication of data to a person other than the data controller or processor. If the data controller intends to transfer personal data to national or foreign third parties, other than the data processor, s/he must communicate to them the privacy notice and the purposes to which the data controller has subjected its processing.

The processing of the data will be done as agreed in the privacy notice, which will contain a clause indicating whether or not the data controller accepts the transfer of his data, and likewise, the third-party recipient will assume the same obligations that correspond to the controller who transferred the data.

No notice to the Data Protection Authority is required.

While consent from the data controller is generally required (clause in the privacy notice), there are certain exceptions to this obligation to obtain consent:

National or international transfers of data may be carried out without the consent of the data subject in any of the following cases

i. When the transfer is provided for in a Law or Treaty to which Mexico is a party.
ii. When the transfer is necessary for the
prevention or medical diagnosis, the provision of health care, medical treatment or the management of health services.

iii. When the transfer is made to holding companies, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group of the data controller operating under the same internal processes and policies.

iv. When the transfer is necessary by virtue of a contract entered into or to be entered into in the interest of the data subject, by the data controller and a third party.

v. When the transfer is necessary or legally required for the safeguard of a public interest, or for the procurement or administration of justice.

vi. When the transfer is necessary for the recognition, exercise, or defence of a right in legal proceedings, and

vii. When the transfer is necessary for the maintenance or fulfillment of a legal relationship between the data controller and the data subject.

The Regulations to the Law specify the territorial scope of application and make explicit a specific regime for international transfers, i.e., when:

1. the controller (data controller) is established in Mexican territory: a. processing carried out in that establishment, b. processing carried out on his behalf, by a processor, regardless of his location.

2. the data controller is not established in Mexican territory: a. Mexican law is applicable to them, by contract or by virtue of International Law, b. they use means located in Mexican territory, unless such means are used solely for transit purposes that do not involve processing, c. if the data controller is “located” in Mexican territory, the provisions on security measures contained in the Regulations shall apply to them.

The law on data protection for the public sector regulates international transfers in a very similar manner. However, this regime contemplates certain exceptions to the general rule of formalization, that is, that every transfer requires the existence of a legal instrument that establishes its existence, content and scope, but there are the following exceptions:

i. When the transfer is domestic and is made between data controllers for compliance with a legal provision or in the exercise of powers expressly conferred on them, or

ii. When the transfer is international and is provided for in a law or treaty signed and ratified by Mexico, or when it is made at the request of a foreign authority or international organization competent in its capacity as recipient, provided that the powers between the transferring and receiving parties are the same, or that the purposes for which the transfer is being made are analogous or compatible with those that gave rise to the processing of the transferring party.

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

Data controller must set and maintain administrative, technical and physical security measures to protect personal data against damage, loss, alteration, destruction or unauthorized use, access or processing.

Data controllers may not adopt security measures less stringent than those they maintain for the handling of your information. In this respect, these measures must also consider the existing risk, the possible consequences for the data subjects, the sensitivity of the data and the technological development.

The Law defines these security measures as follows:

**Administrative security measures:** Set of actions and mechanisms to establish the management, support and review of information security at the organizational level, the identification and classification of information, as well as the awareness, education and training of staff, in the field of personal data protection.

**Physical security measures:** Set of actions and mechanisms, whether or not they employ technology, intended to

a. Prevent unauthorized access, damage or interference to physical facilities, critical areas of the organization, equipment and information; b) Protect mobile, portable or easily removable equipment located inside or outside the facilities; c) Provide maintenance to equipment containing or storing personal data to ensure its availability, functionality and integrity; and d) Ensure secure disposal of data;
**Technical security measures:** A set of activities, controls, or mechanisms with measurable results, which use technology to ensure that:

a. The access to the logical databases or information in logical format is carried out by identified and authorized users; b) The access referred to in the previous paragraph is only for the user to carry out the activities required for their functions; c) Actions for the operation, development and maintenance of secure systems are included; and d) The management of communications and operations of computer resources used in the processing of personal data are carried out.

When the appointed member of staff is not located in Mexican territory, but another person in charge is, the provisions regarding safety measures contained in the leading part of the Regulations will be applicable to the latter.

Among the actions that all data controllers must carry out to establish and maintain a management system for the security of personal data are the following:

i. Draw up an inventory of personal data and processing systems; II. Determine the functions and obligations of those who process personal data; III. Having a personal data risk analysis that consists of identifying hazards and estimating risks to personal data; IV. Establish security measures applicable to personal data and identify those implemented effectively; V. Conduct a gap analysis consisting of the difference between existing and missing security measures necessary for the protection of personal data; VI. Develop a work plan for the implementation of the missing security measures derived from the gap analysis; VII. Conduct reviews or audits; VIII. Train staff who will carry out the processing; and IX. Conduct a record of the means of storage of personal data.

The data controller must also keep the security measures under constant review, specifically updating them when the following events occur:

The security measures or processes are modified for their continuous improvement, derived from the revisions to the security policy of the person in charge; – Substantial modifications are produced in the treatment that derive in a change of the risk level; – The treatment systems are violated, or – There is an affectation to the personal data different to the previous ones.

In summary, in accordance with the above, every responsible person has the following obligations regarding the duty of security: 1. To establish and maintain administrative, physical and technical security measures; 2. Not to adopt security measures less than those maintained for the handling of their information; 3. Update the implemented security measures, when required, according to the criteria described above; 6. Notify the data subjects of the security breaches that occur, with the information and at the time indicated above; 7. Carry out any necessary corrective actions.

It is also relevant to consider the following recommendations and various Guides issued by INAI, for the security of personal data (available in Spanish).

Recommendations on Personal Data Security Published in the Official Gazette of the Federation on October 30, 2013


Guide to Implementing a Personal Data Security Management System, June 2015
http://inicio.ifai.org.mx/DocumentosdelInteres/Gu%C3%A1Da_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Secure Personal Data Erasure Guide


**27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?**

Data Protection Law in Mexico address that breaches of the security of personal data which occur in each processing phase are:

i. Loss or unauthorized destruction; II. Theft, misplacement or unauthorized copying; III. Unauthorized use, access or processing, or IV. Unauthorized damage, alteration or modification.

The Regulations state that in cases where a violation of the security of personal data occurs, INAI may take into consideration compliance with its recommendations to determine the mitigation of the corresponding penalty.
The Law on Personal Data applicable to the Public Sector also regulates security breaches. It defines them in the same way.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

The provisions on personal data security are those mentioned above. However, the Act also provides that sectors or industries may adopt best practices and self-regulation in order to raise the level of protection of personal data. Personal data regulations are complementary to specific regulations, such as telecommunications, tax, financial or health, etc. Therefore, the information security requirements in the first instance observe the particular regulations of the matter in question and harmonize their implementation with those relating to personal data if applicable.

For example, in the case of the financial sector, the Ministry of Finance signed with different financial authorities and the General Attorney’s Office of the Republic some coordination bases on information security.

Likewise, the Law indicates that individuals or corporations may agree among themselves or with civil or governmental organizations, whether national or foreign, on binding self-regulation schemes on the subject, which complement the provisions of this Law. Such schemes must contain mechanisms to measure their effectiveness in data protection, consequences, and effective corrective measures in case of non-compliance.

Self-regulatory schemes may take the form of codes of ethics or good professional practice, seals of confidence or other mechanisms and shall contain specific rules or standards that make it possible to harmonise the processing of data by members and to facilitate the exercise of the rights of the data subjects. These schemes must be notified simultaneously to the corresponding sectoral authorities and to INAI.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

Security breaches occurring at any stage of processing that significantly affect the economic or moral rights of the data subjects must be immediately reported by the controller to the data subject, so that the latter can take the appropriate measures to defend his rights.

In certain sectors such violations must also be notified to the sectorial authorities, as is the case of banks, stock exchange houses or financial companies that want to operate the models provided for in the Law to regulate Financial Technology Institutions, must submit periodic reports to the Ministry of Finance and Public Credit in which they must include security incidents to their information, such as cyber-attacks.

There is no obligation yet in Mexico for the private sector to notify INAI in the event of a breach of security of personal data that significantly affects the rights of the data subjects, in the public sector if it is compulsory.

In accordance with the Data Law, if it is applicable to notify the data subjects, this notification must be carried out immediately, there is no time limit as soon as it confirms that the violation occurred and has taken the actions aimed at triggering a process of exhaustive review of the magnitude of the affectation, and without any delay, so that the affected data subjects can take the corresponding measures.

When notifying data subjects of a given safety violation, the data controller should consider including at least the following requirements:

- The nature of the incident;
- The personal data involved;
- Recommendations to the data subject on measures the data subject can take to protect his/her interests;
- The corrective actions taken immediately; and
- The means by which you can obtain further information about the incident.

It is important to consider what to do after a personal data breach. Corrective measures must be adopted, the data controller must analyse the causes and implement corrective, preventive, and improvement actions to adapt the corresponding security measures in order to prevent the violation from being repeated.

In this respect, INAI has issued Recommendations for the handling of personal data security incidents.


30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the
payment of ransoms in ransomware attacks?

There is no standard or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks. There is a protocol, but it is not public. It is known because in 2017 the Cybersecurity Unit of the then Federal Police (now the National Guard) and its National Center for Cyber-Incident Response activated an action protocol with the government, financial and business sectors to identify, address and follow up on cases where ransomware (Peyta) were detected.

The closest item is the sanctions in the Mexican Federal Criminal Code, (articles 211 bis 1 to 211 bis 7) against illegal access to information contained in computer systems or equipment protected by some security mechanism by both individuals and the State.

Until last year, according to various agencies, Mexico was the country in Latin America with the highest number of attacks by ransomware. One of the signs of weakness and opacity in this issue on the part of the Mexican state was the ransomware attack perpetrated against the state oil company, Pemex, and about which there was very little information from the Mexican government itself.

According to the OECD, Mexico is in last place on cybersecurity, since it is lagging behind in the classification of computer crimes and does not have prepared human resources (ministerial agents, investigative police and knowledgeable judges) to deal with electronic fraud, card cloning, database theft, blocking of portals or hacking of email accounts, among other crimes of this type, which also makes it possible to commit crimes such as child pornography, grooming or sexting, among others. 
https://www.senado.gob.mx/64/gaceta_comision_permanente/documento/71861.

It should be noted that the Budapest Convention seeks to combat Internet crime through the harmonization of national laws, the improvement of investigative techniques and coordination between the countries that are parties to the Convention. Mexico has not yet formalized its entry into the Budapest treaty, but only participates as an observer to the instrument.

31. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

It does not exist. The only State body that takes action against these crimes is the Directorate General of Science of the National Guard and works on the prevention of cybercrime.

The National Cybersecurity Strategy is the document that address the Mexican State’s vision in this area, based on the recognition of A) The importance of information and communication technologies (ICTs) as a factor in Mexico’s political, social and economic development, in the understanding that more and more individuals are connected to the Internet and that both private and public organizations are developing their activities in cyberspace; B) The risks associated with the use of technologies and the growing number of cybercrimes and C) The need for a general culture of cybersecurity.

32. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

Mexican data protection laws provide personal data rights to access, rectify, oppose, and/or cancel (ARCO rights), as follow:

Right of Access: This is the right that a data subject has, to request access to his/her personal data that is in the databases, systems, files, records or files of the data controller for holding, storing or using them, as well as to know information related to the use given to his/her personal information.

Right of Rectification: This is the right of a data subject to request the rectification or correction of their personal data, when these are inaccurate, incomplete, or outdated. In other words, you can ask whoever holds or uses your personal data to correct them when they are incorrect, outdated, or inaccurate.

Right of Cancellation: This is the right that a data subject to request the rectification or correction of their personal data, when these are inaccurate, incomplete, or outdated. In other words, you can ask whoever holds or uses your personal data to correct them when they are incorrect, outdated, or inaccurate.

Right of Opposition: This is the right that a data subject to request the rectification or correction of their personal data, when these are inaccurate, incomplete, or outdated. In other words, you can ask whoever holds or uses your personal data to correct them when they are incorrect, outdated, or inaccurate.

Right of Cancellation: This is the right that a data subject to request the rectification or correction of their personal data, when these are inaccurate, incomplete, or outdated. In other words, you can ask whoever holds or uses your personal data to correct them when they are incorrect, outdated, or inaccurate.

Right of Opposition: This is the right that a data subject to request the rectification or correction of their personal data, when these are inaccurate, incomplete, or outdated. In other words, you can ask whoever holds or uses your personal data to correct them when they are incorrect, outdated, or inaccurate.

Right of Cancellation: This is the right that a data subject to request the rectification or correction of their personal data, when these are inaccurate, incomplete, or outdated. In other words, you can ask whoever holds or uses your personal data to correct them when they are incorrect, outdated, or inaccurate.

Right of Opposition: This is the right that a data subject to request the rectification or correction of their personal data, when these are inaccurate, incomplete, or outdated. In other words, you can ask whoever holds or uses your personal data to correct them when they are incorrect, outdated, or inaccurate.
be terminated in order to avoid harm. Also in this case, the use of personal data may not always be prevented, when it is necessary for some legal matter or for the fulfilment of obligations.

Limits: Like any other right, the right to protection of personal data has limits, so under certain circumstances ARCO rights may not be exercised or their exercise may be limited by issues of national security; public order, safety and health, as well as the rights of third parties.

Some reasons why the data controller might deny the exercise of ARCO rights are:

- When the data subject of the personal data or his representative has not proved his identity
- When the personal data are not in the possession of the person data controller.
- When there is a legal system that prevents the exercise of ARCO rights.
- When the exercise of ARCO rights may affect the rights of another person.
- When the exercise of ARCO rights could hinder judicial proceedings or the tasks of an administrative authority.
- When there is a decision by a competent authority that prevents access to the personal data or does not allow their rectification, cancellation or opposition.
- When the data subject has previously requested the cancellation or opposition of their personal data.
- When the data controller who is asked to exercise ARCO rights is not competent to do so.
- When they are necessary to protect the legally protected interests of the data subject.
- When they are necessary to comply with obligations legally acquired by the data subject.

However, even if the exercise of the ARCO rights is not appropriate, the data controller must answer the request and inform the causes of the impropriety.

The right to the protection of personal data is an absolutely personal one, so only the data subject of the personal data or, where appropriate, his representative may request the exercise of ARCO rights. Therefore, it will be necessary and of great importance that prior to the exercise of the right in question, the identity of the data subject is duly accredited.

It should be considered that for a data subject to be able to request one of the rights it is not necessary that s/he has previously exercised another, nor does the exercise of one of them prevent them from later asserting a different one. For example, data subjects can request the rectification of personal data without the need to have previously requested access, and can exercise her/his right to cancel the data regardless of whether the data subject has previously accessed her/his data.

The requirements may vary depending on the nature of the data controller, that is, whether he or she is from the public or private sector, as the laws governing the right to protection in both sectors are different.

The first aspect to note is that the application to exercise ARCO rights must be submitted to the data controller for the personal data about which you require access, rectification, cancellation or opposition. The means for submitting these requests must be indicated in the privacy notice.

To exercise these rights there are a series of requirements that must be met, some of which are general and others specific depending on the right to be exercised.

As for the general requirements that must be covered by the request, there are the following:

- Name of the data subject of the personal data.
- Documents accrediting the identity of the data subject.
- If applicable, name of the representative of the data subject and documents to prove his/her identity and personality.
- Address or any means of receiving notifications.
- Clear and precise description of the personal data and the right to be exercised or requested.
- Where appropriate, documents or information that facilitate the location of personal data.

In relation to the specific requirements, according to the right to be exercised, there are the following:

Access: – Indicate the modality in which the data subject prefers that the requested personal data be reproduced.

Rectification: – Specify the modifications that are requested to the personal data, as well as provide the documents that support the request.

Cancellation: – Indicate the reasons for the request to remove the data from the files, registers or databases of the data controller.

Opposition – State the causes or the situation that led the data subject to request that the processing of his
personal data be terminated, as well as the damage that would be caused by the continuation of such processing.

Accreditation of the identity of the data subject and his representative, as well as the personality of the latter: As previously stated, a fundamental requirement for the exercise of ARCO rights is that it must be previously demonstrated that the person who wishes to exercise the right is the data subject. To this end, it is necessary that, prior to the exercise of the right of access, rectification, cancellation or opposition, the identity of the data subject and of his representative, if the application is made through the latter, be accredited through the presentation of an official identification.

However, when the application is submitted through a representative of the data subject, it will be necessary for this person to prove that he or she is authorized to submit the application on behalf of the data subject of the personal data. To this end, the representative must prove his or her identity, prior to the exercise of the right in question, by presenting a public instrument (document signed by a Notary Public) or a simple power of attorney signed before two witnesses, attaching a simple copy of the official identification of those signing the letter. Alternatively, the data subject and the representative may appear to testify in person before the data controller. If the representation is exercised by a legal entity, it must prove its personality by means of a public instrument.

Request for the exercise of ARCO rights of a person underage, in a state of interdiction or legal incapacity, or deceased When it is intended to exercise ARCO rights in relation to personal data of a person under age or in a state of interdiction or legal incapacity, the provisions of civil law must be observed and the representation will be in accordance with the rules established by such legislation. As regards the personal data of a deceased person, only the person who proves to have a legal interest, in accordance with the applicable laws, may exercise the ARCO rights, provided that the data subject has reliably expressed his or her will or there is a court order to that effect, and that the request is made to a public sector official.

The procedure for dealing with applications for ARCO rights will depend on whether the application is submitted to a public or private sector controller.

In both cases, this procedure begins when the data subject or his representative submits the application to exercise ARCO rights to the data controller for the personal data for which access, rectification, cancellation, or opposition is required.

33. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

The individual data privacy rights first must be exercised through the regulator, i.e., INAI. The resolutions emitted by INAI may be challenged before the judicial system.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

The laws in Mexico provide for a form of this private right of action, contemplated as a civil or criminal complaint, depending on the damage, in this sense: data subjects who consider that they have suffered damage or injury to their property or rights as a result of the breach of the provisions of the Data Law, by the responsible party or the person in charge, may exercise the rights they deem relevant for the purposes of the appropriate compensation, in terms of the corresponding legal provisions.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Yes, data subjects can demand compensation for financial damages or indemnification when they have suffered damage or injury to their property or rights because of non-compliance with the provisions of the Law.

That is to say, the data subject, once s/he is notified or becomes aware of a security breach that has occurred at any stage of the processing, and that this breach significantly affects his economic or moral rights, may take the corresponding measures to defend her/his rights—such as a claim for moral or economic damages; or in general when they consider that they have suffered damage or injury to their goods or rights as a result of the breach of the provisions of the Data Law.

In a sue for moral damages it is appropriate to allege a spiritual affectation or a psychological disorder. In other words, that the data subject experiences suffering. Moral damage is understood as the affectation that a person suffers in his feelings, affections, beliefs, decorum, honour, reputation, private life, physical configuration, and appearance, or in the consideration that others have of him.
The elements of liability for moral damage that must be observed before exercising the action for reparation, and which derive from judicial interpretation, are: 1. The production of damage to any of the goods of the personality. 3. The cause-effect relationship between the act and the damage.

36. How are the laws governing privacy and data protection enforced?

The Data Protection Authority is the INAI.

INAI will be first instance for every data protection procedure. INAI's resolutions may be challenged before Judicial Federal Courts.

Besides, damages may be sought in Civil Courts.

The enforcement of data protection laws tends to be harsh. Around 97% of the cases that are initiated before the Data Protection Authority for the violation of the legislation on data protection conclude with the imposition of a fine. During the first semester 2021, the Data Protection Authority imposed fines for a total of approx. USD 1,600,664.28

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

Violations of the Data Law are sanctioned by INAI with:

- The warning for the person in charge to carry out the acts requested by the data subject, related to the failure to comply with his/her request for access, rectification, cancellation, or opposition to the processing of his/her personal data.

Fines ranges from 100 to 320,000 units called UMA. Currently the value of a UMA is 96.2 Mexican pesos (approx. USD 4.7). Therefore, fines range from approx. USD 470 to approx. USD 1,500,000. Fines may double if sensitive personal data is involved.

Fines will be imposed depending on categories of processed data; the intentional nature or not, of the action or omission constituting the infraction; the economic capacity of the person in charge, and recidivism.

Penalties:

- Three months to three years imprisonment will be imposed, to whom being authorized to process personal data, for profit, causes a security breach of the databases in their custody.
- Six months to five years imprisonment will be sanctioned to whom, in order to achieve an undue profit, process personal data through deception, taking advantage of the error in which the data subject or the authorized person to transmit them is found.
- In the case of sensitive personal data, the penalties referred to shall be duplicated.

38. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

No. The Federal Law articles 63 and 64 establish the reference for calculating fines and the conducts that constitute the imposition of sanctions, explained in previous answer.

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Individuals have legal remedies against INAI decisions which they may bring before the Federal Courts.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

There are several bills to amend the Federal Law for the Protection of Personal Data Held by Private Parties, however it is uncertain if they will be discussed and approved.

In connection with cybersecurity laws in Mexico there is no specific regulation. However, there are Law proposals at the Congress in order to issue a general law on cybersecurity.
Contributors

Adolfo Athié
Partner
aathie@basham.com.mx

Renata Buerón
Associate
rbueron@basham.com.mx

Erika Rodriguez
Associate
erodriguez@basham.com.mx

Maria Fernanda Gonzalez
Associate
mgonzalez@basham.com.mx