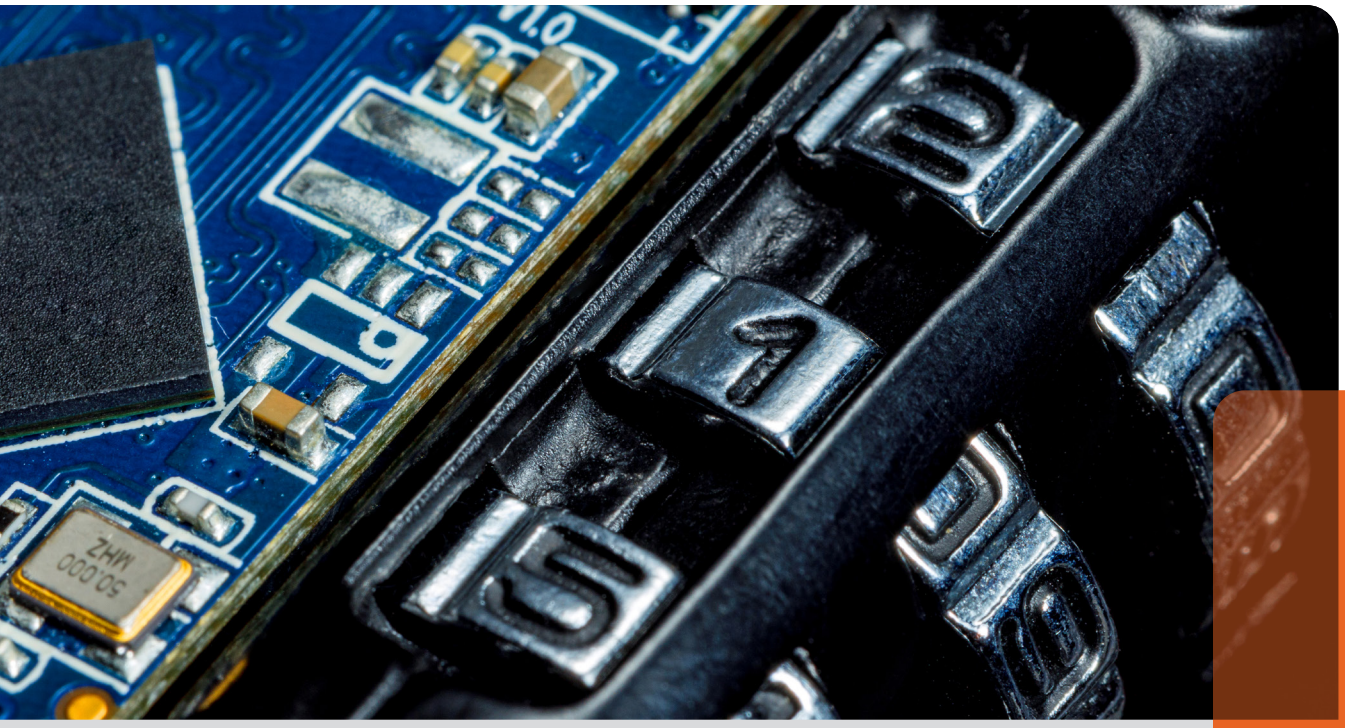
International
Comparative
Legal Guides



Data Protection

2024

11th Edition

Contributing Editors:
Tim Hickman & Detlev Gabel
White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Mexico


Abraham Díaz


Gustavo Alcocer


Carla Huitron

OLIVARES

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The legal framework for data protection is found in Articles 6 and 16 of the Mexican Constitution, as well as in the Federal Law for the Protection of Personal Data Held by Private Parties, published in July 2010, and its Regulations, published in December 2011 (hereinafter the "FLPPDHPP").

1.2 Is there any other general legislation that impacts data protection?

Yes, as follows: the General Law for the Protection of Personal Data in the Possession of Obliged Subjects, which regulates the processing of personal information ("PI") in the possession of any Federal, State or local authority (the "Law"); the Privacy Notice Rules, published in January 2013; the Binding Self-Regulation Parameters, also published in January 2013; and the General Guidelines for the Protection of Personal Data for the public sector (Federal, State or local authorities). It is worth mentioning that Mexican data protection laws and general legislation follow international correlative laws, directives and statutes, and thus have similar principles, regulatory scope and provisions. Moreover, there are other laws such as: the Criminal Code; the Law for the Regulation of Credit Information Companies; the Law for Regulating Financing Technology Institutions; provisions set forth in the Copyright Law and the Federal Law for Consumer Protection; and some specific provisions set forth in the Civil Code and the Commerce Code, which are also related to data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

Mexican data protection legislation is not based on sectoral laws. The Law, as described above, regulates the collection and processing of any PI by any private entity acting as a Controller or Processor, which impacts any sector that is involved in any sort of personal data collection or processing.

1.4 What authority(ies) are responsible for data protection?

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

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  Any information concerning an individual that may be identified or identifiable.
- "**Processing**"
  The collection, use, disclosure or storage of personal data, by any means. Use covers any action of access, management, benefit, storage, transfer or disposal of personal data.
- "**Controller**"
  The individual or private legal entity that determines the processing of personal data or provides the guidelines for the said processing.
- "**Processor**"
  The individual or legal entity that, solely or jointly with another, processes personal data on behalf of the Controller.
- "**Data Subject**"
  Any identified or identifiable natural person.

- "**Sensitive Personal Data**"/"**Special Categories of Personal Data**"
  Any personal data 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 data are considered those that 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.
  Other than the "sensitive personal data definition" there are no special categories of personal data in our law.
- "**Data Breach**"
  Data breach means any security breach that, if occurring in any phase of the data collection, storage or use, may affect in a significant manner the patrimonial or moral rights of individuals.
- "**ARCO Rights**"
  Refers to the access, rectification, cancellation or opposition rights, which can be enforced by any data subject, in connection with the collecting or processing of its PI.
- "**Consent**"
  An expression of will made by any data subject, or by any person with legal authority to act on behalf of the data subject, for conducting any activity related to the collecting or processing of the PI of the data subject.
- "**Pseudonymisation**"
  The processing of personal data in such a manner that it can no longer be attributed to a specific data subject, without the use of additional information.
- "**Privacy Notice**"
  A document issued by the Controller either in physical, electronic or any other format, which is made available to the data subject prior to processing his/her personal data, and whereby the Controller informs the data subject, among other matters, about: the terms for the collection of personal data; which PI will be collected; the identity of the Controller; the purpose of the data collection; the possible transfers of data; and the mechanisms for the data subject to enforce its ARCO rights.
- "**Transfer**"
  Any data communication made to a person other than the Collector or the Processor, either in Mexican territory or abroad.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Mexican data protection law is 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 being applicable to companies established or operating under Mexican law (whether or not located in Mexican territory) apply to companies not established under Mexican law that are subject to Mexican legislation derived from the execution of a contract or under the terms of international law.

Additionally, Mexican regulations on data protection apply to: company establishments located in the Mexican territory; persons or entities not established in the 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 personal data; and when the Controller is not established in the Mexican territory but the person designated as the party in charge of the control and management of its personal data (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.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Mexican Data Privacy Law does not carve out any processing activities from the material scope. Our Law only indicates that the Controller should be responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties, regardless of the processing activity or material scope.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  This principle is not defined in the Law; however, the Law makes it clear that personal data can in no way be collected, stored or used through deceitful or fraudulent means.
- **Lawful basis for processing**
  The Controller is responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties.
- **Purpose limitation**
  Personal data shall only be collected and processed in compliance with the purpose or purposes set forth in the Privacy Notice. Moreover, the purpose of the Privacy Notice must be certain, which is achieved by establishing the purpose for which the personal data will be collected and processed in a clear, objective manner, not leaving any room for confusion.
- **Data minimisation**
  The Controller will be responsible and shall endeavour to make reasonable efforts so that the personal data processed are the minimum necessary according to the purpose that originated the collection of PI.
- **Proportionality**
  Controllers can only collect personal data that are necessary, appropriate and relevant for the purpose(s) of their collection.
- **Retention**
  This translates into the obligation of the Controller to retain personal data only for the period of time necessary for complying with the purpose(s) for which the data were collected, with the obligation to block, cancel and suppress the personal data afterwards.
- **Accuracy**
  This principle refers to ensuring that the processed personal data is correct and updated and is strictly related to the following "Quality" principle as described below, which includes accuracy.
- **Responsibility**
  The Controller must safeguard and be accountable for any PI under its custody, or any PI that it has shared with any vendor, either in Mexico or abroad. In order to comply

with this principle, the Controller must make use of any of the best international practices, corporate policies, self-regulatory schemes or any other suitable mechanism to this effect.

- **Quality**
  This principle is accomplished when the personal data processed are accurate, complete, pertinent, correct and updated as required, in order to comply with the purpose for which the personal data will be collected.
- **Consent**
  The Controller must obtain the consent of the data subject prior to the collection of any PI, and must keep evidence of the consent.
- **Loyalty**
  This consists of the obligation of the Controller to process any PI collected favouring the protection of the interests of the data subject and the reasonable expectation of privacy.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
  Data subjects have the right to access their personal data held by the Controller at any time they request.
- **Right to rectification of errors**
  Data subjects have the right to request the rectification of any of their personal data, held by a Controller, which turns out to be inaccurate, incomplete or out of date.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to request the cancellation of their personal data. The cancellation of personal data will result in a blocking period, after which the suppression of the data will take place. Notwithstanding the foregoing, the Controller may keep such personal data exclusively for the purposes of the responsibilities regarding their treatment. Likewise, the Law establishes some cases where the Controller is not obliged to cancel or delete the personal data.
- **Right to object to processing**
  Data subjects have the right to object to the processing of their personal data due to a legitimate reason.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of their personal data due to a legitimate reason.
- **Right to data portability**
  Data subjects have the right to obtain, from the subject concerned, a copy of their processed data, which allows the data subject to continue using their PI.
- **Right to withdraw consent**
  At any time, the data subject may withdraw their consent for the treatment of their personal data. The Controller must establish simple and free mechanisms that allow the data subjects to withdraw their consent at least by the same means by which they granted it.
- **Right to object to marketing**
  In addition to the general rights described above, data subjects have the right to oppose the use of their personal data for marketing or advertising purposes.
- **Right protecting against solely automated decision-making and profiling**
  Data subjects have the right to oppose to the treatment of their data, at any time, by any mechanism, including automated decision-making and profiling.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects are entitled to submit a claim before the INAI. The claim must be filed in writing and must clearly state the provisions of the Law that are deemed infringed; also, it must be submitted within the 15 days following the date on which the response to the data subject has been communicated by the Controller.
- **Right to a verification procedure**
  Data subjects have the right to request a verification procedure before the INAI, by which the authorities will check the Controller's compliance with all the provisions set forth in the Law, or any other applicable regulations.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The only person that might seek remedies for data protection infringements are the data owners themselves, or in its case, their legal representatives. The Law does not contemplate collective redress.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Children's legal guardians' consent must be always given when processing children's personal data. This applies to any individual younger than 18 years of age.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No there is not.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable.

7.10 Can the registration/notification be completed online?

This is not applicable.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

7.12 How long does a typical registration/notification process take?

This is not applicable.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer (person or department) by the Controller is mandatory.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a Data Protection Officer (person or department) is not expressly catalogued as an infringement in the Law. However, Section XIX of Article 63 of the FLPPDHPP contains a "catch all" provision that considers any failure to comply with the obligations set forth in the Law to be an infringement. Therefore, failure to appoint a Data Protection Officer must be deemed an administrative infringement. Nevertheless, there is no express sanction in the law for the infringements referred to in Section XIX above.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

No, they are not.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, it can.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no statutory requirements. Notwithstanding the foregoing, it is recommended to appoint a person, team or department with at least the following qualifications: (i) data privacy expertise (certification desired); and (ii) enough authority and resources to advocate and implement measures in order to protect the personal data within the company.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The responsibilities of a Data Protection Officer required by law are to: (i) process all claims related to the enforcement of ARCO rights; and (ii) foster and enhance the protection of personal data inside the company.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, there is no statutory obligation to register or notify the appointment of a Data Protection Officer to any authority.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

It is necessary to mention in the Privacy Notice the name and domicile (contact information) of the person or department that will be responsible for the collection, use and storage of the personal data.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the relationship between the business and the Processor must be established by means of contractual clauses or other legal instruments determined by the business; and it is necessary to prove the existence, scope and content of the relationship.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement must be in writing and signed by both parties. The agreement must contain at least the following obligations on the Processor: (i) to treat personal data according to the instructions of the business; (ii) to treat personal data for the purposes instructed by the business; (iii) to implement security measures in accordance with the Law, and other applicable provisions; (iv) to keep confidentiality regarding the personal data processed; (v) to delete all PI processed once the legal relationship with the business is over, or when the instructions of the business have been fulfilled, provided that there is no legal provision that requires the preservation of the personal data; and (vi) to refrain from transferring PI unless the business determines so, or when it is required by a competent authority. It is worth mentioning that agreements between the business and the Processor in relation to the treatment of personal data must be in accordance with the corresponding Privacy Notice.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Mexico does not have any specific regulations dealing with unsolicited text messages or spam emails, but the Federal Bureau for Consumer Protection operates a call-blocking registry, covering both landlines and mobile phone numbers, which gives suppliers 30 days to make marketing calls, send marketing messages and to stop disturbing the consumer at his/her registered address, electronic address, or by any other means. Likewise, all the marketing purposes must be specified clearly in the Privacy Notice.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Please refer to question 10.1 above.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please refer to question 10.1 above.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Please refer to question 10.1 above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Issues regarding marketing restrictions are regularly addressed by the Federal Bureau for Consumer Protection.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Since Mexican law expressly provides that the collecting or processing of any PI must be through lawful means, the purchasing of marketing lists, including any PI not collected in accordance with Mexican law, would not be deemed legal. 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 an easy opt-out from the marketing service.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

According to the Federal Consumer Protection Law, the maximum penalties for marketing breaches may reach the amount of MXN$1.9 million (approximately US$111,765).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Guidelines for drawing up the Privacy Notice require individuals be informed as to any technology that allows the automatic collection of PI simultaneously with the first contact with the individuals; data owners to request consent from individuals through an opt-in mechanism; and individuals to be informed as to how to deactivate said technology, unless said technology is required for technical reasons.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, they do not.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, they have not.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Although there is not any express infringement regulated in the Law in connection with the use of cookies, their use in

contravention of the Guidelines mentioned above would translate to an illicit collecting of PI, which would be sanctioned with a fine of up to US$1.5 million, and if the infringement persists, an additional fine of up to US$1.5 million may be imposed.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

If the Controller wishes to transfer any PI to any third parties, either domestic or foreign, it needs to obtain the informed consent of data subjects for the said data transfer, in advance, through the corresponding Privacy Notice. There are some cases where third parties do not require the consent of the data subject for the transfer of PI. According to Article 37 of the Law, consent will not be necessary only in the following cases:

(i) when expressly permitted by the Law;
(ii) when PI is available in publicly accessible sources;
(iii) when personal data has been dissociated;
(iv) when the collection of personal data is needed for compliance with obligations derived from a legal relationship between the data subject and the data owner;
(v) when there is an emergency situation that jeopardises the person or the commodities of the data subject; and
(vi) when the collection of PI is indispensable for medical attention and/or diagnosis, rendering sanitary assistance, and medical treatment or sanitary services, provided that the data subject is not in a condition to give consent, and provided that the data collection is performed by a person subject to legal professional privilege.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

As stated above, according to Article 36 of the Law, if a Controller wishes to transfer any PI to third parties, either domestic or foreign, it must obtain consent from the data subject in advance, through a Privacy Notice. When the transfer is performed, the vendor or third party will be obliged on exactly the same terms as the Controller, by means of an agreement that must be executed in writing.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no registration/notification requirement set forth in the Law for data transfers.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Conducting a transfer impact assessment is not mandatory under our Law, for transfer of personal data to other jurisdictions.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

There has been no guidance from the Mexican DPA following the decision of the Court of Justice of the EU in *Schrems II* (Case-311/18).

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

There has been no guidance in relation to the use of standard contractual/model clauses as a mechanism for international data transfer, directly issued by the Mexican DPA. However, as part of the Ibero-American Data Protection Network, the Mexican DPA contributed in the elaboration of the "Implementation Guide on Model Contractual Clauses for the International Transfer of Personal Information", which can be consulted at: https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-es.pdf (Available only in Spanish language).

This is not an official document and does not constitute any regulation. The principles discussed in this guide are still to be enacted in Mexican regulations and on the Mexican DPA's resolutions.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Whistle-blower hotlines can be put into operation, but the Law is silent as to any restrictions on the personal data that may be processed through them.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous and non-anonymous reporting is permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There is no registration or notification requirement for the use of CCTV.

14.2 Are there limits on the purposes for which CCTV data may be used?

The Law is silent as to the limits on the purposes for which CCTV data may be used.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In January 2021 there was an amendment to the Mexican Federal Labor Law, introducing the regulation of "telework", thus establishing the right of employers to monitor employees' activities working under this modality, and the obligation of employees to use the technology provided by employers in order to monitor the activities carried out under the modality of telework.

The monitoring of the employee is limited to the activities carried out under the modality of telework, and this amendment also recognises the right of employees to "disconnect", whenever they are not performing their work, in order to respect their privacy.

This amendment only established a general legal framework that will have to be detailed in the years to come.

The general rules set forth by this amendment will also have to be interpreted by the Mexican Courts on a case-by-case basis, in order to generate jurisprudence in this regard.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

A written agreement will have to be executed between the employer and employees working under the modality of telework, and in said agreement the consent to be monitored during working hours will have to be collected.

Also, since the collection, storage and use of any audio or video material featuring the voice and image of any individual within the workplace may be deemed a collection of PI, employers are required to give employees notice as to the use of video surveillance technology at workplaces.

The INAI has drawn up a short model Privacy Notice to be used by any individual or company introducing video surveillance technology on their premises.

Said summary Privacy Notice must be visible at the entrance to monitored spaces, and must inform individuals of the purpose of the surveillance and the treatment of the collected information.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Currently, it is not mandatory to consult or notify employees' representatives at works councils/trade unions. However, in light of the above-mentioned amendment, it may change in the near future when negotiating collective labour agreements for employees working under the modality of telework.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes, as long as an employment agreement exists that includes a data protection clause, by which an employer is entitled to monitor employees' attendance in office as a result of its internal policies and such policies are duly presented to employees.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Article 19 of the Federal Law for the Protection of Personal Data Held by Private Entities requires every Controller to implement and maintain administrative, technical and physical security measures, which protect the collected and stored PI from any loss, alteration, destruction or any unauthorised access and use.

Said measures cannot be lesser than those used by the data owner to protect its own information. For their implementation, the data Controller must consider the existing risk and the possible consequences for the data subjects, the sensitivity of the data, and technological developments. Therefore, security measures may vary from industry to industry, and from company to company.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is no legal requirement to report data breaches to the INAI, and so far, there are no guidelines for voluntary breach reporting to the INAI.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Mexican law sets forth that if any phase of collection, storage or use of data "may in any way affect in a significant manner the patrimonial or moral rights of individuals", data owners must immediately notify individuals about this situation.

However, so far there is no further explanation in the law or in the jurisprudence as to what is to be deemed a significant effect on the patrimonial or moral rights of data subjects.

Likewise, Article 64 of the Regulations of the Law requires data owners to notify individuals, without any delay, as to any breach that significantly affects their moral or patrimonial rights, as soon as the data owner confirms that a breach has occurred, and when the data owner has taken any actions towards starting an exhaustive process to determine the magnitude of the breach.

In said notification, data owners must state at least:

- the nature of the incident;
- the compromised PI;
- recommendations for the data subjects to protect their interests;
- the corrective measures immediately implemented by the data owner; and
- the means of obtaining more information regarding the breach.

16.4 What are the maximum penalties for personal data security breaches?

According to the Federal Consumer Protection Law, the penalties for personal data security breaches regarding marketing matters (as explained in question 10.7) are up to MXN$1.9 million (approximately US$111,765).

If the personal data authority (INAI) determines that a personal data breach is attributable to a Controller or Processor, a fine from MXN$24,900 (approximately US$1,464.70) up to MXN$79,680,000 (approximately US$4,687,058) may be imposed depending on the breach.

If the personal data security breach refers to sensitive personal data, then these amounts may be duplicated.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative Powers:** Verification proceeding: the INAI is entitled to conduct inspections *ex officio* at any company, in order to determine its compliance with the legislation on PI.

(b) **Corrective Powers:** The INAI is entitled to declare administrative infringements in order to enforce the ARCO rights of any individual, for omitting in the Privacy Notice any or all of the elements established in the Law, collecting or transferring personal data without the express consent of the holder, for obstructing the authority's acts of verification, and violating the security of databases, programs or equipment, when it is attributable to the responsible party, among others.

(c) **Authorisation and Advisory Powers:** The INAI is entitled to develop, promote and disseminate analyses, studies and research on the protection of personal data held by private parties and to provide training to regulated entities. It may also provide technical support to those responsible, upon request, for compliance with the obligations established in the Law.

(d) **Imposition of administrative fines for infringements of specified legal provisions:** The INAI is entitled to declare administrative infringements and impose administrative fines for non-compliance with any of the principles or provisions of the Law.

(e) **Non-compliance with a data protection authority:** The INAI is entitled to issue the criteria and recommendations, in accordance with the applicable provisions of this Law, for the purposes of its enforceability and operation.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

This authority is not expressly designated in the Law as the INAI. However, considering that the Law recognises the INAI as the specialised authority in charge of the protection of PI in Mexico, the INAI should be deemed as having the authority to ban a particular processing activity. However, if contested by any third party, any ban issued by the INAI should be validated by the Mexican Federal Administrative Courts.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

There are no recent cases or precedents illustrating the INAI's approach.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

So far there is no precedent for the INAI having exercised its powers against businesses established in other jurisdictions.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Any e-discovery requests or requests for disclosure from foreign law enforcement agencies must be validated by Mexican Courts for them to be validly enforced in Mexico. If any order or request from any foreign law enforcement agency is not validated through a Mexican Court, a company may refuse to comply with it.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been issued by our data protection authority on disclosure of personal data to foreign law enforcement or governmental bodies.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

There have been additional guidance criteria issued by the INAI in connection with the COVID-19 pandemic and enforcement actions, which are expected to increase in the near future.

19.2 What "hot topics" are currently a focus for the data protection regulator?

There have been no legislative changes or updates that have occurred during the last year in connection with the Mexican Data Protection legal framework.

On March 31, 2023, the Second Chamber of Mexican Supreme Court ruled that the INAI is an autonomous constitutional entity with regulatory authority, which means that the INAI may issue certain regulations necessary for its proper operation. This opens the door for the INAI to issue certain regulations aimed at improving the Data Protection system, without the need of having to wait for said regulations to be discussed and approved in Mexican Congress.

With the urgency to regulate artificial intelligence, changes to our data protection Law are expected in the near future to include additions to the definition of personal data such as biometric data.

Abraham Díaz co-chairs OLIVARES' Litigation Team, as well as Data Privacy and IT Industry groups, and focuses on trademark law, unfair competition, litigation, trade secrets and plant breeder's rights, as well as on data privacy matters. His Internet experience includes handling domain disputes under the Uniform Domain Name Dispute Resolution Policy (UDRP) and the Local Dispute Resolution Policy (LDRP), as well as providing strategic advice across a range of legal matters.

OLIVARES
Pedro Luis Ogazon 17
San Angel, 01000
Mexico City
Mexico

Tel: +52 55 532 23041
Email: abraham.diaz@olivares.mx
LinkedIn: www.linkedin.com/in/abrahamdiazarceo

Gustavo Alcocer, with more than 30 years of law firm and in-house experience, brings a wealth of knowledge to his domestic and foreign clients at OLIVARES, where he heads the Corporate, Commercial and Life Sciences Law Groups and co-chairs the Data Privacy and IT Industry Groups. His practice focuses on transactional work for companies across IP-intensive industries such as life sciences, information technology, food and beverage, transportation and retail.

OLIVARES
Pedro Luis Ogazon 17
San Angel, 01000
Mexico City
Mexico

Tel: +52 55 532 23000
Email: gustavo.alcocer@olivares.mx
LinkedIn: www.linkedin.com/in/gustavo-alcocer-5150b88

Carla Huitron has been a Member of the Corporate and Commercial Law Group since 2011, providing assistance to national and international clients. Among her work, she supports clients in drafting and reviewing documents such as: service, distribution and merchandise NDAs; franchise and licence agreements; structuring e-commerce, legal framework and marketplace compliance with Data Privacy; companies' by-laws or corporate minutes; and providing legal opinions on civil, commercial and data protection law, among others.

OLIVARES
Pedro Luis Ogazon 17
San Angel, 01000
Mexico City
Mexico

Tel: +52 55 5322 3000
Email: carla.huitron@olivares.mx
LinkedIn: www.linkedin.com/in/carla-huitron-piña-076940238

Our mission is to provide innovative solutions and highly specialised legal advice for clients facing the most complicated legal and business challenges in Mexico.

OLIVARES is continuously at the forefront of new practice areas concerning privacy compliance, corporate and commercial law, copyright, litigation, regulatory, anti-counterfeiting, plant varieties, domain names, digital rights and internet-related matters, and the firm has been responsible for precedent-setting decisions in patents, copyrights and trademarks.

Our firm is committed to developing the strongest group of legal professionals to manage the level of complexity and interdisciplinary orientation that clients require. During the first decade of the 21st century, the team successfully led efforts to reshape IP, privacy, corporate and commercial laws and change regulatory authorisations procedures in Mexico, not only through thought leadership and lobbying efforts, but the firm has also won several landmark and precedent-setting cases at the Mexican Federal and Supreme Courts levels, including in constitutional matters.

Today, the team at OLIVARES includes 11 partners and more than 45 associates working across IP, regulatory, administrative, civil, commercial and corporate law and privacy compliance, serving many different industries, and is constantly awarded for excellence in legal service.

We aim to utilise every available resource to help clients achieve optimum results, protecting their business interests, intellectual property and other rights at every level and through the applicable administrative or judicial venue, in order to maximise successful outcomes – all while maintaining an overarching goal of contributing to Mexico's broader stance in the global economy and for the greater good of the Mexican people.

www.olivares.mx

OLIVARES®
we know

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2024 includes two expert analysis chapters and 31 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Definitions
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group