Mexico


Abraham Díaz Arceo


Gustavo Alcocer

OLIVARES

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The legal framework for data protection is found firstly 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 "Law").

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

Yes: the General Law for the Protection of Personal Data in the Possession of Obliged Subjects which regulates the processing of personal information in the possession of any Federal, State or local authority ("the Law"); the Privacy Notice Rules, published in January 2013; and the Binding Self-Regulation Parameters, also published in January 2013. 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 personal information ("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. The 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**"
  Any personal data which 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.
- "**Data Breach**"
  Data Breach means any security breach which occurred in any phase of the data collection, storage or use, which may affect in a significant manner the patrimonial or moral rights of individuals.

Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data").

- **"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 personal information.
- **"Consent"**
  An expression of will made by any data subject, of 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 personal information 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 personal information 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.

3 Territorial 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?

Businesses located outside Mexico will be subject to the terms of the Privacy Notice, and to the Law, only when the Controller transfers personal data collected in Mexico, in accordance with the provisions of the Law.

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 Collector 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 processed for 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 processed in a clear, objective manner, not leaving any room for confusion.
- **Data minimisation**
  The Collector 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 Collector 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.
- **Responsibility**
  The Collector must safeguard and be accountable of 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 shall obtain the consent of the data subject, prior to the collection of any personal information, 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 data/copies of data**
  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 turn 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 owners have the right to object to the processing of their personal data due to a legitimate reason.
- **Right to restrict processing**
  Data owners have the right to restrict the processing of their personal data due to a legitimate reason.
- **Right to data portability**

The data owner has the right to obtain, from the subject concerned, a copy of his/her processed data, which allows the data subject to continue using his/her personal information.

- **Right to withdraw consent**
  At any time, the data owner may withdraw his/her consent for the treatment of his/her personal data. The Controller must establish simple and free mechanisms which 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 owners have the right to oppose the use of their personal data for marketing or advertising purposes.
- **Right to complain to the relevant data protection authority(ies)**
  Data owners are entitled to submit a claim before the INAI. The claim must be filed in writing and shall 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 owner has been communicated by the Controller.

Other key rights – please specify

- **Right to a verification procedure**
  Data subjects will have the right to request before the data protection authority (INAI), a verification procedure, by which the authority will check the Controller's compliance with all the provisions set forth in the Law, or any other applicable regulations.

6 Registration Formalities and Prior Approval

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

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

This is not applicable.

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

This is not applicable.

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

This is not applicable.

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

This is not applicable.

6.10 Can the registration/notification be completed online?

This is not applicable.

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

This is not applicable.

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

This is not applicable.

7 Appointment of a Data Protection Officer

7.1 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.

7.2 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 regulated as an infringement yet.

7.3 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.

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

Yes, it can.

7.5 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.

7.6 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.

7.7 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.

7.8 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 of the person or department that will be responsible for the collection, use and storage of the personal data.

8 Appointment of Processors

8.1 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.

8.2 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 shall be in writing and signed by both parties. The agreement shall contain at least the following obligations on the Processor: i) to treat only personal data according to the instructions of the business; ii) to treat only 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.

9 Marketing

9.1 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 regulation dealing with unsolicited text messages or spam emails, but the Federal Bureau for Consumer Protection operates a call-blocking registry ("REPEP"), covering both landlines and mobile phone numbers, which gives suppliers 30 days to stop making marketing calls, sending 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 have to be specified clearly in the Privacy Notice.

9.2 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 9.1 above.

9.3 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 9.1 above.

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

Please refer to question 9.1 above.

9.5 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.

9.6 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 personal information has to be through lawful means, the purchasing of marketing lists, including any personal information 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.

9.7 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$1,798,305.81 (approximately US$71,600).

10 Cookies

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

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

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

No, they do not.

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

No, they have not.

10.4 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 to the Guidelines mentioned above would translate to an illicit collecting of PI, which would be sanctioned with a fine of up to US$1,500,000, and if the infringement persists, an additional fine of up to US$1,500,000 may be imposed.

11 Restrictions on International Data Transfers

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

If the Controller is willing 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 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 allowed 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; for rendering sanitary assistance; for 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.

11.2 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 any Controller is willing 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 in exactly the same terms as the Controller, by means of an agreement that has to be executed in writing.

11.3 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 Whistle-blower Hotlines

12.1 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.

12.2 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 allowed.

13 CCTV

13.1 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.

13.2 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.

14 Employee Monitoring

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

Mexican legislation is silent as to the types of employee monitoring that are permitted and the circumstances under which said monitoring is allowed.

Therefore, the balance between the monitoring that can be carried out by employers and the respect of the privacy of employees is to be found in the general rules set forth in Articles 6 and 16 of the Mexican Constitution, which regulate the right to privacy, and the general rules established by the legislation on data privacy. These rules should be interpreted by the Mexican Courts on a case-by-case basis, in order to generate jurisprudence in this regard.

For instance, video surveillance of public spaces in workplaces is allowed, while surveillance in restrooms and locker rooms is prohibited.

Monitoring phone calls made by employees is allowed, but only to determine the persons on the phone call and the length of the call, and not the content of the call.

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

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.

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

Employee representatives at works councils/trade unions do not need to be either consulted or notified.

15 Data Security and Data Breach

15.1 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 Information in the Possession of 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 from 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 owner 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.

15.2 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.

15.3 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 shall 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.

15.4 What are the maximum penalties for data security breaches?

According to the Federal Consumer Protection Law, the penalties for data security breaches regarding marketing matters are up to MXN$1,798,305.81.

On the other hand, the INAI is entitled to impose administrative sanctions such as fines of up to MXN$39,430,400 (approximately USD$1,500,000).

Additionally, there are two activities deemed as felonies related to the wrongful use of PI, which are:

i) When a data owner authorised to collect, store and use PI with the aim of profit-making, causes a security breach in the database containing PI under its custody. This is sanctioned with imprisonment for three months to three years.

ii) To collect, use or store PI with the aim of profiting through error or deceit of the data subject, or error or deceit of the person who has to authorise the transfer. This is sanctioned with imprisonment for six months to five years.

16 Enforcement and Sanctions

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

Investigatory/ Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
The INAI is entitled to conduct visits of inspection *ex officio* at any company, in order to determine its compliance with the legislation on PI. The INAI is also entitled to pursue and resolve any complaint in order to enforce the ARCO rights of any individual.	The INAI is not entitled to declare damages, thus it is necessary to file an independent civil action before the Mexican Civil Courts to that effect.	As stated above, the Law provides some criminal sanctions if there is an intention to profit from the security breach of PI. However, the INAI is not entitled to prosecute criminal actions, thus it is necessary to file the corresponding criminal complaint before the Attorney General's Office, and the criminal action will be decided by a Criminal Court.
Not applicable.	The administrative infringements set forth in the Law are prosecuted before the INAI, and the ruling that this authority issues, can be appealed to the Federal Court for Administrative Affairs. The decision that this Court issues can be further appealed through a constitutional rights action, known as *Amparo*, before the Federal Circuit Courts.	Not applicable

16.2 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.

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

There are no recent cases or precedents illustrating this authority's approach.

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

Please refer to question 16.1 above.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 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 have to be validated by Mexican Courts, in order that they may 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.

17.2 What guidance has/have the data protection authority(ies) issued?

In connection with e-discovery and disclosure to foreign law enforcement agencies, no guidance has been issued by the INAI.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There are no enforcement trends which have emerged during the previous 12 months.

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

Currently, the INAI is looking forward to Mexico joining the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Protocols ("Convention 108+"), as well as making the corresponding amendments to the Federal Law for the Protection of Personal Information Held by Private Entities, in accordance with the provisions of said Convention.

Abraham Díaz Arceo co-chairs OLIVARES' Privacy and IT Industry Groups and has a wealth of knowledge across all areas of intellectual property ("IP"), with a focus on copyright, trademarks, unfair competition, litigation, licensing and prosecution matters. He also handles domain disputes under the Uniform Domain Name Dispute Resolution Policy ("UDRP") and the Local Dispute Resolution Policy ("LDRP") and provides strategic advice on website development, protection of website content, online advertisement, and compliance with e-commerce and privacy law regulations. Mr. Díaz has authored articles on IP and Internet matters, as well as on privacy law, for leading industry publications, and has lectured on cutting-edge IP topics in national and international fora. His representative cases include defence of the producers of the documentary film *Presunto Culpable* from various civil law suits filed by individuals portrayed in this work, which set the basis for regulations now applicable to the documentary film industry in connection with the use of a person's image.

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

Tel: +52 55 5322 3041
Email: abraham.diaz@olivares.mx
URL: www.olivares.com.mx

Gustavo Alcocer manages the Corporate and Commercial Law Group and co-chairs the Privacy and IT Industry Groups at OLIVARES, advising domestic and foreign businesses, and the owners of those businesses, on Mexican and cross-border corporate and commercial transactions. He serves as outside general counsel in Mexico to many of his domestic and foreign clients, and has significant experience in domestic and cross-border transactions. With more than 30 years of law firm and in-house practice experience, Mr. Alcocer possesses a wealth of transactional knowledge of M&A, finance and business law, and advises clients across IP-intensive industry sectors such as life sciences, information technology, food and beverage, leisure, and retail. Clients routinely turn to him for sophisticated strategic advice regarding structuring, maintaining and expanding operations in Mexico, as well as on valuation and monetisation. He has published articles in leading industry publications including *Managing Intellectual Property*, *Getting the Deal Through*, and *International Comparative Legal Guides (ICLG)*.

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

Tel: +52 55 5322 3000
Email: gustavo.alcocer@olivares.mx
URL: www.olivares.com.mx