Contributors Abraham Diaz Arceo, Gustavo Alcocer

The ICLG to: Data Protection Laws and Regulations covers relevant legislation and competent authorities, territorial scope, key principles, individual rights, registration formalities, appointment of a data protection officer and of processors - in 42 jurisdictions

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 possession of any Federal, State or local authority); 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, regulation 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, the Federal Consumers Law and some specific provisions set forth in the Civil Code and the Commerce Code.

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 implies 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 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, transfer or disposal of personal data.

- **"Controller"**

The individual or private legal entity that determines the treatment of personal data.

- **“Processor”**

The individual or legal entity that solely or jointly with another processes personal data on behalf of the Controller.

- **“Data Subject”**

An identified or identifiable natural person.

- **“Sensitive Personal Data”**

Personal data which concerns the private life of an individual, or the misuse of such information which 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 ethnical 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 to the personal data processing.

- **“Consent”**

An expression of will made by the data owner concerning data collection.

- **“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 in 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 others, about: the terms for the collection of personal data; the identity of the Controller; the purpose of the data collection; the possible transfers of data; and the mechanisms for enforcing the ARCO rights.

- **“Transfer”**

Any data communication made to a different 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 data 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 also makes 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 the compliance of 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 giving room for confusion.

- **Data minimisation**

The Collector will be responsible and shall endeavour to make reasonable efforts so that the personal data processed are of the minimum necessary, according to the purpose that originated the collection of PI.

- **Proportionality**

Data controllers can only collect personal data that are necessary, appropriate and relevant for the purpose(s) of the 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 was collected, with the obligation to block, cancel and suppress the personal data afterwards.

Other key principles – please specify

- **"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 for this effect.

- **"Quality"**

This principle is accomplished when 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, in advance, with the aim of processing any PI, and must keep evidence of the consent.

- **"Loyalty"**

This consists of the obligation of the data 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 data 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 data controller, if it is inaccurate, incomplete or dated.

- **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 data controller may keep such personal data exclusively for the purposes of the responsibilities regarding the treatment. Likewise, the Law establishes some cases where the data 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 obliged subject 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, for which the data 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 data controller.

Other key rights – please specify

- **Right to a verification procedure**

Data subjects will have the right to request before the data protection authority ("DPA"), a verification procedure, in which the authority will check the data 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.

Yes, 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?

The failure in appointing the 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, they 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 or department at least with the following qualifications: i) data privacy expertise; and ii) enough authority and resources to implement measures in order to protect the personal data.

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 the 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?

No, it is not mandatory to appoint a Data Protection Officer, being only 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 for 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 the agreements between the business and the Processor related to the treatment of the personal data must be in accordance with the corresponding Privacy Notice.

9. Marketing

<div ">

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, called 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.

9.2 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.

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

Please refer to question 9.1 above.

9.4 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.

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

Yes, but in the Privacy Notice the Controller must provide detailed information as to the data transfers that it is willing to make, involving PI, expressly indicating the name of the data processor(s), of the type, category of activity sector of the latter; and expressly indicating the purpose(s) of such transfer(s). Also, when required, a clause indicating whether or not the data subject consents to the data transfer should be included.

9.6 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$1,317,141.34 (approximately US$70,000).

10. Cookies

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

Yes. The Guidelines for elaborating the Privacy Notice require that individuals are informed as to any technology that allows the automatic collection of PI simultaneously to the first contact with the individuals; requiring data owners to request the consent from individuals through an opt-in mechanism, and informing individuals 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 fines of up to US$680,000, and if the infringement persists, additional fines of up to US$1,300,000 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 FLPPIPPE, consent will not be necessary only in the following cases:

i) when expressly allowed by the Law;

ii) when PI is available in public access 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 FLPPIPPE, 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 exactly in the same terms as the Controller.

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 set 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 made 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 regulates 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 at restrooms and locker rooms is prohibited.

Monitoring phone calls made by employees is allowed, but only to determine the user of 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 as a collection of PI, employers would be required to give employees notice as to the use of video surveillance technology at workplaces.

The Mexican DPA has drawn up a model short 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 of the 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 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 Possession of Private Entities requires every data controller to implement and maintain administrative, technical and physical security measures, which prevent 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, and for its implementation the data owner must consider the existing risk and the possible consequences for the data subjects, the sensitivity of the data and the technological development.

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 Mexican DPA, and so far, there are no guidelines for voluntary breach reporting to the Mexican DPA.

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.

If any phase of the data collection, storage or use 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.

Likewise, Article 64 of the Regulations of the FLPPIPPE 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 for getting 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 range from MXN$260.56 to MXN$833,823.71.

On the other hand, the Mexican DPA (INAI) is entitled to impose administrative sanctions such as fines of up to MXN$25,000,000 (approximately USD$1,400,000).

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

i) When a data owner authorised to collect, store and use PI with the aim of profiting, causes a security breach in the database containing PI under its custody. This is sanctioned with imprisonment from 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 from six months to five years.

16. Enforcement and Sanctions

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

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

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

So far 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, so that they can 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 Mexican DPA.

18. Trends and Developments

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

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

However, at the time of writing this article, as a result of an investigation process started by the Mexican DPA (INAI), in February 2019, related to a data breach at KPMG Mexico, INAI is raising its voice as to the need to modify Mexican data protection law, in order to include an obligation to notify the DPA in case of a data breach.

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

In June 2018, Mexico joined the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), and the additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181). This constitutes a very important step for Mexico towards the enhancement of personal information, since these documents bind Mexico into carrying out the automatic processing of personal information, in accordance to European standards. At the same time, this provides international tools that will enhance trans-border data flows, which should trigger foreign investment into Mexico.

A lot of buzz was also created by the entering into force of the GDPR in May 2018, which posed the question to many Mexican companies, as to whether or not there was something additional to be done in order to comply with the GDPR, as well as complying with domestic privacy law.