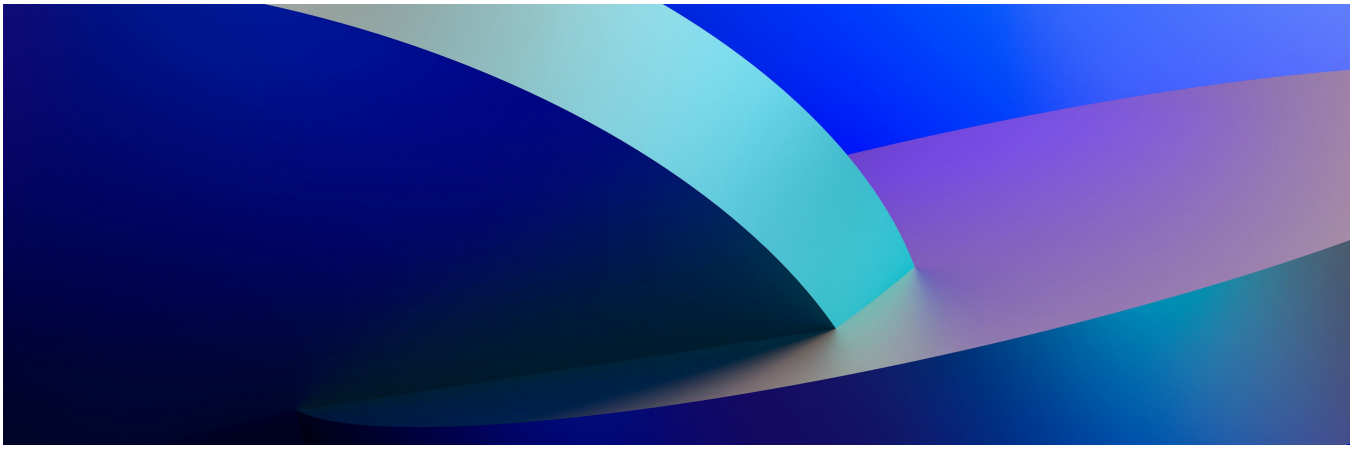


Data protection and cybersecurity laws in Mexico

Data protection

1. Local data protection laws and scope

The main data protection legislation for private parties is the Federal Law on the Protection of Personal Data held by Private Parties (the "**Data Protection Law**") and its supplementary regulation (the "**Data Protection Regulations**"), together the "Data Protection Legislation". The Data Protection Law came into force in July 2010 and the Data Protection Regulation came into force in December 2011.

For government and regulated entities, such as autonomous entities, political parties, public funds etc., there is the General Law on the Protection of Personal Data held by Public Entities (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*). This law regulates government access to personal data from the overall public.

The Data Protection Law was amended in March 2025, this follows a constitutional reform passed in December 2024, to reduce autonomous entities and absorb the relevant functions by government institutions (the "**Constitutional Reform**").

The Data Protection Law remained substantially the same, however one of the most relevant changes is that it changed the definition of personal data from "physical person" (*persona física*) to a more ambiguous "person" which may include companies or other types of entities. This has not yet been addressed in the secondary regulations but can have an important impact on the overall data protection ecosystem in Mexico.

Other relevant legislation containing data protection provisions includes:

- Articles 6 to 16 of the Mexican Constitution;
- The Privacy Notice Guidelines, which govern the content of data privacy notices and obtaining consent for processing personal data;
- The General Law for the Protection of Personal Data in Possession of Obligated Subjects governs personal data held by public bodies; and

- The Federal Consumer Protection Law governs certain aspects concerning marketing activities.

Mexico is a signatory of international agreements on Data Protection, like the Convention for the Protection of the People Regarding the Automated Treatment of Personal Information. Mexico is also a member or the Inter American Network of Data Protection.

Additionally, following the aforementioned Constitutional Reform and the amendment to the Data Protection Law, the new secondary regulation, guidelines or official recommendations have not yet been issued by the relevant authority.

Please note that the previous authority had issued different non-binding guides detailing different subjects such as:

- Security Management System for Personal Data.
- Criteria for the hiring of Computing Services in the Cloud (related to cybersecurity).
- Biometric Personal Data Guide.
- Best Practice Code for the Processing of Personal Data from Minors.
- Recommendations for the Processing of Personal Data resulting from the use of Artificial Intelligence.

These guides are provided in the site of the extinct INAI (https://home.inai.org.mx/) (the "**INAI Guides**"), and will be slowly migrated to the new authority sitestransparencia.gob.mx and www.gob.mx/buengobierno.

2. Data protection authority

Following the amendment to the Data Protection Law, Ministry of Antibribery and Good Government (*Secretaría de Anticorrupción y Buen Gobierno*) (The "**Ministry**"), is responsible for overseeing the Data Protection Legislation. Its aim is to encourage access to all public information about governmental activities, and budgets, as well as seeking the protection of personal data and the right to privacy.

The Ministry, if requested by a data subject, may carry out an investigation to ensure compliance with the Data Protection Legislation of a specific undertaking and sanction those found to be in breach the Data Protection Legislation.

3. Anticipated changes to local laws

Following the Data Protection Law amendment and the dissolution of the INAI (Federal Institute for Access to Information and Data Protection (*Instituto Nacional de Acceso a la Información y Protección de Datos Personales*) ("**INAI**"), the Ministry has yet to issue secondary regulations to the Data Protection Law.

Additionally, the non-binding guides provided in INAI's site are being migrated to the new Ministry sites as provided in section 1 above. The non-binding guides can still be used as references for best industry practices.

4. Sanctions & non-compliance

The Ministry has the authority to impose the following administrative fines:

- 100 to 160,000 units of measure for:
  - Acting negligently or fraudulently in processing and responding to requests for personal data access, rectification, cancellation or objection;
  - Fraudulently declaring the inexistence of personal data where such exists in whole or in part in the databases of the Data Controller;

- Processing personal data in violation of the principles established in the Data Protection Law;
- Omitting from the Privacy Notice any or all of the information it requires;
- Maintaining inaccurate personal data when such action is attributable to the Data Controller, or failing to perform legally due rectifications or cancellations where the data subject's rights are affected; and
- Failure to comply with the notice warnings issued by the Ministry.

- 200 to 320,000 units of measure for:
  - Breaching the duty of confidentiality set out in the Data Protection Law;
  - Materially changing the original data processing purpose in contravention of the Data Protection Law;
  - Transferring data to third parties without providing them with the Privacy Notice containing the limitations to which the data subject has conditioned data disclosure;
  - Compromising the security of databases, sites, programmes or equipment;
  - Carrying out the transfer or assignment of personal data outside of the cases where it is permitted under the Data Protection Law;
  - Collecting or transferring personal data without the express consent of the data subject where required;
  - Obstructing verification actions of the Ministry;
  - Collecting data in a deceptive and fraudulent manner;
  - Continuing with the illegitimate use of personal data when the Ministry or the data subjects have requested such use be ended;
  - Processing personal data in a way that affects or impedes the exercise of the rights of access, rectification, cancellation and objection set;
  - Creating special data databases in violation of the Data Protection Law.

In the event that the infractions mentioned in the preceding paragraphs persist, an additional fine of 100 to 320,000 units of measure 3 can be imposed.

Sanctions may be doubled for any of the above infractions committed in the treatment of sensitive data.

The value for the unis of measure is annually updated, for 2025, the daily value for the unit of measure is MXN 113.14, roughly USD 5.00.

5. Registration / notification / authorisation

The Data Protection Legislation does not require prior notification or registration for any data processing activities.

6. Main obligations and processing requirements

The Data Protection Law recognises two parties who deal with personal data:

- **Data Processors**: the subject or legal entity that processes personal data on behalf of the Data Controller.
- **Data Controller**: the subject or legal entity that decides on the processing of personal data.

Their relationship must be established through contractual clauses or other legal instruments in a way that proves the existence, scope and nature of such relationship.

According to the Data Protection Legislation, the principles that must be observed by controllers and/or processors in the processing of personal data are the following:

- **Legitimacy**: Personal data must be collected and processed in a lawful manner;

- **Consent**: The data subject must give its consent for the processing of its personal data;
- **Information**: Through a Privacy Notice, the Data Controller must inform the data subject about the existence and the characteristics of their personal data processing;
- **Quality**: This principle is given when the personal data is provided directly by the data subject; if not, the Data Controller must take the measurements to meet the quality principle and adopt mechanisms that are considered necessary to ensure that the data is accurate, complete, updated and correct;
- **Purpose**: Personal data can only be processed for the purposes established in the Privacy Note.
- **Loyalty**: Personal data must be processed safeguarding the protection of the data subjects' interests and the reasonable expectation of privacy;
- **Responsibility**: Data Controllers must ensure the processing of personal data in their custody, as well as the data transferred to a Data Processor.

Additionally, the following legal requirements should be taken into account when processing personal data:

- Personal data must be collected and processed in a lawful manner in accordance with the provisions established by the Data Protection Legislation and other applicable regulations;
- Personal data must not be obtained through deceptive or fraudulent means;
- In all processing of personal data, it is presumed that there is a reasonable expectation of privacy, understood as the trust any one person places in another for personal data provided to be treated pursuant to any agreement of the parties in the terms established by the Law;
- Personal data should not be kept for any longer than is necessary in order to comply with the purposes for which the personal data was originally held. Data Controllers must establish and document retention procedures, including deletion and/or blocking of personal data, taking the nature of the data into account.

7. Data subject rights

All data subjects are entitled to exercise rights of access, rectification, cancellation and objection regarding their personal data (collectively known as ARCO rights). These rights are not mutually exclusive.

Right of Access

The data subject is entitled to access its personal data held by the Data Controller, as well as information regarding the conditions and generalities of the processing.

Right of Rectification

Data subjects may request, at any time, that Data Controllers rectify personal data if it is inaccurate or incomplete.

Right of Cancellation

Data subjects have the right to cancel (i.e. seek erasure of) its personal data. There are certain situations where Data Controllers have the right to object to such erasure (e.g. if required by applicable law or public interest).

Right of Objection

Data Subjects may, at any time, oppose the processing of their personal data for legitimate purposes.

8. Processing by third parties

According to the Data Protection Law, if the Data Controllers intend to transfer personal data to third

parties, it must provide them with a Privacy Notice and the purposes to which the data subject has limited data processing. The data subject must consent to such transfer via the Privacy Notice.

Subcontracting

Data Processors must obtain permission from Data Controllers if subcontracting may involve the subcontractor processing personal data. Once consent is obtained, the Data Processor must enter into a contract with the subcontractor.

The subcontractor will assume the same obligations required for Data Processors under the Data Protection Legislation and other applicable law.

The Data Processor's right to subcontract processing activities should be outlined in the contract between the Data Controller and Data Processor. If this right is not covered in that contract, the Data Processor must seek specific consent from the Data Controller in order to subcontract processing activities.

9. Transfers out of country

International transfers of personal data must be consented to by the data subject and the purposes of such transfers must be included in the Privacy Notice. Such consent is not required where the transfer is:

- pursuant to a Law or Treaty to which Mexico is party;
- necessary for medical diagnosis or prevention, healthcare delivery, medical treatment or health services management;
- made to holding companies, subsidiaries or affiliates under common control of the Data Controller, or to a parent company or any company of the same group as the Data Controller, operating under the same internal processes and policies;
- necessary by virtue of a contract executed or to be executed in the interest of the data subject between the Data Controller and a third party;
- necessary or legally required to safeguard public interest or for the administration of justice;
- necessary for the recognition, exercise or defence of a right in a judicial proceeding; or
- necessary to maintain or fulfil a legal relationship between the Data Controller and the data subject.

10. Data Protection Officer

Data Controllers must appoint a Data Protection Officer (or equivalent role) to deal with data subjects' requests and promote data protection compliance within the Data Controller's organisation.

11. Security

Data Controllers and Data Processors are required to establish and maintain administrative and physical, security and, if applicable, technical measures for the protection of personal data.

In developing security measures, the data controller should take at least the following into account:

- the inherent risk given the type of personal data;
- the sensitivity of the personal data;
- technological developments;
- the potential consequences of a breach for data subjects;
- the number of data subjects;
- prior vulnerabilities in the processing systems;
- value of the data for an unauthorised third party; and

- other factors that may impact the level of risk or that result from other applicable laws and regulations.

The Data Protection Regulation also sets out actions that Data Controllers can take in order to comply with the security requirements:

- prepare an inventory of personal data;
- determine the functions and obligations of the person(s) who will process personal data;
- conduct a risk analysis of personal data consisting of identifying dangers and estimating the risks;
- establish the necessary security measures;
- identify gaps between existing security measures and those required for each type of data and each processing system;
- prepare a work plan based on the gap analysis in (v) above;
- carry out revisions and/or audits;
- train personnel who process personal data; and
- keep a record of the methods of processing personal data.

The non-binding INAI Guides provide information regarding the Data Protection Security Management System and other security recommendations, encouraging data processors to adopt updated technical and organizational safeguards, including encryption standards and access controls. Although not mandatory, these guides are considered as best practices in the data protection industry even considering the dissolution of the INAI.

12. Breach notification

There are no requirements for Data Controllers to notify the Ministry in the event of a data breach (other than Data Controllers which are government entities). However, Data Controllers must notify data subjects if their personal data is subject to a breach with at least the following information:

- nature of the breach;
- the personal data compromised;
- recommendations of actions that may be taken by the data subject to protect its interests;
- immediate measures being taken by the data controller; and
- any means by which the individual can find further information regarding the matter.

13. Direct marketing

Personal data can be processed for advertising and marketing purposes in accordance with the Data Protection Legislation, provided that these purposes are made clear in the Privacy Notice and in any other medium required for communicating the processing purposes.

14. Cookies and adtech

When the Data Controller uses remote or local mechanisms for electronic, optical or other forms of technological communication which allow collection of personal data automatically and simultaneously to the time the data subject has contact with such communications mechanisms, the data subject must be informed about the use of these technologies, at the time the data subject makes contact with the technology and must be informed of the obtention of personal data as well as the way in which the cookies can be disabled.

15. Risk scale

Moderate.

Following the amendment to the Data Protection Law and the commencement of the Ministry’s

functions, the risk scale remains moderate, given that enforcement activity has not drastically increased. However, heightened public awareness of data protection issues in Mexico has led to more frequent inquiries to the extinct INAI and a growing trend of private enforcement actions.

Cybersecurity

1. Local cybersecurity laws and scope

There is currently no specific federal cybersecurity law in force in Mexico.

Cybersecurity is regulated in the Federal Criminal Code, the Data Protection Legislation and other sector-specific legislation applicable to entities operating within those sectors (e.g. the Fintech Law). Specific cybersecurity measures are normally regulated through tertiary regulatory instruments such as manuals, official operating parameters and guides.

In the INAI continued to emphasize the importance of risk-based security measures. In the non-binding INAI Guides it provides updated guidance on security standards, referencing international frameworks such as ISO/IEC 27001:2022 as benchmarks for both data controllers and processors. These are still recommendations rather than binding regulations.

2. Anticipated changes to local laws

A National Cybersecurity Strategy document was published in 2017, but since the change in government in December 2018, there has not been much progress in terms of actual regulation.

In February 2020, a Mexican Senator submitted a bill proposing amendments to the Data Protection Law (the “DP Bill”).

The DP Bill proposed implementing best practices with respect to cybersecurity but made no specific recommendations.

There have been no developments regarding the DP Bill since it was announced in February 2020.

In April 2023, a Mexican member of the House of Representatives submitted a bill proposing a Federal Cybersecurity Law.

There have been no developments regarding the Federal Cybersecurityy Law since it was announced.

3. Application

With the recent changes following the Constitutional Reform, it is unlikely that the DP Bill will be passed as the Data Protection Law was recently amended, and there is no indication of when (or if) the Federal Cybersecurity Law will be passed.

4. Authority

The primary authority in charge of responding to any issue regarding cybersecurity is the National Guard (previously Federal Police, now formally though not materially fully integrated into the National Guard) and the Ministry of Public Security. Additional to this, there are other local authorities in some regions, such as the Police for the Prevention of Cybercrimes in Mexico City.

The Ministry is responsible for overseeing personal data security breaches in general.

There are other authorities that could have jurisdiction regarding sector-specific cybersecurity breaches e.g. the Mexican Securities and Exchange Commission or Mexico’s Central Bank in case of cybersecurity breaches in the banking and financial sector.

5. Key obligations

Given there is no legislation specifically regulating cybersecurity, companies operating in sectors that do not have their own cybersecurity requirements are not subject to any particular obligations.

Similarly, there is no obligation to report cyber incidents to the authorities. However, gaining access or trying to access a protected system is considered a crime in Mexico and therefore the offended party has the capacity to report the crime to Federal Prosecutors.

With respect to personal data, under the Data Protection Legislation, every organisation must implement corrective and preventive measures to improve security and avoid the violation personal data rights. In any case, the recommendations provided in the non-binding INAI Guides can be used as a baseline for cybersecurity practices.

Certain sectors, such as banking, have seen new guidelines from the Mexican Central Bank to bolster cybersecurity requirements for financial service providers. Nevertheless, no cross-sector or federal cybersecurity statute has been enacted.

6. Sanctions & non-compliance

Even though there is no definition of “cybercrime”, the Federal Criminal Code sanctions some behaviours that can be identified as cybercrimes, such as hacking, phishing, infections of IT systems with malware, identity theft or fraud. These illegal behaviours can be punished with prison sentences and a range of fines, depending on the severity of the crime.

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

The authority responsible for the prevention and response of any cybersecurity issue is the National Response Centre for Cyber Incidents of the Federal Police (now formally incorporated to the National Guard) or CERT-MX. This body is in charge of preventing and mitigating any threat to technological infrastructure and operability in Mexico. Additionally, the Ministry is responsible for supervising compliance with legislation regarding personal data protection.

8. National cybersecurity incident management structure

The CERT-MX is responsible for dealing with any cybersecurity incidents, but only after a specific request, complaint or demand is submitted. The Ministry can also initiate investigations regarding the protection of personal data.

9. Other cybersecurity initiatives

In the private sector, the Mexican Association for Cybersecurity offers services and products regarding cybersecurity and data protection. It also encourages the protection of information and proper information handling.

Key Contacts



Cesar Armando Lechuga Perezanta
Mexico City
Partner
Head of Real Estate

Authors

Héctor Gerardo González Martínez
Senior Associate
left_cms