LATIN LAWYER REFERENCE DATA PROTECTION & CYBERSECURITY 2019

Mexico

Carmina Mogollón González
Greenberg Traurig

FEBRUARY 2019

LATIN LAWYER INSIGHT

1 Is there any provision in your country's law for privacy and data protection?

Mexico has a sophisticated and thorough personal data protection legislation. The rights to privacy and to the protection of personal data are recognised under the Mexican Constitution and the Federal Law on the Protection of Personal Data Held by Private Parties (the Mexican DP Law). The National Institute for Transparency, Access to Public Information and Personal Data Protection (INAI) is the governmental entity responsible for increasing awareness among the Mexican society about the right to data protection and of encouraging data subjects to exercise such right (the DP Agency). The DP Agency is also responsible for supervising and enforcing compliance with the Mexican DP Law by private parties that hold personal data.

On 1 October 2018, the Convention for the protection of individuals with regard to the processing of personal data – known as Convention 108 – and its Additional Protocol entered into force in Mexico. Mexico became the 53rd Party and the second Latin American country to accede to the Convention 108. Convention 108 was concluded in 1981 and an amending protocol was adopted on 18 May 2018 to modernise it. This Convention is opened for signature by member states of the Council of Europe and for accession by non-member states and serves as a multilateral legal framework to facilitate cross-border transfers of personal data and provides safeguards for the protection of personal data.

2 Is privacy or personal data protection a fundamental right in your country?

It is, privacy (including the right to intimacy and the right to be let alone) and the protection of personal data are recognised as fundamental human rights by the Mexican Constitution. Under article 16 of the Constitution, a person's body, family, home, documentation, personal communications and possessions are private and third parties should abstain from intruding onto them, except if ordered by an authority through a duly substantiated request. The same article provides that all individuals are entitled to the protection of their personal data and have the right to access, rectify, cancel and oppose to the processing of their personal data. Further, paragraph II of section A of article 6 of the Constitution provides that information related to the private life and the personal data of an individual must be protected by law. Such right is a limit to the fundamental right to access public information maintained by the government, which is also available under the Mexican Constitution.

3 Has your country adopted a general legal framework for the protection of personal data?

The Mexican DP Law was enacted on 5 July 2010 per mandate of the Mexican Constitution. The Mexican DP Law is a law of public order and of general observance throughout the Mexican territory. Its main purpose is the protection of personal data held by private parties. This law regulates the legitimate, controlled and informed processing of personal data and protects people's right to informational self-determination. The Mexican Data Protection Regulations were enacted on 21 December 2011 by Mexico's executive branch, with the main purpose of regulating the provisions set forth in the Mexican DP Law.

Please note that as described in the response to question 26, the processing of personal data controlled by government entities is specifically regulated in the General Law for the Protection of Personal Data held by Government Entities, enacted on 26 January 2017. All answers contained in this chapter refer to the processing of personal data by parties pertaining to the private sector and, thus, the law of 26 January 2017 is outside its scope.

4 Has your country adopted a general legal framework on cybersecurity matters?

The Mexican DP Law is a comprehensive law that also regulates cybersecurity matters. In accordance with such statute, all private parties that process personal data are bound by a duty of care or security duty, under which they must implement and maintain technical, administrative and physical security measures to protect personal data against damage, loss, alteration and deletion and against unauthorised or unlawful use, access or processing. The security measures implemented by data controllers must provide, at least, the same level of protection as those used and implemented to safeguard the controller's own information. Data controllers should consider diverse factors when designing and implementing security measures, including: (i) the potential risk and undesired effects on the data subjects in case of a breach; (ii) the type of data that is processed – note that sensitive data as well as financial or asset data are subject to enhanced protection, (iii) the technological development; (iv) the number of data subjects; (v) previous data breaches; and (vi) the databases potential value to third parties not authorised to access the data. Chapter III of the Regulations of the Mexican DP Law (Security Measures in the Processing of Personal Data) regulates cybersecurity matters and sets forth a catalogue of suggested actions.

The Mexican DP Agency has developed and published materials to assist data controllers to comply with their security duty, including the following: (i) Recommendations on personal data security, (ii) Functional equivalency chart of security measures contained in the Mexican DP Law, its Regulations and the Recommendations on personal data security; (iii) Manual

on personal data security for micro, small and medium-sized enterprises; and (iv) Manual on security matters in a Microsoft environment for micro, small and medium-size enterprises.

5 How does the law of your jurisdiction define personal data? Can the definition extend to data relating to businesses?

"Personal data" is defined in the Mexican DP Law as "any information related to an identified or identifiable individual". An "identifiable individual" is someone whose identity can be determined, directly or indirectly, through any information. An individual will not be deemed identifiable if disproportionate efforts or time are required to identify such person.

The definition of personal data does not extend to data relating to businesses. Under article 5 of the Regulations of the Mexican DP Law, the following information is expressly excluded from the definition of personal data and, in principle, from the protection of the Mexican privacy legislation: (i) information of entities, (ii) information of employees or contractors that is only used for representing his or her employer or client – for example, information contained in a business card, and (iii) information of individuals in their capacity as business people or professionals. However, it should be noted that in a non-binding precedent issued by the Mexican Supreme Court of Justice in February 2014, the Constitutional Court ruled that, although in the first instance the constitutional right to privacy and personal data protection could seem to be granted only to individuals (ie, people), legal entities should also be entitled to the protection and confidentiality of their data and information that could equate to that identified as personal data of individuals. In the opinion of the Court, this information includes any documentation or data that, if revealed to third parties or to the public, could harm the free and proper development of the company. As mentioned above, this is a non-binding precedent that would require further development in other decisions to allow effective protection of legal entities' data as personal data.

6 Does your country's data protection legal framework distinguish between sensitive and non-sensitive data?

Yes. The term "personal data" is defined as "any information related to an identified or identifiable individual". Personal data is considered "sensitive data" when it is related to the most intimate sphere of the data subject and, if misused, could result in discrimination or in a serious risk for its holder. In accordance with the Mexican DP Law, sensitive personal data includes racial or ethnic origin, political opinions, religious, philosophical and moral belief, trade union membership, physical or mental health, genetic information and sexual preference.

7 Identify the basic principles in force in your country for the processing of personal data. Is there a general limitation for the processing of personal data?

In the processing of personal data in Mexico, data controllers must observe the data protection principles of: legality, consent, information (notice), quality, purpose, loyalty, proportionality and accountability. Data controllers are also bound by a duty of care and a duty of confidentiality. Below is a brief description of each of the personal data protection principles.

Legality: the processing of personal data must be carried out in compliance with Mexican and international legislation.

Consent: to legally process personal data, the consent of the data-subjects must be obtained, except in the cases expressly set forth in article 10 of the Mexican DP Law; namely: (i) when authorised in an applicable statute, (ii) when the personal data is available to the public, (iii) if the data cannot be associated to an individual as a result of a prior anonymisation process, (iv) if the processing is required to comply with the legal relationship between the data controller and the data subject, (v) in case of an emergency situation, or (vi) a competent authority authorises the processing of the personal data. When consent is required, implied consent is sufficient, except in case of financial or asset data, which requires the express consent of the data subject and in the case of sensitive data where the data controller must obtain the data subject's express written consent to the processing (which could include electronic signature or other electronic means implemented by the data controller).

Information (notice): to legally process personal data in Mexico, controllers must inform data subjects what personal data is being collected and the purpose of processing such information. This principle is accomplished through the delivery of a privacy notice to all data subjects. For privacy notices to be legally compliant they must be in Spanish and must fulfil the requirements set forth in the Mexican DP Law, its Regulations and the Guidelines for the Privacy Notice – the main purpose of the Guidelines is to provide guidance on the content and scope of the privacy notice, in line with the Mexican DP Law and its Regulation. Typically, standard worldwide privacy policies do not comply with all Mexican law requirements.

Quality: personal data must be accurate and up to date, and shall only be retained for as long as required to fulfill the purpose or purposes informed in the privacy notice. To the extent that the personal data is provided by the data subjects it is understood that the data controller complies with the obligation of keeping accurate personal data.

Purpose: personal data shall only be processed for the purpose or purposes identified in the privacy notice, which must also differentiate between main purposes (those that trigger and are necessary to fulfil the legal relationship between the data subject and data controller) and secondary uses of the information (not strictly required to fulfil the legal relationship between the parties, including marketing and advertising activities). If the data controller is going to process the personal data for purposes not included in the privacy notice, it must obtain the consent of the data subject for such additional purposes.
Loyalty: under the loyalty principle the personal data shall be processed favoring the data subjects' interests and reasonable expectation to privacy. In the processing of personal data, it should be assumed that the data subjects have placed their trust in another person or entity, for their personal data to be processed in accordance with what has been agreed among them.
Proportionality or minimisation: the personal data that is processed by a data controller must be limited to the one that is necessary, adequate and relevant for the purposes set forth in the privacy notice.
Accountability: data controllers must assure and are responsible for the legal processing of personal data held by them, or shared with a data processor, irrespective if the data processor is based in Mexico or abroad.

Without underrating any of the above-mentioned principles, the main general limitation for the processing of personal data is the delivery of the privacy notice to the data subjects and obtaining, when required, the consent for the processing of the personal data. Where the express or the written express consent of the data subjects is required, it is usually obtained through the privacy notice; however, data controllers could obtain the consent through other means.

8 Do special data protection rules apply to certain industries, such as financial services, healthcare and telecommunications? Is the processing of personal data on the internet specifically provided for?

As described herein, the Mexican DP Law applies to all private parties that process personal data, irrespective of the industry or sector they belong to or the means through which it is processed (internet, telephone, physically, etc) and, thus, all data controllers must comply with the personal data protection principles and duties set forth in the law. In addition, there are some special data protection rules that only apply to certain industries or areas of the law. For example, in the processing of personal data contained in medical records, the Mexican Official Standard NOM-004-SSA3-2012 must be observed. The Federal Consumers' Protection Law regulates the use of consumers' personal data for marketing and advertising purposes and the processing of personal data in apps and technological platforms connecting supply and demand will be further regulated through a Mexican standard that is currently under discussion and identified as PROY-NMX-COE-001-SCFI-2018. Financial services regulations, for example, require that financial institutions, as well as the corporations that render services to credit institutions, fulfil different requirements and comply with specific data protection and cybersecurity obligations set forth in different statutes and in the General Provisions Applicable to Credit Institutions (known as the Circular Única de Bancos).

9 Are there specific rules for the processing of personal data of minors?

Personal data pertaining to minors can only be obtained and processed with parental/tutorial authorisation. In cases where minors' personal data is gathered, data controllers should ideally indicate in the privacy notice the mechanisms they have implemented to ensure that the required parental/tutorial authorisation is obtained.

Furthermore, minors' privacy is specifically protected under the General Law on the Rights of Girls, Boys and Adolescents, which sets forth that the personal data of all minors should be properly protected, and that reiterates that girls, boys and adolescents have a right to intimacy that should be protected and respected by all parties.

10 What are the sanctions and remedies for non-compliance with data protection and cybersecurity laws? Is there criminal liability for non-compliance with the data protection and cybersecurity laws?

The Mexican DP Law identifies a list of conducts that are considered administrative offences that could be penalised by the Mexican DP Agency with: (i) an order for the data controller to comply with the request from a data subject to access, rectify, cancel or oppose to the use of their personal data, or (ii) a fine, that could go from 100 to 320,000 times the UMA, which is a measuring unit published by the National Institute of Statistics and Geography used to determine fines, fees and other payments established in federal and local laws (between 8,449 and 27,036,800 pesos in 2019). In case of recurrence or if the violation involves sensitive data, the amount of the penalty could be doubled. By way of example, the following conducts are considered as administrative offences in article 63 of the Mexican DP Law: (i) processing of personal data without a privacy notice issued in compliance with the Mexican DP Law, (ii) processing of personal data in breach of one or more of the data protection principles set forth in the Mexican DP Law, (iii) breach of the controller's confidentiality duty, (iv) unauthorised and/

or unconsented transfers of personal data, and (v) the transfer of personal data to third parties without disclosing to such parties the corresponding privacy notice under which the data-subjects' restricted the use of their personal data.

To impose a fine, the DP Agency must follow a process. The process leading to the imposition of fines starts with an administrative procedure where the DP Agency has access to all information and documentation related to an alleged violation and would most likely visit the data controller's facilities. Once that administrative procedures have been completed, it is followed by a fines imposition procedure, where the DP Agency resolves that a data controller carried out one of the penalised conducts set forth in the applicable law.

Under the Mexican DP Law, the following behaviors are considered criminal offences that can be sanctioned with imprisonment: (i) the intentional breach, for purposes of obtaining a gain, of a database under the offender's control, and (ii) the processing of personal data with the purposes of obtaining an illicit gain, through deception means or taking advantage of the error of the data subjects or of the person authorised to transfer the data.

11 Does your jurisdiction have an independent authority (or authorities) with responsibility for regulating data protection and cybersecurity? What are the enforcement powers of the authorities?

Yes, INAI is a constitutional autonomous governmental entity responsible for regulating data protection and cybersecurity in Mexico. The INAI is empowered by the Mexican DP Law to hear and resolve the administrative procedures set forth in the Mexican DP Law and to impose sanctions on data controllers where applicable.

INAI

Insurgentes Sur No. 3211 Col. Insurgentes Cuicuilco, Alcaldía Coyoacán, CP 04530 http://inicio.ifai.org.mx/SitePages/ifai.aspx Tel. 01800 8354324

12 Is notification or registration required before collecting, processing and transferring personal data?

Yes, prior to collecting, processing and transferring personal data, data controllers must provide to the data subjects a privacy notice (known in many jurisdictions as privacy policies or statements) informing them, among other things, about the personal data that is collected and the purposes of the processing of the personal data. Data controllers are not required to register themselves or their databases with the Mexican DP Agency.

13 What are the main obligations applicable to data controllers to process personal data?

Data controllers must comply with the privacy principles of legality, consent, information (notice), quality, purpose, loyalty, proportionality and accountability and with the duties of care and confidentiality set forth in the Mexican DP Law and must adopt all actions required for such purposes. Data controllers are bound by these principles and duties even when the data is processed by data processors on behalf of the controller. Data controllers are also required to handle and respond to the requests from data subjects to exercise (i) their data protection rights of access, rectification, cancelation and opposition, (ii) the right to revoke their consent to the processing of their personal data and (iii) the right to limit the use and disclosure of personal data.

14 Is there a specific regime applicable to the processing of personal data on behalf of third parties?

Yes, the processing of personal data on behalf of third parties is carried out by data processors. Data processors process personal data only on behalf, and per the instructions, of a data controller as set forth in a data processing agreement. The data processing agreement must be formalised to properly document its existence and define its scope. Data controllers must provide to data processors the privacy notice that regulates the processing of the personal data, as such document defines the scope of the processing of the data as authorised by the data subjects. The sharing of personal data by a data controller with a data processor is defined in the Mexican DP Law as a "transmission" of personal data, which does not need to be informed to the data subjects and does not require their authorisation.

Data processors must comply with the following obligations set forth in articles 49 and 50 of the Regulations of the Mexica DP Law: (i) process the data only on behalf and for the benefit of the data controller and in accordance with the instructions received from it, which may be specific instructions or instructions of a general nature, (ii) abstain from processing the data for purposes beyond those instructed by the data controller, (iii) implement security measures in line with the Mexican Data

Protection Law, its Regulations, and other applicable provisions in order to prevent damage, loss, alteration and deletion and unauthorised or unlawful use, access or processing of the information, (iv) maintain in strict confidentiality all personal data, except as otherwise allowed in an agreement with the data controller or as authorised by the data controller, (v) abstain from transferring and/or disclosing the data without the data controller's authorisation, and (vi) delete the personal data per the instructions of the data controller or once the legal relationship with the data controller terminates, to the extent that the data processor is not required under an applicable statute to maintain the data.

A data processor could be characterised as a data controller and be subject to all responsibilities imposed on controllers, if: (i) it uses the personal data beyond the instructions received from the data controller, or (ii) it transfers the data without the prior consent of the data controller.

15 Is the informed consent of the data subjects required before processing personal data? Are there lawful ways to process personal data without consent?

Yes, the processing of personal data is subject to the consent of data-subjects. The processing of financial or asset data is subject to the express consent of the data-subjects and the processing of sensitive data requires the express and written consent. Personal data can be lawfully processed without consent in the specific cases set forth in article 10 of the Mexican DP Law, and explained in our answer to question 7 where the personal data protection principle of consent is described.

16 What types of rights are granted in the law to data subjects over their information?

All data subjects are entitled to: (i) access the personal data held by the data controller and be informed about the way in which the information is processed, (ii) rectify their personal data in case it is not up to date, it is inaccurate or incomplete, (iii) cancel their data, and (iv) object to the processing of the personal data for specific purposes. These rights are known as ARCO Rights. The Mexican DP Law also requires that data controllers put in place mechanisms to enable data subjects to object to the use of their personal data for purposes not strictly related with the legal relationship between the data controller and the data subject (eg, advertising and publicity), to revoke their consent to the processing of their personal data and to limit the use and disclosure of personal data. Data subjects are also entitled to authorise or reject the transfer of their personal data to third parties, except for the cases established in article 37 of the Mexican DP Law.

17 What is the general regime for the transfer of personal data abroad? Is there a general restriction on the transfer of personal data out of your country? Is the notification of, and approval of the transfer by, the competent authority necessary?

The communication of personal data with any third party in Mexico or abroad, that is not a data processor, is considered a transfer of personal data. The sharing of personal data with data processors is considered a "transmission" of personal data. Each of these types of sharing of personal data (transfers and transmissions) is subject to different rules.

All domestic and international transfers of personal data must be informed to the data subjects and are, generally, subject to their consent, which must be obtained through the privacy notice. All transfers of data must be limited to the purposes justifying the transfer. The transfer of personal data to third parties may only be carried out without the prior consent of the data subjects in the specific cases set forth in article 37 of the Mexican DP Law, including: (i) if the transfer is required to fulfil the legal relationship between the data controller and the data subject, (ii) if the personal data is transferred to the controllers' holding company, subsidiaries or affiliates or to any other entity that forms part of the same corporate group that operate under the same internal data protection procedures and policies, (iii) if the transfer is required under a statute or treaty to which Mexico is a party, (iv) if the transfer is necessary or legally required to safeguard a public interest or for the administration or procurement of justice, and (v) if the transfer is required within a judicial process. The sharing of personal data between a data controller and a data processor, whether domestic or international, does not require the consent of the data subjects.

All international transfers of data must be documented in contractual clauses or other type of legal instrument where the recipient of the personal data agrees to assume at least the same obligations of the data controller, as well as the conditions for the processing of the data that were authorised by the data subject in the corresponding privacy notice, which must be provided by the transferor to the recipient of the personal data.

Data controllers are not required to notify or obtain the authorisation of the Mexican DP Agency to transfer personal data to third parties located in Mexico or abroad; however, data controllers may request the DP Agency's opinion about their compliance with the requirements set forth in the Mexican DP Law before carrying out the corresponding transfer of data.

Under the Additional Protocol to Convention 108, in case of international transfers of data from Mexico to jurisdictions that are not a party to the Convention, the transferor must ensure that the recipient (state or organisation) has an adequate level of protection for the intended data transfer or put in place safeguards, such as contractual clauses, that comply with Mexican

law requirements and thus, would be found acceptable by the DP Agency. The Protocol also allows corporations or individuals located in Mexico to transfer personal data if Mexican law authorises such transfer because of specific interests of the data subject or legitimate prevailing interests, especially important public interests.

18 What data security requirements are imposed in relation to the processing of personal data?

See question 4.

19 Is there any legal requirement in your jurisdiction for a data processor to have a data protection officer (DPO)? What are the main roles or responsibilities of the DPO? Can the DPO incur criminal liability for acts and omissions?

Yes, in accordance with article 30 of the Mexican DP Law, all data controllers must have a data protection officer or a data protection department. The DPO is responsible for handling requests from data subjects exercising their personal data protection rights established in the Mexican DP Law and to promote the protection of personal data within their organisation. The DPO would only incur in criminal liability if his or her acts or omissions are categorised as a felony in terms of the Mexican DP Law or criminal codes (as any other individual would), but not because of his or her role as DPO in case of punishable acts and omissions of the data controller he or she represents.

20 Does your jurisdiction require notification to affected individuals or the authority in the event of data security breach?

Security breaches occurring at any phase of the processing must be immediately notified to the affected data subject if the breach materially affects the property or moral rights of the individuals. The notification must contain, at least, the following information: (i) the nature of the breach, (ii) the personal data that was compromised, (iii) recommendations to the data subjects on the measures that can be adopted to protect their interests, (iv) corrective actions implemented immediately by the data controller, and (v) the means through which the data subject can obtain more information about the breach. Data controllers in the private sector are not required to notify the DP Agency in the event of a data security breach.

In 2018, the DP Agency issued a set of recommendations to handle personal data security breaches. The main purpose of such recommendations is to describe the suggested internal processes and controls that could be used by data controllers to design and implement an incident response plan that would guide them in case of a security breach and could mitigate the impact of the corresponding breach.

21 Is there any national law, regulation or guidance on the use of cookies in general or the use of tracking technologies?

The use of cookies, web bacons and other tracking technologies is broadly regulated in the Regulations of the Mexican DP Law. Under the Regulations, data subjects must be notified through a visible notice or warning about the use of such technologies to obtain and process personal data and about the way they can be disabled – unless its use is required for technological purposes. Information on the use of tracking technologies should also be included in the privacy notice, where it should be specified the type of personal data that is obtained through the cookies and web beacons and the purposes of processing such information.

In accordance with the Regulations of the Mexican DP Law, data controllers must also inform data subjects whenever decisions are made based on the automated processing of personal data without human intervention. This information allows individuals to exercise their right to access their personal data and to be informed about the data that was used as part of the decision-making process. If data subjects deem that the personal data that was used to make the decision is inaccurate or incomplete, they could exercise their rectification right and request that the data controller reconsiders its decision.

22 Is there any national law, regulation or guidance regarding financial technology companies, data protection and cybersecurity?

Yes, the Law to Regulate Financial Technology Institutions (the FinTech Law) was enacted on 9 March 2018, as a comprehensive FinTech legislation that serves as the general legal framework regulating the operation and services of distinct types of financial technology companies. The Fintech Law, and the regulations derived therefrom, deal with matters related to the safeguarding of information, requirements for audits from independent third parties to evaluate security and operational continuity, third-party services, use of electronic media, authentication mechanisms for data access, among others. Furthermore, under the FinTech

Law, all clients' information, including personal data, must be treated as confidential and may not be disclosed to third parties. Also, to obtain an authorisation to operate as a technology company from competent authorities, an entity must have in place measures and policies regulating the use of electronic means and automated data processing systems and assure a certain standard of security and confidentiality. They must comply both with the FinTech Law provisions that apply to technology companies, and those imposed on all data controllers by the Mexican DP Law.

23 What requirements are imposed in your jurisdiction regarding "privacy by design", "privacy by default" and privacy impact assessment?

The Mexican data protection framework includes the concept of "privacy by design" as it requires that data controllers implement a process to handle and mitigate the risks on the protection of personal data that could result from the implementation of new products, services, technologies or business models. Furthermore, for data controllers to fulfil with their accountability principle and duty of care, they should, before beginning a project, carry out a privacy impact assessment to identify and assess how personal data will be processed within their organisation, including its collection, protection, use, deletion, etc, and identify and address potential risks. Article 61 of the Regulations of the Mexican DP Law contains a catalogue of suggested actions, including the following: (i) preparation of an inventory of personal data and of data processing systems, (ii) conducting a risk and gap analysis to identify and mitigate potential vulnerabilities, (iii) launch a work plan to implement missing safeguards that could have been identified during the gap analysis, (iv) preparing a registry of storage means, (v) conducting internal and external reviews and audits, (vi) determine the roles and responsibilities of the personnel involved in the processing of personal data, etc. In addition, data controllers must comply with all obligations set forth in the Mexican DP Law throughout the life cycle of the personal data. In other words, data protection should be integrated into the business practices and models of all organisations (including internal projects, product development, IT and software development, new products and services), from their design phase and through their complete implementation.

24 What requirements are imposed in your jurisdiction on the sending of unsolicited electronic commercial communications?

Data subjects must be informed, through the privacy notice, whether their personal data will be used to send electronic commercial communications for marketing, advertising or commercial prospecting purposes and must be provided with the option to refuse receiving such type of communications. Data-controllers must also indicate in the privacy notice the mechanisms that they have implemented for the data subject to limit the use and disclosure of their personal data. These mechanisms could include: (i) creating their own exclusion lists, or (ii) refer data subjects to the Public Registry of Consumers (REPEP) managed by the Federal Consumers' Protecting Agency or the Public Registry of Users of Financial Services (REUS) managed by the National Commission for the Protection and Defence of the Users of Financial Services. Corporations and financial institutions must avoid sending electronic commercial communications to all individuals registered in such list or registries and, thus, should first review them.

25 Do any specific requirements apply in your country to cloud computing?

Yes. The Regulations of the Mexican DP Law specifically regulate cloud computing services, and define "cloud computing" as follows: "a model for the external rendering of on-demand computing services, that involve the provision of an infrastructure, a platform and software, distributed in a flexible manner through virtualisation processes in dynamically shared resources".

In accordance with article 52 of the Regulations of the Mexican DP Law, data controllers should only engage providers of cloud computing services that can ensure due protection of the personal data. Cloud computing services providers must fulfil the following requirements to legally process personal data under Mexican law: (i) design and implement internal policies that are in line with the personal data protection principles and duties set forth in the Mexican DP Law and its Regulations, (ii) be transparent about their outsourced services that involve the processing of personal data, (iii) abstain from including terms in the engagement that would entitle them to assume ownership over the personal data, and (iv) maintain in strict confidentiality all the personal data that is subject to the rendering of the services. Furthermore, the providers of cloud services must have in place mechanisms to: (i) publicise their internal privacy policies and terms of services, (ii) implement and maintain appropriate security safeguards to protect personal data, (iii) ensure the deletion of personal data upon termination of the services and once the data has been retrieved by the data controller, (iv) prevent access to personal data by individuals without the required access privileges, and (v) promptly inform the data controller about any request for personal data from a competent authority.

Recently, in a joint effort to guide data controllers, the DP Agency and the Ministry of Economy issued a manual with the minimum suggested criteria for the acquisition of cloud computing services that involve the processing of personal data. The

purpose of this guide is to provide guidance on the engagement of cloud computing services providers by those individuals and entities that maintain personal data and require such services to fulfil the purposes of the processing of such personal data.

26 Does your country provide for protection of personal data under the control of government agencies?

Yes, the processing of personal data controlled by government entities is specifically regulated in the General Law for the Protection of Personal Data Held by Government Entities, enacted on 26 January 2017. This law provides a legal framework for the protection of personal data held by any authority at a federal, local or municipal level, that forms part of the executive, legislative and judicial branches of government; as well as autonomous agencies, political parties and public trusts and funds. The provisions of this law apply directly to all federal government entities. State laws that regulate the processing of personal data by government entities at a local level must adjust their provisions in line with the general law, as otherwise the mentioned general law is directly applicable.

27 Does your country allow the right to access data under the control of government agencies?

The Mexican Constitution and the General Law for the Protection of Personal Data Held by Government Entities grant data subjects the right to access their personal data under the control of government agencies. Under article 44 of the General Law for the Protection of Personal Data Held by Government Entities, any individual can access his or her personal data held by a government entity, and be informed about the terms and conditions of its processing. Data subjects can also exercise their rights to rectify, cancel (including deletion) and oppose to the use of their personal data by the government.

28 Does your country provide for self-regulation?

Yes, self-regulation is encouraged in the Mexican DP Law and its Regulations and could even be considered exculpatory circumstances by the DP Agency when imposing a sanction on a data controller. Self-regulating schemes include: (i) the implementation of personal data protection compliance programmes, including a privacy impact assessment, the design of internal manuals and policies, training of personnel, follow-up audits, (ii) certification mechanisms to demonstrate compliance, and (iii) codes of conduct and of professional best practices. Self-regulation schemes could be agreed upon between different corporations or with national or international governmental or non-governmental organisations. Under article 80 of the Regulations of the Mexican DP Law, the primary objectives of self-regulating schemes are the following: (i) assist on compliance with the accountability principle, (ii) establish qualitative processes and practices that complement those set forth in the Mexican DP Law and its Regulations, (iii) promote compliance with the personal data protection principles and to guarantee the privacy and confidentiality of the personal data, and (iv) facilitate the transfer of personal data among data controllers that have implemented data protection programmes.

Carmina Mogollón González

Greenberg Traurig

Carmina Mogollón González focuses her practice on global data protection and privacy matters in a variety of markets. She advises clients on complex issues related to evaluating and strategically managing personal data protection. She has been involved in the representation of several companies in administrative processes before the Mexican Data Protection Agency. She is also experienced on a variety of commercial matters involving the development and implementation of information privacy in mergers and acquisitions, compliance and transactional issues in the technology, e-commerce, manufacturing and other industries.

Carmina represents multinational and local companies doing business in Mexico as well as global chapter-based non-governmental organisations, based in Mexico or abroad, in governance and compliance matters, and in administrative and regulation issues and general corporate law.

Greenberg Traurig, LLP is an international, multi-practice law firm with more than 2000 attorneys serving clients from 39 offices in the United States, Latin America, Europe, Asia, and the Middle East. GT has been recognised for its philanthropic giving, diversity, and innovation, and is consistently among the largest firms in the US on the Law360 400 and among the Top 20 on the Am Law Global 100.

Greenberg Traurig's Mexico City office includes attorneys with proven experience who have been key contributors to major national projects in Mexico, as well as attorneys who have held positions in Mexican government offices and regulatory agencies. Our team has played a role in shaping current Mexican jurisprudence in key judicial procedures that have set legal precedents in important sectors of the Mexican economy.

Our lawyers offer clients strategic legal advice with a collaborative approach based on our understanding of how legal services can support business objectives, from handling major transactional matters to advising clients on dispute prevention and resolution. With our emphasis on cross-border work, the lawyers in the Mexico City office play an integral role in GT's Latin America Practice, as well as the firm's broader global practice. Our service offering includes real estate, corporate and securities, mergers and acquisitions, antitrust, banking and finance, employment law, data privacy, anticorruption and compliance, energy and infrastructure, telecommunications, environmental and administrative litigation.

Greenberg Traurig, S.C.
Paseo de la Reforma No. 265 PH1
Colonia Cuauhtémoc, CDMX, C.P. 06500,
México
Tel: +52 55.5029.0000
Fax: +52 55.5029.0002

www.gtlaw.com

Carmina Mogollón González
mogollonc@gtlaw.com