Data Protection & Privacy 2022

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY®
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Tenth edition
ISBN 978-1-83862-644-0

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2022

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the tenth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Jordan, Pakistan and Thailand.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

Mexico

Abraham Díaz and Gustavo A Alcocer
OLIVARES

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legal framework for PII protection is found in:

- article 6 of the Mexican Constitution:
- the Federal Law for the Protection of Personal Information Held by Private Entities, published in July 2010; its Regulations published in December 2011;
- the Privacy Notice Rules, published in January 2013;
- the Binding Self-Regulation Parameters, published in January 2013 and May 2014; and
- the General Law for the Protection of Personal Data Held by Public Governmental Entities, published in January 2017.

Mexican PII protection law is not based exclusively on an international instrument on data protection, but instead follows international correlative laws, directives and statutes, and thus has similar principles, regulation scope and provisions.

The Federal Law for the Protection of Personal Data (the Law) regulates the collection, storage, use and transfer of PII and protects individual data subjects' (individuals) rights. It is a federal law of public order that makes its provisions applicable and enforceable at the federal level across the country and is not waivable under any agreement or covenant between parties since it is considered to be a human right. This Law regulates the use and processing given to the PII by PII data controllers (PII controllers) and PII processors, thus providing several rights to individuals and obligations to PII controllers and PII processors, to ensure privacy, security and confidentiality of such information. The Privacy Notice Rules comprise the requirements for such notices, whereas the Binding Self-Regulation Parameters contain the requirements and eligibility parameters to be considered by the authority for approval, supervision and control of self-regulation schemes and authorisation and revocation of certifying entities as approved certifiers.

Since June 2018, Mexico is a member of the Convention for the Protection of Individuals Concerning the Automated Processing of Personal Data, and its Protocol (Convention 108).

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

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

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Since the Federal Law for the Protection of Personal Information Held by Private Entities proposed a centralised model of protection of PII instead of a sectorial model, the INAI is the only data protection authority in charge of the protection of personal information.

Further, section VII of article 38 of the Federal Law for the Protection of Personal Information Held by Private Entities sets forth as a general obligation of the INAI:

> *To cooperate with other supervising authorities and national and international entities, to help in the protection of personal information.*

Likewise, article 40 of the Federal Law for the Protection of Personal Information Held by Private Entities makes clear that this law constitutes the legal framework that any other authorities must observe when issuing any regulations that may imply the processing of PII, and said regulations must be issued in coordination with the INAI. This obligation is also included in articles 77 and 78 of the Regulations of the Federal Law for the Protection of Personal Information Held by Private Entities.

Breaches of data protection

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Administrative sanctions are provided for violations to the law from 100 to 320,000 times the minimum general daily wage applicable in Mexico City for PII controllers and PII processors. Depending on the seriousness of the breach and specific behaviour and conduct (profit-making with PII or the methods used to get consent for the use of PII), it may lead to criminal penalties, which are sanctioned with between three months and five years of imprisonment. This also depends on the nature of the PII (penalties are doubled if the personal data is considered by law as sensitive personal data).

Also, related conduct may be sanctioned under the Criminal Code, such as professional secrecy breaches and illegal access to media systems and equipment.

SCOPE

Exempt sectors and institutions

5 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Federal Law for the Protection of Personal Data (the Law) applies to non-public individuals and entities that handle personally identifiable information (PII). Also, the following non-public persons and entities are excluded from the application of the Law:

- credit information agencies or companies, where such companies are specially regulated by the Law for the Regulation of Credit Information Companies; and
- persons who handle and store PII exclusively for personal use and without any commercial or disclosure purposes.

Also, from January 2017, the Law for the Protection of Personal Data Held by Public Governmental Entities applies to any authority, entity, body or organism of the executive, legislative and judicial powers of the government, autonomous entities, political parties, trusts and public funds, at federal, state and municipal levels.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Federal Law for the Protection of Personal Data covers PII regardless of the means or media where such data is stored, processed or organised (whether physical or electronic); however, there is no regulation regarding the unauthorised interception of communications (as it would relate to surveillance or espionage), electronic marketing or surveillance of individuals. In this regard, such matters as illegal access to media, systems and equipment could be covered by criminal law, including:

- article 166-bis of the Federal Criminal Code sanctions with imprisonment from three months to up to three years for the person who in virtue of his or her position in a telecommunications company, unlawfully provides information regarding people using the said telecommunication services;
- article 177 of the Federal Criminal Code sanctions with imprisonment from six to 12 years, and a fine up to 600 the minimum general daily wage (MGDW), for the person who intervenes in any private communication without a judicial order issued by a competent authority;
- article 211-bis of the Federal Criminal Code sanctions with imprisonment from six to 12 years, and a fine up to 600 MGDW, for the person who reveals, divulges or improperly uses any information or images obtained from the intervention of private communication;
- article 36 of the Federal Law for Consumers' Protection sanctions the publication in any mass media of any notice addressed undoubtedly to one or various specific consumers, to collect a debt from them or have them comply with an agreement; and
- article 76-bis of the Federal Law for Consumers' Protection recognises as a consumer's right in transactions effected through electronic, optic or other technologic means, that the supplier of a commodity or service uses the information confidentially provided by the consumer, and consequently said information cannot be transmitted to other different suppliers unless consented by the consumer or ordered by competent authorities.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

Along with other laws already pointed out herein, such as the Criminal Code, the Law for the Regulation of Credit Information Companies and the Law for the Protection of Personal Data Held by Public Governmental Entities, there is additional legislation covering specific data protection rules, such as the Civil Code and the Code of Commerce. However, to date, Mexico does not count on specific and express rules for data protection in connection with employee monitoring, e-health records or the use of social media.

In the case of e-health records, there are some specific regulations for the creation and handling thereof. However, concerning the protection of PII, there is a referral to the rules outlined in the Federal Law for the Protection of Personal Information Held by Private Parties, its Regulations, and the General Law for the Protection of Personal Data Held by Public Governmental Entities (the latter in the case of e-health records for the public sector).

Additionally, in January 2021, an amendment to the Federal Labor Law was published and set into force, establishing a general law framework for the regulation of telework. Although this law framework refers to the rules set forth in the Federal Law for the Protection of Personal Information Held by Private Entities, it introduces some rules that must be observed by employers and employees, when operating in telework mode.

PII formats

8 | What forms of PII are covered by the law?

The Federal Law for the Protection of Personal Data covers PII regardless of the means or media used for its storage, process or organisation. Such means or formats include:

- digital formats (eg, hardware, software, web, media, applications, services or any other information-related technology that allows data exchange or processing; among these formats, the Law specifically includes PII stored in the cloud);
- electronic support (ie, storage that can be accessed only by the use of electronic equipment that processes its contents to examine, modify or store the PII, including microfilm); and
- physical support (ie, storage media that does not require any device to process its content to examine, modify or store the PII or any plain sight intelligible storage medium).

Extraterritoriality

9 Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Mexican PII protection laws are not limited to PII controllers established or operating in Mexican territory. Although the Federal Law for the Protection of Personal Data does not provide a specific reach or scope of its applicability, the Regulations to the Law do. In this regard, such regulations (and, therefore, the Law), in addition to applying to companies established or operating under Mexican law (whether or not located in Mexican territory) apply to companies not established under Mexican law that are subject to Mexican legislation derived from the execution of a contract or under the terms of international law.

Additionally, Mexican regulations on PII protection apply:

- to companies' establishments located in Mexican territory;
- to persons or entities not established in Mexican territory but using means located in such territory, unless such means are used merely for transition purposes that do not imply a processing or handling of PII; and
- when the PII controller is not established in Mexican territory but the person designated as the party in charge of the control and management of its PII (a service provider) is.

In the case of individuals, the establishment will mean the location of the main place of business or location customarily used to perform their activities or their home.

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

All processing or use of PII is covered by the Mexican legal framework.

Mexican PII protection law makes a distinction between PII controllers and those who provide services to controllers, where the latter are independent third parties who may be engaged by the PII controller to be the parties responsible for the PII processing and handling. While it is not mandatory to have this third-party service provider, should a company (PII controller) engage such services, it shall have a written agreement stating clearly all the third party's responsibilities and limitations in connection with the PII.

By virtue of this obligation of PII controllers to execute an agreement with any PII processor they use, the duties acquired by the PII processor must be the same as those imposed by the Federal Law for the Protection of Personal Dataon the PII controller.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The law provides eight main standards for the processing of PII:

- legality: PII controllers must always handle PII according to the law. All personal data shall be lawfully collected and processed, and its collection shall not be made through unlawful or deceitful means;
- consent: PII controllers must obtain consent from individuals for the processing and disclosure of their PII. In this regard, the consent of individuals shall not be required if:
  - PII is contained in publicly available sources;
  - PII cannot be associated with the individual, or if by the way its structure or content cannot be associated with the individual;
  - PII processing is intended to fulfil obligations under a legal relationship between the PII controllers and individuals;
  - an emergency situation exists in which the individual or its properties may be potentially damaged;
  - PII is essential for certain medical or health matters where the individual is unable to provide consent under applicable laws; or
  - a resolution is issued by a competent authority to process and disclose PII, without the required consent; and
- information: PII controllers must notify the individual of the existence and main characteristics of the processing that will be given to the PII;
- quality: PII handled must be exact, complete, pertinent, correct and up to date for the purposes for which it has been collected;
- purpose (the finality principle): PII may only be processed to fulfil the purpose or purposes stated in the privacy notice provided to the individual;
- loyalty: PII controllers must protect individuals' interests when handling their PII;
- proportionality: PII controllers may only handle the PII necessary for the purpose of the processing; and
- responsibility: PII controllers are responsible for the processing of the PII under their possession.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

The law makes a distinction regarding 'sensitive' PII. This information is deemed the most personal of the individual, and if mistreated, could lead to discrimination or general risk to the individual (ie, racial or ethnic origin, present or future health status, genetic information, religion, political opinions, trade union membership or sexual orientation).

Given this, the Federal Law for the Protection of Personal Data provides more stringent rules for the processing of this sensitive PII, such as the obligation for PII controllers to always get written and express consent from individuals for the processing of their sensitive PII. Likewise, PII controllers may not hold sensitive PII without justified cause pursuant to the purpose of the processing.

Several additional limitations apply to the general handling of this type of information (eg, PII controllers must use their best efforts to limit the processing term of sensitive PII, the privacy notice must expressly point out the nature of such information when required; and, when it comes to penalties for the breach or mistreatment of PII, these may double when processing sensitive PII).

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The PII controller must have a privacy notice available for all individuals whose data is in their possession or collected for use and processing. According to the Federal Law for the Protection of Personal Data and its Regulations, there are three types of privacy notices:

- an integral privacy notice;
- a simplified privacy notice; and
- a short privacy notice.

The privacy notice must include, at least, the following information:
- the identity and address of the PII controller;
- PII that would be subject to processing;
- the purpose of the processing;
- the mechanisms provided by the PII controller to the individuals to limit the use or disclosure of the information;
- the means for individuals to exercise their rights to access, rectify, cancel or oppose the processing of their PII;
- any transfer of the PII to be made, if applicable;
- the procedure and vehicles in which the PII controller will notify individuals about modifications to the privacy notice;
- the procedure and means by which the PII controller should notify the individuals of any modification in such privacy notice; and
- regarding sensitive PII, the privacy notice shall expressly state that the information is of a sensitive nature.

In addition and pursuant to the privacy notice rules, the notice must take into account the following characteristics:
- inaccurate, ambiguous or vague phrases must not be used;
- the individual's profile must be taken into account;
- if an individual's consent is granted through tick marks in text boxes, these must not be pre-ticked; and
- reference to texts or documents not available to individuals must be omitted.

Exemption from notification

14 | When is notice not required?

A privacy notice is not necessary when:
- the exemption is available in a specific provision of applicable law;
- the data is available in public sources;
- PII data is subject to a prior dissociation procedure (anonymised data);
- there is an existing legal relationship between the individual and the PII controller;
- there is an emergency situation that could potentially harm an individual or his or her property;
- it is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the individual is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation; or
- a resolution is issued by a competent authority.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The Federal Law for the Protection of Personal Data provides individuals with the right of access, rectification, cancellation and opposition of the holders on their personal data ARCO rights:
- to access (the right to know what information is being held and handled by the PII controller);
- rectify (the right to request at any time that the PII controller correct the PII that is incorrect or inaccurate);
- cancel (the right to request the PII controller to stop treating their PII); or
- oppose (the right to refuse) the processing of their PII.

However, there is room for enhancement as to the regulation of the obligation of PII owners, to offer individuals better degrees of choice or control over the use of their information.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

Personally identifiable information has to fulfil the standard of quality (PII should be exact, complete, pertinent, correct and up to date).

Quality is presumed when PII is provided directly by the individual, and remains such until the individual does not express and prove otherwise, or if the PII controller has objective evidence to prove otherwise.

When personal data has not been obtained directly from the individual, the PII controller must take reasonable means to ensure the quality standard is maintained.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

The Federal Law for the Protection of Personal Data provides a 'need-to-hold' basis; PII controllers must not hold PII any longer than the time required to fulfil its purpose (as stated in the privacy notice). After the purpose or purposes have been achieved, a PII controller must delete the data in its collection after blocking them for subsequent suppression.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The Federal Law for the Protection of Personal Data does provide a 'finality principle', whereby a PII controller is restricted to using the PII only to fulfil the purpose or purposes stated in the privacy notice provided to the individuals, the purpose of which must comply with the legality standard. If the PII controller intends to process data for other purposes that are not compatible with, or similar to, the purposes set out in the privacy notice, an individual's consent must be collected again for such additional purposes.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The PII controller is not allowed to use PII for any purposes other than that authorised or notified to the individual, unless such new purpose is authorised by or notified to (in such cases where express authorisation is not required) the individual, or unless such use is explicitly authorised by law or regulation.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII on their behalf?

PII controllers or entities in charge of processing PII must take and observe various security measures for the protection of the PII, including administrative, physical and technical measures.

Administrative measures must be taken, such as actions and mechanisms for the management, support and review of the security in the information on an organisational level, the identification and classification of the information, as well as the formation and training of the personnel, in matters of PII.

Also, certain physical measures such as actions and mechanisms – technological or otherwise – designed to prevent unauthorised access,

damage or interference to the physical facilities, organisational critical areas equipment and information, or to protect mobile, portable or easy to remove equipment within or outside the facilities.

Technological measures must also be taken, including controls or mechanisms, with measurable results, that ensure that:

- access to the databases or the information is by authorised personnel only;
- the aforementioned access is only in compliance with authorised personnel's required activities according to his or her duties;
- actions are included to acquire, handle, develop and maintain safety on the systems; and
- there is correct administration on the communications and transactions of the technology resources used for the processing of PII.

Other actions that must be taken include:

- making an inventory of the PII and the systems used for its processing;
- determining the duties and obligations of the people involved in the processing;
- conducting a personal data risk analysis (assessing possible hazards and risks to the PII of the company);
- establishing security measures applicable to PII;
- analysing the identification of security measures already applied and those missing;
- making a work plan for the implementation of any security measures missing as a result of the aforementioned analysis;
- carrying out revisions and audits;
- training to the personnel in charge of the processing of PII; and
- maintaining a register of the PII databases.

Notification of data breach

21 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the Federal Law for the Protection of Personal Data, PII controllers must notify individuals if any of their personal data is breached. Such notice must include:

- the nature of the incident;
- the personal data compromised;
- details on the actions that the individual may adopt to protect his or her interests;
- any corrective actions taking place immediately; and
- any means by which the individuals may find more information on the subject.

In the case of a violation of PII, the PII controllers must analyse the causes of its occurrence and implement the corrective, preventive and improving actions, to adapt the corresponding security measures to avoid the repetition of the violation.

However, to date, Mexican law does not include an obligation for private PII controllers to notify the supervisory authority. Although not required by law, the Mexican data protection authority does, however, recommend the issuing of notices in the event of any data breaches.

Government agencies are obliged to notify the National Institute of Transparency, Access to Information and Personal Data Protection of any data breaches.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

It is mandatory for the personally identifiable information (PII) controller (or manager) to appoint an officer (person or department) in charge of the PII, who will be in charge of attending to and taking care of individuals' requests to exercise any of their rights provided by the Federal Law for the Protection of Personal Data. Likewise, this officer must promote the protection of PII within the company.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Although the Federal Law for the Protection of Personal Data does not specify record keeping as a mandatory requirement, it is recommended that PII controllers have a PII database, as well as a register on the means and systems used for the storage of those databases to provide the maximum security for the PII under their possession or control. Likewise, it is suggested to keep records as to the consents obtained from individuals for the collecting and processing of their PII.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The law does not yet include an obligation to adopt new processing operations such as a privacy by design approach. However, PII controllers must carry out privacy impact assessments to determine the security measures to be adopted, as outlined in articles 60 and 61 of the Regulations of the Federal Law for the Protection of Personal Information Held by Private Entities.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There is no need for PII controllers or processors to register with the National Institute of Transparency, Access to Information and Personal Data Protection (INAI); however, the INAI has the authority to request a surprise inspection to monitor that PII controllers are complying with the Federal Law for the Protection of Personal Data and Regulations.

Formalities

26 | What are the formalities for registration?

Registration with the Mexican data protection authorities is neither required by law nor mandatory.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Registration with the Mexican data protection authorities is neither required by law nor mandatory.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

Registration with the Mexican data protection authorities is neither required by law nor mandatory.

Public access

29 | Is the register publicly available? How can it be accessed?

Registration with the Mexican data protection authorities is neither required by law nor mandatory.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

Registration with the Mexican data protection authorities is neither required by law nor mandatory.

Other transparency duties

31 | Are there any other public transparency duties?

No other public transparency duties are imposed on PII controllers.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

To explain the regulations on transfer of PII, it must first be understood that the Federal Law for the Protection of Personal Data defines the transfer of PII as the communication of PII to third parties, whether they are located in Mexico or abroad, other than the PII controller (PII controlling company), in which the third party has to comply with the provisions outlined in the privacy notice of the PII controller.

The transfer of PII to entities that provide PII processing services is not construed as a transfer of PII per se; therefore, any such transfer of PII will be the responsibility of the PII controller and, thus, the PII controller will be liable for any risk or breach in the PII information, which is why it is mandatory to regulate business relationships with PII processors and vendors through the execution of agreements, under which PII processors acquire the same obligations and duties as PII controllers.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

Any transfer of PII (as defined by the Federal Law for the Protection of Personal Data) must be made with the individual's consent unless otherwise provided by the Law (certain exceptions to consent apply). PII disclosure to other recipients must be made under the same conditions as it was received by the PII controller, so, in the case of such disclosure, the PII controller will be able to demonstrate that it was communicated under the conditions as the individual provided such PII. The original PII controller always has the burden of proof in these cases.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The following transfers are allowed without restrictions:

- where the transfer is made pursuant to a law or treaty to which Mexico is a party;
- where the transfer is necessary for medical diagnosis or prevention, healthcare delivery, medical treatment or health services management;
- where the transfer is made to holding companies, subsidiaries or affiliates under common control of the PII controller or to a parent company or any company of the same group as the PII controller operating under the same internal processes and policies;
- where the transfer is necessary pursuant to an agreement executed or to be executed in the interest of the individual between the PII controller and a third party;
- where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
- where the transfer is necessary for the recognition, exercise or defence of rights in a judicial process; and
- where the transfer is necessary to maintain or to comply with a legal relationship between the PII controller and the individual.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

There is no mandatory notification or authorisation required from supervising authority. The Federal Law for the Protection of Personal Data only provides that the PII controller may, if it deems necessary, request an opinion from the National Institute of Transparency, Access to Information and Personal Data Protection regarding the compliance of any international PII transfer with the Law.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Not applicable. Transfers outside the jurisdiction are neither subject to restriction nor authorisation.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Among the main rights of individuals (the right of access, rectification, cancellation and opposition of the holders on their personal data (ARCO) right (the rights to access, rectify, cancel (request the PII to stop treating their PII); or oppose (ie, refuse) the processing of their PII is the right to access a copy of the information being held and treated by the PII controller. This right may be limited for national security reasons, regulations on public order, public security and health or for the protection of third-party rights, and with the limitations provided in the applicable laws, or through a resolution of a competent authority.

Other rights

38 | Do individuals have other substantive rights?

In addition to the right of access, the Federal Law for the Protection of Personal Data provides individuals with their ARCO right (the rights to access, rectify, cancel (request the PII to stop treating their PII); or oppose (ie, refuse) the processing of their PII.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is entitled to declare neither damages nor compensations in favour of any individuals. Therefore, the breach of any PII law does not automatically grant monetary damages or compensation to any PII owner.

It is important to mention that, under Mexican legislation, damages must be claimed and proven through a civil law action. Also, injury to feelings can be claimed as moral damage, but moral damages must also be claimed through a civil action before Mexican civil courts. This means that any PII owner has to prosecute first an administrative action before the INAI to prove the breach of the law, and after obtaining a final decision declaring the administrative infringement to initiate an independent civil law action, before civil courts to collect any damages, or loses, or to claim any compensation derived from any moral damage.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights are exercisable by the INAI. The process is initiated either by the filing of a complaint by an affected individual or directly by the INAI, as a result of any anomalies found during a verification procedure.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Aside from the limitations and exclusions already described herein, the Federal Law for the Protection of Personal Data does not include any additional derogations, exclusions or limitations.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Yes. Since the National Institute of Transparency, Access to Information and Personal Data Protection is an administrative authority, any of its resolutions can be challenged through a nullity trial before the Federal Court for Administrative Affairs, and later on through a constitutional rights action known as Amparo suit.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

The Federal Law for the Protection of Personal Data (the Law) specifically refers to the use of personally identifiable information (PII) in the cloud; the Law provides a list of requirements any third party providing these types of storage service must comply with to ensure the safety of the PII to be uploaded therein.

Further, when PII controllers use remote or local means of electronic communication, optical or other technology mechanisms, that allow them to collect PII automatically and simultaneously at the same time that individuals have contact with PII (cookies or web beacons), the individuals must be informed, through a communication or warning duly placed in a conspicuous location, concerning the use of these technologies and the fact that PII has been collected, as well as the process to disable such access, except when the technology is required for technical purposes.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

The Federal Law for the Protection of Personal Data does not provide any specific rules on marketing by email, fax or telephone; nonetheless, any such contact with individuals is treated as PII and any marketing through those media will, therefore, be regulated according to the Law.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

Mexican law regulates the processing of PII in services, applications, and infrastructure in cloud computing. That is the external provision of computer services on demand that involves the supply of infrastructure, platform, or software distributed flexibly, using virtual procedures, on resources dynamically shared. For these purposes, the data controller may resort to cloud computing by general contractual conditions or clauses.

These services may only be used when the provider complies at least with the following:

- has and uses policies to protect personal data similar to the applicable principles and duties set out in the Federal Law for the Protection of Personal Data and these Regulations;
- makes transparent subcontracting that involves information about the service that is provided;
- abstains from including conditions in providing the service that authorises or permits it to assume the ownership of the information about which the service is provided;
- maintains confidentiality concerning the personal data for which it provides the service; and
- has mechanisms at least for:
  - disclosing changes in its privacy policies or conditions of the service it provides;
  - permitting the data controller to limit the type of processing of personal data for which it provides the service;
  - establishing and maintaining adequate security measures to protect the personal data for which it provides the service;
  - ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it; and
  - impeding access to personal data by those who do not have proper authorisation for access or in the event of a request duly made by a competent authority and informing data controller. In any case, the data controller may not use services that do not ensure the proper protection of PII.

No guidelines have yet been issued to regulate the processing of PII in cloud computing.

UPDATE AND TRENDS

Key developments of the past year

46 Are there any emerging trends or hot topics in international data protection in your jurisdiction?

On 16 April 2021, an amendment to the Federal Telecommunications and Broadcasting Law was published in the Official Gazette, aimed at the creation of a national registry of mobile phone users, through which it is intended to create a database with information on individuals or legal entities who own mobile phones.

The registration of mobile phone numbers, including all of the aforementioned requirements, is mandatory for all users of mobile phones in Mexico, and the telecommunications concessionaires will be responsible for collecting and updating or modifying the users' information, which will be available for Mexican competent authorities.

This reform has caused alarm among specialists in the field, as well as among users in general, due to the lack of security that has been observed in the past in the handling of personal data by the government, as well as the disproportionate demands it places on mobile phone users, forcing them to reveal sensitive data such as biometric data, in contravention to international trends.

The Mexican data protection authority (the National Institute of Transparency, Access to Information and Personal Data Protection) has just filed a legal action denouncing the unconstitutionality and illegality of this amendment.

Additionally, in January 2021, an amendment to the Federal Labor Law was published and set into force, establishing a general law framework for the regulation of telework. Although this law framework refers to the rules set forth in the Federal Law for the Protection of Personal Information Held by Private Entities, it introduces some rules that must be observed by employers and employees, when teleworking.

Coronavirus

47 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

During the period of the covid-19 pandemic, e-commerce in Mexico has boomed, as well as worldwide. One of the few programmes or initiatives put into force by the Mexican government dealing with the risks inherent to e-commerce has been the creation of an ethics code and a digital trust seal, administered by the Federal Bureau of Consumer's Protection, for online e-commerce platforms and providers. One of the requirements for access is the granting of the digital trust seal under the compliance of Mexican data protection laws.

Since coronavirus prompted telework homeworking in many companies, at the beginning of 2021, it became necessary to amend the Federal Labor Law to establish a general law framework for the regulation of telework. Although this law framework refers to the rules set forth in the Federal Law for the Protection of Personal Information Held by Private Entities, it introduces some rules that must be observed by employers and employees, when teleworking.

OLIVARES we know MEXICO

Abraham Díaz Arceo
abraham.diaz@olivares.mx

Gustavo A Alcocer
gustavo.alcocer@olivares.mx

Pedro Luis Ogazón 17
San Angel
01000
Mexico City
Mexico
Tel: +52 55 5322 3000
Fax: +52 55 5322 3001
www.olivares.com.mx

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-644-0