IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 12

MEXICO

Paola Morales and Marcela Flores González[1]

I OVERVIEW

The right to privacy or intimacy is contemplated in Paragraphs 1 and 12 of Article 16 of the Mexican Constitution, and prohibits the intrusion of an individual's person, family, domicile, documents or belongings (including any wiretapping communication devices), except when ordered by a competent authority supported by the applicable law. The right to data protection is stipulated in Paragraph 2 of Article 16 of the Mexican Constitution, and seeks to set a standard for collecting, using, storing, disclosing or transferring (collectively, processing) of personal data (as defined below) to secure the right to privacy and self-determination. The right to privacy and data protection are closely related fundamental rights that seek to protect individuals' ability to guard a portion of their lives from the intrusion of third parties. Notwithstanding this, while a breach of privacy usually results in a breach of the right to personal data protection, a data protection breach does not always result in a breach of privacy.

The first formal effort to address personal data protection was introduced in 2002 when Mexican Congress approved the Federal Law for Transparency and Access to Public Governmental Information (the Former Transparency Law). Although the Former Transparency Law was mainly aimed at securing access to any public information in the possession of the branches of government and any other federal governmental body, it also incorporated certain principles and standards for the protection of personal data being handled by those government agencies. This effort was followed by similar legislation at the state level.

After several attempts to address data protection rights more decisively, in 2009 Congress finally approved a crucial amendment to the Constitution that recognised the protection of personal data as a fundamental right. Consequently, Congress enacted the Federal Law for the Protection of Personal Data in Possession of Private Parties (the Private Data Protection Law), which came into effect on 6 July 2010 and was followed by the Regulations of the Private Data Protection Law on 22 December 2011.

In January 2014, Congress approved an amendment to the Constitution to create an autonomous entity to be in charge of enforcing the Private Data Protection Law and to take on the duties of the former Federal Institute for Access to Information and Protection of Data (the former IFAI), which was originally created as a semi-autonomous agency separate from the federal public administration. However, in a rather controversial move, the former IFAI amended its internal regulations so that it could assume the necessary characteristics and role

1 1 Paola Morales is a partner and Marcela Flores González is an associate at Santamarina y Steta, SC.

of the proposed autonomous entity. Consequently – and as a result of the new General Law for Transparency and Access to Public Governmental Information, which annulled the effect of the former Transparency Law – all matters previously dealt with by the former IFAI are now being handled by the 'new IFAI' as an autonomous entity; and it has adopted the name National Institute of Transparency, Access to Information and Protection of Personal Data (INAI).

The Private Data Protection Law is an omnibus data protection law that sets the principles and minimum standards that shall be followed by all private parties when processing any personal data. However, the Private Data Protection Law also recognises that standards for implementing data protection may vary depending on the industry or sector. Accordingly, the Private Data Protection Law can certainly be complemented by sectoral laws and self-imposed regulatory schemes, which focus on particular industry standards and requirements, to the extent that those standards and requirements comply with the data protection principles in the Private Data Protection Law. There have been efforts to promote such sector-specific rules among those processing any personal data within the same industry. On 13 December 2016, Congress approved the General Law for the Protection of Personal Data in Possession of Governmental Entities (the Governmental Data Protection Law, and collectively with the Private Data Protection Law, the Data Protection Laws), which was enacted on 27 January 2017, to set forth a legal framework for the protection of personal data processed by any authority, entity or organ of the executive, legislative and judicial branches, political parties and trusts operating with public funds at federal, state and municipal levels. Provided that this particular publication is intended to address issues arising from data protection in the private sector, we will not address the governmental Data Protection Law in detail, unless it is necessary to add context.

The INAI is in charge of promoting the rights to protection of personal data and enforcing and supervising compliance with the Data Protection Laws and those secondary provisions deriving from those Data Protection Laws. To this end, with respect to the private sector, the INAI has been authorised to supervise and verify compliance with the Private Data Protection Law; interpret administrative aspects of the Data Protection Laws; and resolve claims and, inter alia, impose fines and penalties. The INAI has been actively working through media campaigns to raise awareness among corporations and individuals of the relevance of adequate protection of personal data. Although the INAI has the authority to initiate enforcement activities, most fines and penalties imposed have resulted from claims filed by data subjects. We are aware that companies that have been fined by the INAI for breaching the Private Data Protection Law have challenged the decisions by means of nullity claims and *amparo* lawsuits; however, the relevant files are not publicly available.

II THE YEAR IN REVIEW

During 2023, the INAI has continued to enforce the Private Data Protection Law and, at the same time, has issued non-binding guidelines and bulletins related to the protection of personal data. Some of the most relevant ones are the summarised here.

In November 2022, the INAI published the guideline 'The Privacy in the Social Media Era' in which the following main conclusions about the privacy in social media are described:

a the constant and rapid evolution of technology and digital services, such as social networks, means that privacy is also constantly changing;

b privacy is not the only right that users of social networks should be aware of. When a person uses social media, his or her rights to the protection of personal data and to the secrecy of communications are also exposed to possible risks and threats;

c the right to the protection of personal data means that the user of a social media or other digital services, such as applications, must have control over the processing and use of his or her personal data;

d the right to privacy allows the user to protect his or her most intimate sphere or private life;

e the right to secrecy of communications protects the content of emails or private messages sent over a private network from unauthorised third parties;

f according to INAI figures, the five most used social networks in Mexico in 2021 were Facebook, WhatsApp, Twitter, YouTube and Instagram;

g the Federal Institute of Telecommunications, in its study Privacy of User Information in the Use of Digital Services, Mexico highlighted that 'social networks are the digital services that collect the most information from users';

h when using social media it is necessary to act with caution and consider that there may be risks such as massive manipulation, disinformation, fake news and illicit actions such as grooming, cyberbullying or sexting; and

i any activity in social media can be known by other people, so it is necessary to take care of what is done to avoid that an action may have negative consequences such as loss of job opportunities or damage to third parties.

In May 2022, the INAI published the Recommendations for the Processing of Personal Data that Derives from the Use of Artificial Intelligence. Artificial Intelligence is relevant to the protection of personal data, since the latter are part of the main input for the operation of some systems, for example: the ability to: (1) collect data; (2) profile; and (3) share information through components such as Global Positioning System (GPS) receivers for geolocation, speakers, cameras for face detection, microphones for audio input, and so on. The INAI published the recommendations with the purpose of disseminating knowledge concerning the relationship of artificial intelligence to the fundamental right of the protection of personal data, and to promote the proper and ethical use of personal information through the different technologies that use artificial intelligence for their operation and compliance with the obligations of the duty of security of personal data, for responsible parties in the private and public sector that develop or use artificial intelligence products or services.

On 8 January 2023, the INAI published a bulletin stating that in 2022 fines imposed for failure to comply with the Private Data Protection Law amounted to almost 60.1 million Mexican pesos. The more frequent infractions were for processing personal data in contravention of the principles established in the Private Data Protection Law, namely the process or transfer of personal data without the proper consent of the data subjects applicable to the personal data being processed, and deficient privacy notices. In previous years, the most sanctioned sectors were the financial and insurance sectors. In 2022, other services and sectors were fined such as information in mass media, the financial and insurance sectors and waste management and remediation services.

On 17 February 2023, the INAI published a bulletin stating that in the next decade, cybercrime and cybersecurity are two of the most serious risks that society will face:

> *Mexico is in first place with 85 billion cyberattack attempts in the first half of last year alone, so this represents a 40 per cent increase in annual figures. Also, Kaspersky released a study revealing that, during the first eight months of the same year 2022, a total of 817 million attempted attacks were recorded in Latin America. . . . the World Economic Forum the World Economic Forum points out in no uncertain terms that cybercrime and cybersecurity cybercrime and cyber insecurity will be one of the most serious risks over the next decade.*

On 1 April 2023, the INAI published a bulletin with recommendations to avoid being a victim of fraud, identity theft or any cybercrime during the holiday season.

On 4 April 2023, the INAI published a bulletin with recommendations to avoid cyberbullying towards minors, considering that in Mexico, there are 88.6 million internet users; of which, 10.5 per cent are children between the ages of six and 11, and 13.6 per cent are between the ages of 12 and 17 according to data from the *18th Study on the Habits of Internet Users in Mexico*, by the internet association *Asociación de Internet MX*.

On 6 April 2023, the INAI published a bulletin with recommendations to protect personal data when using social media.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The most relevant pieces of legislation addressing personal data protection in Mexico are the following:

a the Mexican Constitution;
b the Private Data Protection Law;
c the Governmental Data Protection Law;
d the Regulations to the Private Data Protection Law;
e the Guidelines for Privacy Notices; and
f the Self-Regulation Parameters on Data Protection, which are applicable to the private sector.

The Private Data Protection Law identifies data protection principles governing all processing of personal data, as well as the obligations imposed on any private person, whether an individual or entity, that has control over the processing of personal data (a data controller), data processors (as defined below), third parties and any others engaged in the processing of personal data. As set forth in the Private Data Protection Law, the Mexican executive branch issued the Regulations to the Private Data Protection Law with the intention to clarify the scope of those principles and obligations provided by the Private Data Protection Law. The Regulations also set forth the rules applicable to the exercise by data subjects of their rights in relation to data controllers and those proceedings arising from claims before the INAI filed by data subjects in the event of a breach of the Private Data Protection Law by a data controller.

Finally, the Guidelines for Privacy Notices (the Guidelines), issued by the Ministry of the Economy, set the standard of detail that should be met by data controllers when drafting their own privacy notices, the scope of the language in privacy notices and certain optional but recommended good practices with respect to privacy notices. The Self-Regulation Parameters on Data Protection set forth the rules, criteria and procedures for the development and implementation of self-regulatory schemes on data protection, which were also issued by the Ministry of the Economy.

Also, the Federal Consumer Protection Law and the Federal Consumer Protection Law for the Users of Financial Services contain stipulations protecting consumers, whether individuals or entities, from any processing of their information for marketing purposes. Corporations or financial entities that wish to market products must first review the list of consumers who do not wish to receive marketing information and record it in the Consumer Public Registry held by the Federal Consumers Attorney's Office (Profeco), or the Public Registry of Individual Users, which is managed by the National Commission for the Protection of Financial Services Users (Condusef). Any marketing activity with any consumers enrolled in the registries may result in fines by Profeco or Condusef, as applicable.

Key definitions

In addition to any other terms defined herein, the following terms should be taken into consideration for a better understanding of Mexican law on the subject:

a data processor: any natural person or entity that individually or jointly with others carries out the processing of personal data on behalf of the data controller;

b data subject: the natural person to whom the personal data concerns;

c personal data: any information related to an identified or identifiable individual. The following information would not be subject to the Private Data Protection Law:
- information collected and stored for personal use and not intended for disclosure or distribution;
- information collected by the credit bureau;
- information about entities;
- information about any individual when acting as a merchant or professional practitioner; and
- data about any individual when rendering services to a legal entity or to a merchant or professional practitioner, provided that information is limited to the subject's name, duties or position, business address, business email, business telephone and business facsimile, and the information is processed when representing the merchant or professional practitioner;

d public access source: a database that may be accessed by anyone without complying with any requirement, except for the payment of a fee;

e sensitive personal data: personal data affecting the most intimate sphere of the data subject, or of which misuse may be a cause for discrimination or great risk for the data subject, such as information regarding racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical or mental health and sexual orientation;

f transfer: any kind of communication of personal data made to a person other than the controller, data processor or data subject; and

g remittance: any kind of communication of personal data between the data controller and the data processor, within or outside Mexican territory.

Data protection principles

Considering the fact that the Private Data Protection Law is inspired by the European model provided in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal

data and on free movement of such data, the Private Data Protection Law is based on the principles each data controller must abide by to protect the personal data being processed. These principles are summarised as follows:

a legality: all personal data shall be lawfully collected and processed;

b consent: all processing of personal data shall be subject to the consent (whether express or implied) of the data subject, with certain exemptions set out in the Private Data Protection Law. If it is not exempted, when a data controller is processing any sensitive personal data, the data controller must obtain the express consent of the data subject to process this data, which must be evidenced in writing or through an electronic signature or any other authentication mechanism developed for that purpose. Exemptions to the requirement to obtain consent exist when:

- processing is permitted by law;
- the personal data is publicly available;
- processing prevents association between the personal data and the data subject or his or her identification because of the structure, content or grade of disaggregation of the personal data;
- processing is intended to comply with obligations resulting from a legal relationship between the data controller and the data subject;
- there is an emergency situation that may injure an individual or damage his or her assets;
- processing is essential for the purposes of rendering healthcare services or assistance, the application of preventive medicine, determination of medical diagnosis or the management of healthcare services, as long as the data subject is unable, in terms provided by the General Health Law, to grant his or her consent for the applicable procedure; and
- a competent authority orders the processing;

c quality: the data controller shall cause personal data in a database to be relevant, accurate and up to date for the purpose for which it is meant to be used and shall only retain personal data for as long as is necessary to fulfil the specified purpose or purposes. Regarding sensitive personal data, reasonable efforts shall be made to keep the period of processing to a minimum;

d purpose: processing of personal data shall be limited to the purpose or purposes specified in the privacy notice. No database containing sensitive personal data shall be created without justifying that the purpose for its collection is legitimate, concrete and in compliance with those activities or explicit purposes sought by the data controller. Any processing of personal data for a purpose that is not compatible or analogous to what is set forth in the privacy notice shall require a new consent from the data subject;

e proportionality: processing of personal data must be necessary, adequate and relevant for the purpose or purposes set forth in the privacy notice;

f loyalty: processing of personal data shall favour the interests of the data subject and a reasonable expectation of privacy, which shall be understood as the level of confidence that any person deposits in another where the personal data exchange between them shall be processed as agreed between them in compliance with the Private Data Protection Law. Its collection shall not be made through fraudulent or deceitful means;

g transparency: data controllers shall inform data subjects, by means of a privacy notice, about the personal data that will be subject to processing, and the purpose or purposes for the processing. With respect to sensitive personal data, the privacy notice shall expressly state that the information is of a sensitive nature; and

h responsibility: data controllers shall adopt the necessary measures to comply with all data protection principles during the processing of personal data, even if the processing is carried out by data processors or third parties. Therefore, a data controller shall ensure full compliance with the privacy notice delivered to the data subject by that data controller or by third parties with whom it has a legal relationship.

In addition to the aforementioned principles, all data controllers shall comply with the duties of security and confidence, which are also applicable to data processors and third parties receiving any personal data from a data controller, in which case the latter must verify that these duties are observed by those third parties.

Data controllers shall implement appropriate organisational, technical and physical security measures to protect personal data against unauthorised damage, loss, modification, destruction, access or processing. These measures shall be at least equivalent to those implemented for their own confidential information.

Further, all personal data shall be kept confidential, even upon the termination of any relationship with the data subject and among any data controller and data processor.

Compliance

INAI has *ex officio* authority to supervise compliance with the Private Data Protection Law. Currently, many proceedings to verify compliance have resulted from claims filed by data subjects; however, the INAI determined to initiate *ex officio* proceedings when appropriate.

ii General obligations for data handlers

Although data controllers must comply with each and all the principles described above (see Section III.i), the most basic obligations imposed on data controllers are mainly the drafting of privacy notices and making these available to data subjects, as well as obtaining consent for the processing of their personal data, unless exempted under the Private Data Protection Law.

The drafting and delivery of the privacy notice to a data subject constitutes a key factor in complying with the principle of transparency described above and, therefore, there are no exemptions to the same. As a result, the privacy notice must be drafted complying with strict standards and requirements stipulated in the Private Data Protection Law, its Regulations and, particularly, the Guidelines. There are three types of privacy notices whose general characteristics, terms and conditions are as follows:

a full: a full privacy notice must be used when the personal data is personally collected from a data subject and must include all elements contained in the corresponding provisions of the Private Data Protection Law, the Regulations and the Guidelines;

b simplified: a simplified privacy notice may be used when the personal data is collected directly from the data subject but using remote means and must contain all elements contained in the corresponding provisions of the Private Data Protection Law, the Regulations and the Guidelines; and

c abbreviated: an abbreviated privacy notice may be used when personal data is directly obtained from a data subject by printed means and when the personal data collected is minimal. It must be drafted in accordance with Article 28 of the Regulations and Guideline 38 of the Guidelines.

When drafting the privacy notice, data controllers must identify the different uses intended for the personal data, and also distinguish those uses required for the legal relationship between the data controller and data subject (necessary purposes) from those that are not (secondary purposes). This requirement is important, considering that a data subject may choose to reject (or in the future withdraw consent for) processing those secondary purposes without affecting his or her relationship with the data controller.

When required, consent for processing any personal data must be obtained upon the collection of the personal data if the collection is made personally or directly from the data subject, or before any processing, if personal data was not collected by the data controller directly from the data subject.

The data controller shall describe the means available to the data subject to exercise their right to access, rectify, cancel or oppose the processing of their personal data (ARCO rights), as well as to withdraw consent (withdrawal), either in whole or in part, with respect to the processing of personal data, and to limit the use or disclosure of personal data (data limitation), collectively with the ARCO rights and the right of withdrawal (Data Claims). Data Claims shall be exercised free of charge, unless the data subject exercises the same claim to access personal data within a period of 12 months, in which case the data controller may charge a fee that shall not exceed three times the unit of measure and update (UMA) in force. Unfortunately, awareness in Mexico regarding the protection of personal data is still a major challenge, considering the lack of knowledge (and, in some cases, interest) together with the degree of specialisation of this matter, which may be delaying proper compliance with the Private Data Protection Law. Many data controllers are still gaining interest and experience in these matters, which has caused inadequate implementation of privacy notices, as this requires adequately mapping all data being processed to assess all implications. It is still common to see data controllers drafting their privacy notices without considering whether they are in fact processing any personal data and to what extent.

iii Data subject rights

Data subjects have the following rights, which are intended to secure protection of personal data (the ARCO rights):

a access: a data subject is entitled to access his or her personal data held by a data controller, as well as to know the privacy notice to which processing is subject;

b rectification: a data subject is entitled to rectify his or her personal data when it is inaccurate or incomplete;

c cancellation: a data subject shall always be entitled to cancel his or her personal data. The cancellation of personal data implies that the information shall be kept by the data controller as long as required under the applicable legal relationship or once that time has elapsed, the data controller shall delete the corresponding personal data, unless otherwise required by an applicable law; and

d opposition: a data subject shall always be entitled, with legal cause, to oppose the processing of his or her personal data. If a data subject does so, the data controller shall not be entitled to process the personal data concerning that data subject.

Notwithstanding the above, and in addition to the ARCO rights, the data subject shall also be entitled to withdraw consent, either in whole or in part, with respect to the processing of personal data and may limit the use or disclosure of personal data collectively with the ARCO rights and the right of withdrawal. Additionally, a data subject has the right to opt out or join lists of those unwilling to receive marketing communications or materials kept by the data controller, Profeco or Condusef as stated above.

In addition, data subjects have the right to file claims before the INAI if that data controller fails to address a Data Claim concerning the data subject's ARCO rights or when the resolution of the data controller does not satisfy the data subject. If, because of that claim, the INAI becomes aware of a breach of the Private Data Protection Law, it may impose penalties on a data controller. However, the Private Data Protection Law makes no provision for remedies or financial recovery for the data subject as a result of a breach of its data protection rights. Notwithstanding this, data subjects have the right to file a claim before civil courts to seek indemnification resulting from moral damage.

iv Specific regulatory areas

Despite the fact that the Private Data Protection Law is applicable to all private parties processing personal data, with certain exceptions, and that the Governmental Data Protection Law is enforceable in respect to any processing carried out by public agencies, Mexican Official Standard NOM-004-SSA3-2012 regarding medical records is currently the only extant industry – or sector-specific legal framework – despite the idea fostered by the Private Data Protection Law that laws or regulations applicable to specific sectors or industries should be enacted. Among other relevant provisions made by this standard, it defines the concept of 'clinical records' and imposes obligations of confidentiality in respect of these records; health providers and establishments that gather, manage and store clinical records are required to implement all measures necessary to maintain this confidentiality (e.g., password-protected firewalls).

v Technological innovation

Technological innovations pose a challenge under the Private Data Protection Law as this area is broadly and scarcely regulated with no specific rules applicable to processing affected by such developments. Concepts such as 'big-data analytics' and the 'internet of things' have not yet been defined under the Private Data Protection Law or other applicable data protection legislation. However, processing of personal data using any technological innovation (including the use of remote or local communications media or any other technology) is governed by the Private Data Protection Law, therefore the challenge lies in determining the degree of applicability of that Law, given that the data subject must be informed of the processing. When using remote or local communications media or any other technology, to collect personal data, a notification must be given to the data subject through a visible communication or warning about the use of those technologies to process his or her personal data, and about the manner in which the technological mechanism may be disabled (unless its use is fundamental for technical reasons). This information must be also included in the full privacy notice, clearly identifying the personal data being collected by those means,

as well as the purpose of the collection. In addition, notwithstanding that the concept of biometric data is not defined under the Private Data Protection Law or other applicable data protection legislation, the non-binding guideline issued by INAI defines biometric data and reaffirms that biometric data is deemed 'personal data' and could be deemed also as 'sensitive personal data' in certain scenarios.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Mexico is party to several international organisations (such as APEC – the Asia-Pacific Economic Cooperation – and the Organization of American States) that aim to protect personal data being transferred within their respective regions, whether domestically or internationally. Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data dated 28 January 1981 (Convention 108) and its additional Protocol dated 8 November 2001 (ETS 181) establish that the parties shall adopt provisions and restrictions for the transfer of personal data between the parties subject to such convention and non-party countries.

Under the Private Data Protection Law, an international communication of personal data originating from a data controller, subject to the Private Data Protection Law, may be deemed either a 'transfer' or a 'remittance' depending on the purpose for communicating the data and the recipient of the same. Each of these communications must meet specific requirements, which are described below.

i Transfer of personal data

A transfer is any communication of personal data by a data controller to any private or public entity different from the data subject or the data processor. In this regard, any transfer of personal data must be consented to by the data subject concerned, except where exempted pursuant to Article 37 of the Private Data Protection Law. The transfer must be notified to the data subject by means of a privacy notice and limited to those purposes justifying the transfer.

A data controller would be able to transfer personal data without the consent of a data subject if the transfer is:

a stipulated by a law or treaty to which Mexico is party;

b needed for prevention of illness or medical diagnosis, healthcare assistance, medical treatment or management of health services;

c made to holding companies, subsidiaries or affiliates under common control of the data controller who operate under the same processes and internal policies;

d required by an agreement entered into or to be entered into between the data controller and a third party in the interest of the data subject;

e necessary or legally required to protect the public interest or the prosecution or enforcement of justice;

f required for the acknowledgment, exercise or defence of a right in a judicial proceeding; or

g necessary for the preservation of, or compliance with, a legal relationship between the data controller and the data subject.

Any international data transfer shall be evidenced by an agreement or any other document whereby the third party assumes the same data protection obligations undertaken by the data

controller and the conditions for processing, as consented to by the data subject as detailed in the corresponding privacy notice. International data transfers do not require the approval of the INAI or any other Mexican regulatory agency to be completed, and there is no need to submit standard contractual clauses or comparable instruments to any of them. However, a data controller may seek, at its sole discretion, the opinion of the INAI on whether an international transfer complies with these applicable requirements before completing such transfer.

ii Remittance of personal data

A remittance is any communication of personal data made by a data controller to an individual or legal entity that is unrelated to the data controller, with the purpose of conducting any processing on behalf of the data controller.

A remittance does not require to be notified to a data subject by means of a privacy notice, nor does it require the consent of the data subject. However, to carry out the remittance, a data controller and data processor shall enter into a certain agreement with the purpose of evidencing the existence, scope and content of the relationship, which should be consistent with the privacy notice delivered by the data controller to the relevant data subject. Under the General Data Protection Regulation (GDPR), certain restrictions or requirements may have to be fulfilled prior to completion of an international transfer of personal data to data controllers or data processors located in Mexico. Notwithstanding the approval of the Convention 108 and ETS 181, as of the date of our review, Mexico has not been recognised by the European Commission as a third country providing adequate data protection to facilitate personal data transfers to countries within the EU.

V COMPANY POLICIES AND PRACTICES

Data controllers must, inter alia:

a carry out data mapping to identify the personal data that is subject to processing and the procedures involving this processing;
b establish the posts and roles of those officers involved in the processing of the personal data;
c identify risk and carry out a risk assessment when processing personal data;
d implement security measures;
e carry out a gap analysis to verify those security measures for which implementation is still pending;
f develop a plan to implement those security measures that are still pending;
g implement audits;
h conduct training for those officers involved in the processing;
i have a record of the means used to store personal data; and
j put in place a procedure to anticipate and mitigate any risks arising from the implementation of new products, services, technologies and business plans when processing personal data.

Data controllers have the obligation to include in their privacy notice a mechanism for data subjects to exercise their ARCO rights or withdraw consent, either in whole or in part, with respect to the processing of personal data and to limit the use or disclosure of personal data.

Additionally, data controllers should make available to the data subjects, opt-out mechanisms or lists for those unwilling to receive marketing communications. These lists are kept by the data controller, Profeco or Condusef.

In terms of the Private Data Protection Law, while processing personal data, a data controller must distinguish such processing based on the following:

a purposes that, based on a contractual relationship between the data controller and the data subject, require the processing of personal data, in which case consent for such processing is not required, and the opt-out option would not be available; and

b secondary purposes where compliance with any commitments is not required under any relationship between the data controller and the data subject, in which case the data subject is entitled to opt out and the data controller must provide mechanisms allowing the data subject to opt out prior to such processing.

VI DISCOVERY AND DISCLOSURE

Data controllers are obliged to disclose personal data in the event that there is a binding and non-appealable resolution from a competent Mexican authority. A data subject's consent for the processing of personal data shall not be required to the extent that the processing is meant to comply with a resolution from a competent Mexican authority. The Mexican Constitution grants all individuals the fundamental right to protect their personal data, as well as the right to access, rectify, cancel and oppose any processing of the same. The Mexican Constitution recognises that this right is not without limit; therefore, those principles protecting personal data are subject to certain exceptions for national security, public policy, public security and health, or to protect third-party rights.

Transfers of personal data for legal proceedings or investigations in other countries shall always be carried out in compliance with the Private Data Protection Law and through a letter rogatory following the adequate diplomatic or judicial channels. Data controllers should always analyse whether the privacy notice was disclosed to the data subject, whether the consent is required or exempted and was properly granted, and whether the transfer is limited to those purposes used to justify it. Additionally, the data controller and the relevant authority should enter into an agreement or any other document, as described in Section IV.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Initiation of proceedings

The INAI is in charge of data protection proceedings (DPPs) and of compliance-verification proceedings (VPs).

DPPs are intended to resolve claims filed by a data subject or his or her legal representative alleging that a data controller has failed to attend to a claim exercising the data subject's ARCO rights or when the resolution of the data controller does not satisfy the data subject. VPs may be commenced *ex officio* by the INAI or at the request of a party.

An *ex officio* VP will take place following a breach of a resolution issued in connection with a DPP, or if a breach of the Private Data Protection Law is alleged to be founded

and substantiated by the INAI. During a VP, the INAI shall have access to the information and documentation deemed necessary, in accordance with the resolution originating the verification.

Penalties

In the event that, during a DPP or VP, the INAI becomes aware of an alleged breach of the Private Data Protection Law, a proceeding to impose penalties will commence assessing the infringement. The available penalties include the following:

a a warning issued by the INAI urging a data controller to comply with the data subject's demands. Note that this course of action is limited to certain types of infringement;

b fines representing an amount of between 100 and 320,000 times the UMA,[2] which is published by the National Institute of Statistics and Geography, which will be determined based on the nature of the infringement; and

c imprisonment for up to three years in certain cases, such as when someone authorised to process any personal data causes a security breach in relation to the data under his or her control with the purpose of obtaining a gain; or imprisonment for up to five years when someone processes personal data with the intention of obtaining a gain by deceiving, or taking advantage of the error of, a data subject or the person authorised to transfer any personal data.

The penalties set out in item (b) above may be doubled if the infringement involves sensitive personal data. Although the Private Data Protection Law does not entitle a data subject to receive any indemnification, in light of damages suffered because of a data controller's breach, it does acknowledge that any of the fines or penalties indicated above would be imposed against a data controller without prejudice to any liability that the data controller may have in civil and criminal law.

When assessing the fine or penalty to be imposed, the INAI would consider:

a the nature of the personal data;

b the inappropriateness of the failure to comply with the claim of the data subject;

c whether the action or omission was deliberate;

d the economic capacity of the data controller; and

e any reoccurrence of the breach.

Data controllers may challenge these sanctions or fines by means of a nullity claim before the Federal Court of Tax and Administrative Justice.

In addition, Profeco and Condusef are entitled to verify the adequate use of consumer information. If either of them finds that a corporation is engaging in unsolicited marketing to a customer enrolled in the Public Registry of Consumers or the Public Registry of Individual Users, or that it has used consumers' data for a purpose other than marketing, the following shall apply: Profeco may impose fines of up to 1.56 million Mexican pesos; or Condusef may impose fines of up to 2,000 times the UMA in force.[3]

2 Between 10,374 and 33,196,800 pesos in 2023.

3 207,480 pesos in 2023.

In recent years, the INAI has fined, inter alia, financial institutions, telecom companies and healthcare providers. However, most of these fines have been challenged by the data controllers concerned, and the proceedings are pending resolution. In 2022 most of the fines imposed were to companies engaged in financial and insurance services.

Since the enactment of the Private Data Protection Law, the INAI has been actively advertising the importance of complying with this law and pursuing those cases in which there are important breaches and it has imposed fines on several companies. The following are relevant cases in recent years that are worth mentioning.

Hospital

A fine of 4.6 million Mexican pesos was imposed on Operadora de Hospitales Ángeles, SA de CV (the hospital) on the grounds that the hospital was negligent when processing and answering a claim filed by a data subject to request access to her clinical file. Given that the clinical file contained sensitive personal data of the data subject, the fine was doubled.

Banorte

A fine of 32 million Mexican pesos was imposed on Banco Mercantil del Norte, SA, Institución de Banca Múltiple, Grupo Financiero Banorte (Banorte). Banorte collected sensitive personal data without the consent of the data subject and stored the data without a legal justification in breach of the principles of information, proportionality and legality, as it failed to deliver a privacy notice to the claimant and processed personal data of the husband of the claimant that was not necessary, adequate or relevant for the purpose of the data collection.

ii Recent enforcement cases

Considering that many of the resolutions issued by the INAI have been challenged by the data controllers and are pending resolution, and therefore these files have not yet been finalised, the cases shown at the INAI's public webpage for recent years have not been updated or have been removed from the webpage, or the name of the parties involved have been erased.

Several fines that amount to approximately 1.09 million pesos were imposed on Teraba Construcciones, SA de CV. The INAI's decision to fine the data controller was based on the following arguments:

a Teraba Construcciones, SA de CV failed to comply with the information, responsibility and legality principle, as it did not implement and disclose a privacy notice prior to the collection of personal data; and

b the company did not gather express consent to transfer the financial information of the data subjects; and it obstructed the process, considering that the data controller did not provide the information requested by the INAI.

Several fines that amount to approximately 145,680 pesos were imposed on Excel Technical Services de México, SA de CV. The INAI's decision to fine the data controller was based on the following arguments:

a Excel Technical Services de México, SA de CV failed to comply with the information, responsibility and legality principle, as it did not implement and disclose a privacy notice prior to the collection of personal data; and

b the company did not gather express consent to transfer the financial information of the data subjects.

Several fines that amount approximately 972,194 pesos were imposed on Sure Economía Global, SA de CV. The INAI's decision to fine the data controller was based on the following arguments:

a Sure Economía Global, SA de CV failed to comply with the information, responsibility and legality principle, as it did not implement and disclose a privacy notice prior to the collection of personal data; and

b the company did not gather express consent to transfer the financial information of the data subjects.

Several fines that amounted to approximately 193,440 pesos were imposed on Inprax de México, SA de CV (Inprax). The INAI's decision to fine the data controller was based on the following arguments:

a Inprax failed to comply with the information, responsibility and legality principle, as it did not implement and disclose a privacy notice prior to the collection of personal data;

b Inprax did not gather express consent to transfer the financial information of the data subjects; and

c the company also obstructed the INAI's verification process by not providing the information and documentation that was requested.

Several fines that amounted to approximately 322,4000 pesos were imposed on Constructora y Supervisora de Obra Prado Norte, COSUP, SA de CV (Constructora). The INAI's decision to fine the data controller was based on the following arguments:

a Constructora failed to comply with the information, responsibility and legality principle, as it did not implement and disclose a privacy notice prior to the collection of personal data;

b Constructora did not gather express consent to transfer the financial information of the data subjects; and

c the company also obstructed the INAI's verification process by not providing the information and documentation that was requested.

iii Private litigation

The Private Data Protection Law makes no provisions regarding remedies or financial recovery for the data subject as a result of a breach of data protection rights. However, data subjects are entitled to file a claim before the civil courts to seek indemnification resulting from moral damage. We are not aware of any claims of this nature. The first chamber of the Mexican Supreme Court has issued certain groundbreaking, non-binding court precedents resolving that, when awarding damages, courts and judges shall consider aggravating factors such as the degree of responsibility, to determine a fair indemnification, thereby openly recognising concepts such as 'punitive damages', which were not developed in court precedents.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Private Data Protection Law is applicable to:

a data processors not located in Mexico, but that process personal data on behalf of data controllers located in Mexico;

b data controllers that are not located in Mexico, but that are subject to Mexican laws as a result of an agreement or in terms of international laws; or

c data controllers using means located in Mexico (even if they are not established in Mexico), except if those means are merely for transit purposes, without involving the processing of personal data.

As a result of the above, foreign companies must always analyse whether their activities, or the activities of their affiliates, would result in the application of the Private Data Protection Law. Foreign companies have also faced certain challenges considering that, under the premise that privacy notices should be simple and easy to understand, the INAI has been reluctant to accept privacy notices issued by multiple data controllers, even if they are part of the same corporate group.

The Private Data Protection Law does not impose any obligation against data controllers on the location in which personal data should be stored or kept or even whether this should remain in Mexico. As described in Section IV, under the Private Data Protection Law, an international communication of personal data originating from a data controller may be either a 'transfer' or a 'remittance'. Any international data transfer will be subject to consent of the data subject and shall be evidenced by an agreement or any other document whereby the third party assumes the same data protection obligations undertaken by the data controller and the conditions for processing as consented to by the data subject and detailed in the corresponding privacy notice.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity is broadly addressed within the Private Data Protection Law and its Regulations, by establishing that all private entities processing personal data, and data controllers in particular, shall have adequate physical, technical and organisational measures to prevent any personal data breach. The Private Data Protection Law and its Regulations do not attempt to impose a catalogue of security measures to be adopted by those bound by them, but rather outlines general principles applicable to security measures that shall be implemented by those processing personal data. In that spirit, the INAI has issued certain documents in an effort to simplify the implementation of security measures, such as:

a the Recommendations on Personal Data Security outlining the minimum actions needed to securely process personal data; the Methodology for Analyzing Risk to assess the risks when processing personal data;

b the Guide to Implementing a Personal Data Security Management System to establish security measures based on the cyclic model of 'planning, doing, checking and acting'; and

c the Guide on Personal Data Security for Micro, Small and Medium-Sized Businesses, which guides such companies in compliance with the Private Data Protection Law and its Regulations with respect to security measures and the implementation of a personal data security management system.

A data controller must notify each data subject upon confirmation that a data breach has occurred, once it has taken any actions intended to assess the magnitude of the breach. The notice shall contain at least the nature of the incident, the personal data affected, advice on the actions that may be adopted by the data subject to protect his or her interests, the remedial actions that were immediately carried out and the means through which the data

subject may obtain further information. In addition, the data controller would have to take corrective and preventive actions and improve its security measures to avoid the recurrence of the same breach.

The Private Data Protection Law and its Regulations do not oblige a data controller to notify the INAI upon the occurrence of a breach or of the measures taken by the data controller. However, failing to comply with any of the obligations mentioned above may constitute an infraction under the Private Data Protection Law that may result in the imposition of sanctions by the INAI.

Although this is a non-binding document, in an attempt to avoid further cyberattacks or threats, the Cybersecurity Study includes cybersecurity recommendations for the financial system in Mexico including:

a preparedness and governance: having one responsible body or corporate governance body to lead information security and fraud prevention using digital means;

b detection and analysis of digital security events: prioritising the development of capacities using emerging digital technologies, such as big data, artificial intelligence and related technologies;

c digital security incident management, response, recovery and reporting: investigating the source of an incident and guaranteeing the design and implementation of policies or processes for its containment, response and recovery;

d training and awareness: providing training plans and carrying out prevention campaigns; and

e financial system authorities and regulatory bodies: issuing guidelines, recommendations and instructions on digital security best practices and verifying the provision of reporting mechanisms.

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

Software development is protected under the Copyright Law, so that the author of such software enjoys exclusive prerogatives and privileges of a personal and patrimonial nature.

In relation to software vulnerabilities in terms of the Private Data Protection Law and its Regulations, data controllers shall implement appropriate organisational, technical and physical security measures to protect personal data against unauthorised damage, loss, modification, destruction, access or processing. These measures shall be at least equivalent to those implemented for their own confidential information.

A data controller must notify each data subject upon confirmation that a data breach has occurred, once it has taken any actions intended to assess the magnitude of the breach. The notice shall contain at least the nature of the incident, the personal data affected, advice on the actions that may be adopted by the data subject to protect his or her interests, the remedial actions that were immediately carried out and the means through which the data subject may obtain further information. In addition, the data controller would have to take corrective and preventive actions and improve its security measures to avoid the recurrence of the same breach.

The Private Data Protection Law and its Regulations do not oblige a data controller to notify the INAI upon the occurrence of a breach or of the measures taken by the data controller. However, failing to comply with any of the obligations mentioned above may constitute an infraction under the Private Data Protection Law that may result in the imposition of sanctions by the INAI.

Also, the Federal Criminal Code includes a section for crimes related to copyright violations and cybercrimes.

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

Although there have been discussions and law projects to govern or restrain information technology platforms and specifically social media, no projects have been approved yet. The discussion has been centred upon trying to control publications and cyberbullying without affecting free speech rights. However, up to this date, no amendments or new laws have been approved.

In this regard, each technology platform that collects personal data will be responsible to comply with the Private Data Protection Law and its Regulations, including having a privacy notice specifying the data that will be collected and the purposes of the processing of that data.

XII OUTLOOK

We have been expecting the respective bills to make any intended amendments to the Private Data Protection Law since the previous edition of this publication; however, we anticipate that a bill will be submitted to harmonise the Data Protection Laws with Convention 108 and ETS 181.

Although the GDPR applicable in the European Union is not enforceable per se in Mexico, some provisions of the GDPR are intended to address processing beyond the borders of the EU, to the extent of the personal data of EU citizens or residents of EU Member States. As a result of the effectiveness of the GDPR, we foresee more interest in entities that intend to carry out any business operations in the EU (even through remote means), to comply with the standards imposed by the GDPR; and in Mexican companies whose parent company is headquartered in the EU, or that process personal data on behalf of EU companies or subsidiaries.

Also, there has been interest from various sectors to amend the Private Data Protection Law to specifically include biometrics as sensitive personal data. Various discussions have been held and we anticipate that this amendment will be passed in the near future.

Additionally, and as a result of the pandemic, the use of e-commerce was exponential in Mexico, together with the associated effects upon privacy and personal data. Therefore, some discussion on how to better protect an individual's information on platforms, webpages, apps and related means is something that is currently in the loop of commerce chambers and authorities. We are still expecting the modernisation of the Data Privacy Laws to consider the particularities of e-commerce with respect to the protection of personal data to materialise soon.

Finally, an initiative to enact a Federal Cybersecurity Law was filed before ,Congress and it is currently under discussion. This initiative adopts several protection concepts agreed under the United States–Mexico–Canada Agreement mainly with the purpose of increasing cybersecurity under a scheme of co-responsibility, prevention, combating and prosecution of cybercrimes, as well as the protection of personal data and respect for human rights.

ISBN 978-1-80449-214-7