by Gustavo Alcocer & Enrique Lara

Personal data protection has always been recognised as a fundamental human right by most jurisdictions all over the world. In Mexico it was not until a few years ago, when amendments were made to our legal system to regulate personal data protection, following international principles of transparency, legitimate use and proportionality as to when, who and for what purposes personal data is used.

Mexico took the first step on 2007, when the Mexican Constitution was amended to add section II in article 6 to establish that: “Any information regarding private life and personal data is protected in the terms and with the exemptions established by law.” A couple of years later in 2009 two decisive actions were carried out: a reform act was passed so that congress could have authority to legislate on personal data protection; and article 16 was amended, modifying the Constitution in order to establish that every person has a right to personal data protection affording each individual with rights to access, correct, and cancel its personal data controlled by third parties, as well as to oppose to its continued use, with certain exceptions such as national security, public order, public safety and health or to protect the rights of third parties, pursuant to the law.

A new federal law initiative entitled Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Federal Law for the Protection of Personal Data held by Third Parties) was enacted in Mexico and published on July 5 2010, entering into effect one year later (Personal Data Protection Law or PDPL). The main purpose of the PDLP is to protect personal data controlled by private parties. Along with its regulations (being discussed and soon to be issued) the PDPL will begin a new era of compliance, especially for personal data intensive industries and, depending on how these regulations are enacted, we will learn how innovation will be affected.

It’s hard to think of an industry that has low or no use of personal data. On the contrary, as the information revolution continues personal data is being collected, controlled, managed and used for many purposes and industries. Companies handling personal data in Mexico will not be able to collect, process, use or disclose identifiable information of an individual unless they meet the

conditions established in the PDPL and its rules. An important condition is the obligation of the controller of data to furnish notice and obtain consent from the person of whom data is being collected or used, and depending on the type of data, express consent may be required. Based on the PDPL as it relates to personal data an individual has the rights of access, correction, cancellation and objection.

The PDPL incorporates eight general principles that data controllers must follow when handling personal data: legality, consent, notice, quality, purpose limitation, accuracy, proportionality and accountability. With the exception of certain companies in the credit information business that are expressly excluded, this new law is having an important and unavoidable impact on the majority of the companies that operate in Mexico (including Mexican subsidiaries or affiliates of multinational companies whose headquarters are established in jurisdictions where data protection laws and rules are already in effect, such as the United States, Canada and Europe, and that may already have internal personal data compliance policies), due to the fact that most of them will be required to implement or adapt their policies and contractual framework to comply with the new provisions of the PDPL.

Policies to comply with PDPL and its rules will need to observe at least the actions listed under the headings below.

1. Notice and consent

Data controllers must furnish a privacy notice indicating what data is collected and for what purposes. When the data has not been collected directly from the individual, the data controller must still provide a privacy notice and notification of changes in the privacy notice. Moreover, this law establishes that the privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows: (a) where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been previously provided; (b) where personal data is obtained directly from the data owner by any electronic, optical, audio or visual means, or through any other technology, the data controller must immediately provide the data owner with

at least the information regarding its identity, address and purpose of the data processing, as well as provide the mechanisms for the data owner to obtain the full text of the privacy notice.

According to PDPL the privacy notice must contain at least: (i) the identity and address of the data controller collecting the data; (ii) the purposes of the data processing; (iii) the options and means offered by the data controller to the data owners to limit the use or disclosure of data; (iv) the means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of the PDPL; (v) where appropriate, the data transfers to be made, and (vi) the procedure and means by which the data controller will notify the data owners of changes to the privacy notice. On the other hand, consent may be obtained from the data owners, through a privacy notice; however, processing sensitive data or information about personal finances and assets requires express consent which must be recorded in writing, or electronically with authentication.

2. Right of data owners

Data owners have, among others, the right of access, rectification, cancellation and objection. According to the PDPL, any individual, or, where appropriate, the legal representative may exercise these rights. The Law requires the companies to appoint a specific person or department to address requests by individuals asserting these rights.

3. Data purpose of use

The PDPL requires companies to ensure that personal data is accurate and updated. It also requires the companies to dispose of the data once it has served the original purpose specified in the privacy notice. The Companies must make “reasonable efforts” to finish its processing of sensitive personal data as rapidly as possible. Notwithstanding the foregoing, the PDPL does not define the standard of “reasonable efforts”. Accordingly, companies might, at a minimum, consider adopting established industry practices, and implementing internal policies, that define time limitations on the processing of sensitive data, including its destruction, in order to fulfill this requirement. If a company

pretends to use the personal data for any purpose not outlined in the privacy notice, it is required to provide notice and obtain renewed consent from the data subject.

4. Data transfer

Transferring personal data to a third party will usually require an agreement that the transferee will assume the same obligations as found in the privacy notice provided by the transferor. The law provides that national or international transfers of data may be carried out without the consent of a data subject when the transfer is made to, among others, holding companies, subsidiaries or affiliates under common control of the company, or a parent company or any associated company working under the same processes and internal policies. In any case the standards of the law must be met. In most instances, a company must disclose to data subjects any planned transfer of personal data to third parties and include a clause in the privacy notice allowing the data subject to accept or deny such transfer.

5. Security measures

The PDPL requires all responsible companies that process personal data to establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorised use, access or processing. Furthermore, the PDPL establishes that data controllers will not adopt security measures inferior to those they keep to manage their own information.

6. Data breach notice

An immediate report is required to the individuals of any security breach occurring at any stage of processing their personal data that materially affects property or moral rights, so that they can take appropriate action to defend their rights.

7. Confidentiality

According to law, in all processing of personal data, it is presumed that there is a

reasonable expectation of privacy,

understood as the trust any one person places in another for personal data provided to be treated pursuant to any agreement of the parties in the terms established in the PDPL. In such regard, it is a requirement for companies and third parties involved in the processing of personal data to maintain the confidentiality of personal data at all times. The data controller or third parties involved in any stage of personal data processing must maintain confidentiality with respect to such data, and this obligation will continue even after the end of its or their relationship with the data owner or, as the case may be, with the data controller.

8. Penalties

Violation of this law can be punished with financial penalties, the amount of which depends on the gravity of the situation. The fines range from 100 to 360,000 days of mínimum daily wage ($600 to $2.6 million approximately) or double the amount when offences are committed over sensitive personal data. Criminal penalties may also apply as follows: (i) three months to three years of prison for any person that, authorised to process personal data, for profit, causes a security breach affecting the databases under his custody; and (ii) six months to five years of prison for any person who, with the aim of achieving unlawful profit, processes personal data deceitfully, taking advantage of an error of the data owner or the person authorized to transmit such data.

In summary the PDPL imposes restrictions and obligations for the controllers or entities handling personal data and their processing, in the understanding that processing is defined by the law itself, as the “retrieval, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data”.

But, why does this matter for innovation?

From our review of the draft PDPI rules, the treatment of sensitive personal data as it relates to scientific investigation is important, as a patient subject to protocol testing may exercise its rights to oppose or cancel information for the continued use in a particular study, affecting the validity of the whole research.

This may occur when the patient drops out and decides to discontinue the treatment. As you may know sensitive personal data is defined as the information that affects the most intimate sphere of the individual, the disclosure of which may result in discrimination or grave risk to the subject. Such data includes religious beliefs, political opinions, sexual orientation, race and health information. We may have practical solutions to avoid this scenario, for example by simply key-coding or encoding data for its continued use. It is desirable, however, that the proposed rules make a clear exemption to the cancellation or opposition rights as they relate to use of sensitive personal data for medical research reported to pharmaceutical companies, sponsoring clinical studies. Arguments have been made to establish that if sensitive personal data is not identifiable by researchers then their treatment of such data should not be subject to the requirements of personal data protection.

We believe that the PDPL and the extent and detail of how regulations and safe-harbour exemptions will operate will bring a variety of positive and different consequences that will affect innovation and business. Hopefully, the burden of compliance with personal data protection laws in Mexico and around the world will strike a balance to protect personal data without affecting innovation negatively.