Article **Journal-Law and Economy**
June, 2020 Vol.4 No.6 1-4

The Privacy and Data Protection in Mexico

La privacidad y protección de datos en México

QUINTANAR-MONDRAGÓN, Adrián†

Universidad Iberoamericana

ID 1st Author: *Adrián, Quintanar-Mondragón*

DOI: 10.35429/JLE.2020.6.4.1.4 Received March 28, 2020; Accepted June 30, 2020

Abstract

Where topics on the LFPDPPP as well as other regulations such as the GDPR of the European Union were discussed. Mexico has already published this law for 8 years and until today; there are doubts about how to enforce this law, as many companies are unable to comply with it, which entails imposing fines depending on the degree of violation or alteration of the personal information. In the same way, a large part of the citizens do not know how to make use of their ARCO rights or the companies that own sensitive data do not allow it. Throughout this document will address relevant and current issues in our country in relation to the protection of personal data.

Resumen

Donde se discutieron temas sobre la LFPDPPP así como otras normativas como la GDPR de la Unión Europea. México ya ha publicado esta ley desde hace 8 años y hasta el día de hoy; existen dudas sobre cómo hacer cumplir esta ley, ya que muchas empresas no pueden cumplirla, lo que conlleva la imposición de multas en función del grado de violación o alteración de la información personal. Del mismo modo, una gran parte de la ciudadanía no sabe hacer uso de sus derechos ARCO o las empresas propietarias de datos sensibles no lo permiten. A lo largo de este documento se abordarán cuestiones relevantes y actuales en nuestro país en relación a la protección de datos personales.

Citation: QUINTANAR-MONDRAGÓN, Adrián. The Privacy and Data Protection in Mexico. Journal-Law and Economy. 2020. 4-6: 1-4

† Researcher contributing as first author.

A Little history

The first formal effort to address personal data protection was introduced in 2002 when the 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 became effective on 6 July 2010 and was followed by the Regulations of the Private Data Protection Law on 22 December 2011.

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 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.

About GDPR

The General Data Protection Regulation (GDPR) (Regulation 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to reinforce and unify data protection for all individuals within the European Union (EU). It also deals with the export of personal data outside the EU.

The main objective of the GDPR is to give citizens and residents control over their personal data and to simplify the regulatory environment of international business by unifying regulation within the EU.

The new proposed EU data protection regime extends the scope of EU data protection legislation to all foreign companies that process data from EU residents.

In May 2018, the General Regulation of Data Protection of the European Union (GDPR) comes into force to improve the protection of personal data.

The GDPR will have a significant impact on organizations and their way of handling data, with potentially very large penalties for those companies that suffer a violation, reaching up to 4% of global revenues.

GDPR directly impacts the storage, processing, access, transfer and disclosure of an individual's data records and affects any organization worldwide that processes personal data of people in the European Union.

Mexican data controllers or processors not established in the EU who process personal data of individuals covered by the EU GDPR as provided under its territorial scope. It means that these data controllers and processors need to work on some EU technical and organizational measures to be compliant in less than a year. For other data controllers and processor, the EU GDPR may be a benchmark to consider as good practices.

Relevant aspects for compliance

Mexicans increasingly face privacy problems that include aspects such as identity theft and fraud. In Mexico, 88% of companies, have the perception of abiding by the Federal Law for the Protection of Personal Data Held by Individuals (LFPDPPP); However, this is not so.

Almost half, 48%, do not comply with at least one of the requirements of the law, which puts citizens' information at risk and exposes the data to cyber-attacks such as the recent WannaCry.

ISSN: 2524-2113

Juan Carlos Carrillo, director of Cybersecurity and Data Privacy of PwC Mexico, explained that for the firms, the perception of compliance with the law is limited only to have a privacy notice on their website, with which they have 87% of companies, but this is not even close to sufficiency.

One of the most relevant privacy problems in Mexico is related to firms that do not have the adequate security measures to protect the data, which generally leads to filtering or improper use of the information.

Due to the increase in news about the sanctions for the lack of compliance with The Data Privacy Law and the security problems that companies are facing, it is likely that in the coming years the focus will be more on data management and best information security practices to ensure that the data is found protected during their life cycle, establishing appropriate controls in relation to technical control and policies, procedures and administrative processes.

Most companies are starting to create their own culture of privacy and security, implementing an internal privacy policy in which they establish the mission and objectives of the company in relation to privacy and the way in which personal data must be handled. . They are also establishing clauses and privacy obligations in employee contracts.

Relevant data

From a sample of 309 companies surveyed, among which were micro, medium and large organizations and even with international presence in 24 states of the Mexican Republic, 43% were involved in situations that involved loss or leakage of information, and 86% are unaware the impact of these events.

To prevent type of leakage or theft there are few procedures, 88% of the companies consulted established works on privacy, but only 54% currently have a person in charge of said procedures. Regarding training, the percentage of companies that revealed never having submitted one rises to 46%, 22% did so once in the last seven years and 32% indicated that they trained their staff in data protection once a year .

During the last 12 months, 66% of the organizations consulted said they had not received access, rectification, cancellation and opposition requirements -meaning better known as ARCO rights-, compared to 39% that revealed whether they had received any of these requests.

Look to the future

This year, Mexicans are beginning to understand the law better and to learn more about constitutional laws regarding privacy. The most innovative companies in the country will face the challenge of the continuous movement of confidential information and the transactions that take place in the digital space, which will make them more vulnerable to attacks.

Organizations face unprecedented cyber threats against the data and information technologies they store, process and transmit. Companies from all sectors need to create good information security strategies according to their industry to build an environment that protects and applies security measures in their data and generates more confidence in the end user.

Referencias

Chávez, Gabriela (2017) Las empresas mexicanas no tienen ni idea de cómo proteger tus datos personales [En línea] Disponible https://expansion.mx/tecnologia/2017/05/17/las-empresas-mexicanas-no-tienen-ni-idea-de-como-proteger-tus-datos-personales

Cruz Ayala, César (Diciembre 2017) The Privacy, Data Protection and Cybersecurity Law Review - Edition 4 [En línea] Disponible https://thelawreviews.co.uk/chapter/1151292/mexico

Fernando Román Sandoval (2016) Protección de datos y leyes de privacidad. PwC p. 2

Forbes Staff (2017) Empresas, incapaces de cumplir con protección de datos personales [En línea] Disponible https://www.forbes.com.mx/empresas-incapaces-cumplir-proteccion-datos-personales/

PowerData (Noviembre 2017) GDPR: Lo que debes saber sobre el reglamento general de protección de datos [En línea] Disponible https://www.powerdata.es/gdpr-proteccion-datos.

Recio, Miguel (Junio 2017) GDPR matchup: Mexico's Federal Data Protection Law Held by Private Parties and its Regulations [En línea] Disponible https://iapp.org/news/a/gdpr-matchup-mexicos-federal-data-protection-law-held-by-private-parties-and-its-regulations/