Data privacy

Privacidad de Datos

FLORES-ROMÁN, Luis Hugo†

Universidad Iberoamericana

ID 1st Author: *Luis Hugo, Flores-Román*

DOI: 10.35429/JLE.2020.7.4.20.23 Received August 28, 2020; Accepted November 30, 2020

Abstract

Data privacy is an issue that has gained great importance worldwide, in such a way that several countries have legislated in favor of legal frameworks that safeguard the personal information of their citizens in the custody of companies and individuals; however, the implementation of these regulations still has several areas of opportunity, both in the implementation of technical and administrative measures by organizations.

Personal, Data, Privacy, Law, Regulation

Resumen

La privacidad de los datos es un tema que ha cobrado gran importancia a nivel mundial, de tal manera que varios países han legislado a favor de marcos legales que resguarden la información personal de sus ciudadanos en custodia de empresas y particulares; Sin embargo, la implementación de esta normativa aún tiene varias áreas de oportunidad, tanto en la implementación de medidas técnicas como administrativas por parte de las organizaciones.

Personal, Datos, Privacidad, Ley, Regulación

Citation: FLORES-ROMÁN, Luis Hugo. Data privacy. Journal-Law and Economy. 2020. 4-7: 20-23

† Researcher contributing as first author.

Introduction

Data privacy refers to the way in which the data or information should be treated according to its importance or criticality. This concept is traditionally applied to the personal data of individuals, which makes them identifiable, and can cover a wide range of information, from the name to detailed medical records.

In the digital age we live in today, this type of information is not only valuable for companies, but on multiple occasions is essential for its operation, in the same way that proprietary information or financial statements could be.

Considering the above, various regulations have been developed and strengthened in different countries in order to regulate the processing of personal data by companies, being notable examples the General Data Protection Regulation (GDPR) of the European Union and the local privacy law in Mexico (LFPDPPP.)

European Union General Data Protection

Regulation (GDPR)

This regulation, adopted in April 2016, aims to standardize data protection laws throughout Europe, protect the personal data of all citizens of the European Union and regulate the way in which companies treat such information[1].

Its principles remain faithful to the directive 95/46/EC, which it replaces, and to the guidelines of the Organization for Economic Cooperation and Development (OECD), which include:

1. Limitation of the collection. The data collection must be the minimum necessary to achieve the purpose for which they are collected.

2. Data quality. The data must be accurate, complete and current.

3. Specification of purpose. The purpose of the collection must be specified no later than at the time they are collected.

4. Limitation of use. The data should not be treated for any purpose other than the one specified.

5. Safeguarding of security. Security measures must be established to prevent loss, unauthorized access, destruction, use, modification or disclosure of data.

6. Transparency. There should be a general policy on transparency in terms of evolution, practices and policies related to data.

7. Individual participation. Individuals have the right to know what data the companies have about them, express doubts about the data related to their person and get their data deleted, rectified or completed[2].

In general, this regulation guarantees the following rights of the owner of the data:

– Notification of non-compliance. Notification of non-compliance will be mandatory when a data breach is likely to "create a risk to the rights and freedoms of the owners".
– Access. Right to obtain from the organization the confirmation of whether his data is being processed, where and for what purpose.
– Right to be forgotten. Right for the organization to delete his personal data, stop disseminating it and potentially cause third parties to stop processing the data.
– Data portability. Right to request the personal data that concerns him and transmit it to another organization.
– Privacy by design. It requires the inclusion of data protection from the beginning of the design of the systems, instead of as an addition.
– Data protection officers (DPO.) It will be mandatory only for those organizations whose central activities consist of processing operations that require regular monitoring of large-scale data or related to convictions and criminal offenses.

[1] EUGDPR.org. (2018). GDPR Portal: Site Overview. [Online]. Available at https://www.eugdpr.org
[2] Institute of Legal Investigations. (2018). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. [Online]. Available at https://archivos.juridicas.unam.mx/www/bjv/libros/7/3249/28.pdf

The GDPR enters into force in May 2018 and is applicable to organizations that process and maintain personal data of citizens of the European Union, regardless of their headquarters. Organizations can receive fines of up to 4% of their annual global turnover or 20 million euros, whichever is greater.

Mexico privacy law (LFPDPPP)

This Mexican law was published in July 2010, its regulations in December 2011 and its recommendations in October 2012. Its purpose is to protect personal data held by individuals, regulate their treatment and ensure the privacy of individuals[3].

Like the GDPR, this regulation establishes several guiding principles:

1. Lawfulness. Personal data must be collected and treated in a lawful manner in accordance with Mexican and international law.
2. Consent. The data processing is subject to the consent of the owner.
3. Purpose. The data can only be processed for the fulfillment of the purpose established in the privacy notice.
4. Information. The organization must make known the existence and main characteristics of the treatment to which the personal data will be submitted through the privacy notice.
5. Quality. The data processed must be accurate, complete, relevant, correct and up-to-date.
6. Loyalty. It establishes the obligation to treat data privileging the protection of the owner's interests and the reasonable expectation of privacy.
7. Proportionality. Only the data that is necessary, adequate and relevant in relation to the purposes for which it was obtained can be processed.
8. Responsibility. The organization has the obligation to watch over and answer for the treatment of the data that is in his custody[4].

Additionally, it establishes the so-called ARCO rights:

– Access. Right to ask organizations for a list of the data they have about the owner in their databases.
– Rectification. Right to update the data of the owner in the databases of the organizations.
– Cancellation. Right to request that the data of the owner cease to be treated by the organization.
– Opposition. Right to request the data of the owner not be treated for secondary purposes (for example, marketing.)

Organizations that violate this regulation and its provisions may be subject to fines of up to 76 million pesos and even imprisonment of up to 10 years for people who fraudulently disclose information.

Compliance with privacy law and privacy study in Mexico 2016

Six years after the entry into force of the local privacy law in Mexico, the consulting firm PriceWaterhouseCoopers (PwC) conducted a study[5] to know the status of implementation and compliance with this regulation in different companies in the country, which outputted worrying data.

Although 88% of the participating companies declared having initiated actions to safeguard the personal data of their customers and to have a privacy notice, the number of fines imposed by the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI), regulatory entity in Mexico, have increased from 1 in 2012 to 53 in 2016, being the main reasons not having a privacy notice aligned with the requirements of the law and to treat or transfer personal data to a third party without the owner's consent.

[3] Chamber of Deputies of the H. Congress of the Union. (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [Online]. Available at http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[4] Official Journal of the Federation. (2011). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [Online]. Available at http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

[5] PriceWaterhouseCoopers. (2017). Estudio de la Privacidad en México 2016: más allá de los compromisos. Mexico City: PwC.

December, 2020 Vol.4 No.7 20-23

Another important problem identified is not having an adequate governance framework regarding the privacy of the data. According to PwC, 34% of organizations do not have a privacy policy and only 49% have published and disseminated it to their staff. Similarly, 31% of companies do not have a process for the attention of ARCO rights and only 54% have a process published and disseminated.

Despite of the above, the organizations have run with luck, since 60% of them have never received an application to enforce ARCO rights, while 31% have received between 1 and 25 applications. Perhaps this makes us understand why only 55% of participating companies are willing to make a greater investment in their ability to protect the privacy of their data, while only 27% contemplate obtaining a certification in terms of privacy.

Conclusions

While efforts to create the necessary legal frameworks to protect the privacy of personal data have been tangible in various countries and entities, their implementation does not end up being very effective.

In the Mexican case, studies show that organizations still have deficiencies in their approach to data protection, either due to ignorance or because they consider it an unnecessary expense that does not give them any competitiveness.

A comprehensive vision of the treatment of personal data (classification, life cycle) is necessary in order to identify risks and the security measures that must be implemented, whether administrative (governance structure), physical and technical (controls and monitoring).

The success of a privacy program in organizations depends largely on the awareness of their employees, for which training programs can be implemented that promote and strengthen the culture of privacy within.

References

EU GDPR Portal (2018): Site Overview, https://www.eugdpr.org

National Autonomous University of Mexico (2018): OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://archivos.juridicas.unam.mx/www/bjv/libros/7/3249/28.pdf

Mexican Government (2010): Ley Federal de Protección de Datos Personales en Posesión de los Particulares, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Mexican Government (2011): Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

PriceWaterhouseCoopers (2017): Estudio de la Privacidad en México 2016: más allá de los compromisos.

ISSN: 2524-2113