Article **Journal-Law and Economy**
December, 2020 Vol.4 No.7 10-13

LFPDPPP

LFPDPPP

ARENAS, Jorge†

Universidad Iberoamericana, Especialidad en Seguridad de la Información

ID 1st Author: *Jorge, Arenas*

DOI: 10.35429/JLE.2020.7.4.10.13 Received August 15, 2020; Accepted December 20, 2020

Abstract

The LFPDPPP recognizes the rights of citizens (referred to in the Law Headlines) to protect your privacy and empower people to apply to the responsible, at any time, access rectification, cancellation or opposition regarding the personal data that concerns you. Derived from the above, data processing personal is subject to the consent of the Owner. all individuals, such as companies, non-governmental organizations.

Law, Citizen, Personal, Sanctions

Resumen

La LFPDPPP reconoce los derechos de los ciudadanos (referidos en los Titulares de la Ley) de proteger su privacidad y facultar a las personas para que soliciten al responsable, en cualquier momento, la rectificación, cancelación u oposición de acceso respecto de los datos personales que le conciernen. Derivado de lo anterior, el tratamiento de datos personales está sujeto al consentimiento del Titular. todas las personas, como empresas, organizaciones no gubernamentales.

Derecho, Ciudadano, Personal, Sanciones

Citation: ARENAS, Jorge. LFPDPPP. Journal-Law and Economy. 2020. 4-7: 10-13

† Researcher contributing as first author.

Introduction

Non-profit organizations, among others, have the obligation to inform the Data Holders by means of the privacy notice of what is collected from them and for what purposes. The Law establishes as a violation that the request for access, rectification, cancellation or opposition to the processing of the personal data of the citizen is not complied with, as well as acting with negligence or fraud in the treatment of the same. It also sanctions whoever collects or transfers this data without the express consent of the Holder and prohibits the creation of databases in contravention of said Act.

LFPDPPP

The LFPDPPP regulates the right to the protection of personal data so that this information, in the possession of those responsible, has a legitimate, controlled and informed treatment. Therefore, the Mexican Law includes rules, requirements, conditions and minimum obligations to achieve the proper treatment of personal data held by those responsible, without this being translated into the imposition of barriers to the development of economic activities of Mexico.

Article 14 of the Mexican articles of the constitution related to LFPDPPP establishes that both the responsible party and the person in charge are obliged to observe compliance with the principles of protection of personal data (lawfulness, consent, information, quality, purpose, loyalty, proportionality and responsibility), and Therefore, they must establish and maintain administrative, technical and physical security measures to protect personal data against damage, loss, alteration, destruction or unauthorized use, access or processing, which is provided for in Article 19 of this Law .

Similarly, Article 20 of the Law establishes that security breaches that occur in any phase of the processing of personal data that significantly affect the economic or moral rights of individuals, must be immediately reported by the person responsible, to so that the holders of this information can take the corresponding actions for the defense of their rights.

Article 48 of the Regulations of the Law states that the person responsible must adopt measures to achieve the proper treatment of personal data, privileging the interests of the owner and the reasonable expectation of privacy. Among the measures that may be adopted by the person in charge are at least the following:

1. Develop mandatory and enforceable privacy policies and programs within the responsible organization.
2. Implement a training program, update and awareness of the staff on the obligations regarding the protection of personal data.
3. Establish a system of internal supervision and surveillance, external verifications or audits to verify compliance with privacy policies.
4. To allocate resources for the implementation of the programs and privacy policies.
5. Implement a procedure to address the risk for the protection of personal data for the adoption of new products, services, technologies and business models, as well as to mitigate them.
6. SAW. Periodically review security policies and programs to determine the modifications that are required.
7. Establish procedures to receive and answer questions and complaints from the holders of personal data.
8. Have mechanisms for compliance with the policies and programs of privacy, as well as sanctions for non-compliance.
9. Establish measures for the assurance of personal data, that is, a set of technical and administrative actions that allow the responsible party to compliance with the principles and obligations established by the Law and its Regulations.
10. Establish measures for the traceability of personal data, that is, actions, technical measures and procedures that allow the tracking of personal data during your treatment.

Article 60 of the Regulations of the Law stipulates that the person in charge must determine the security measures applicable to the personal data that he / she deals with, considering factors such as:

ISSN: 2524-2113

1. The risk.
2. The sensitivity of the personal data processed.
3. The technological development.
4. The possible consequences of a violation for the owners.
5. The number of owners.
6. The previous vulnerabilities occurred in the treatment systems.
7. The risk due to the quantitative or qualitative potential value that personal data treated by a third party not authorized for possession may have.
8. Other factors that may affect the level of risk or that result from other laws or regulations applicable to the person responsible.

The equivalence table

The Equivalence Table is a reference material for those responsible and in charge that will allow them to evaluate if the implementation of certain international standards in terms of information security and privacy in their organization facilitate compliance with the requirements and obligations established by Law and its Regulation with regard to security measures, as well as the Recommendations on the Security of Personal Data issued by the Institute.

The advantages of the Equivalence Table are the following:

1. Provides technical support to those responsible and charged with the protection of personal information.
2. It contains international standards related to information security and privacy and wide acceptance in Mexican organizations.
3. It helps determine if the implementation of the controls established in international standards related to information security and privacy facilitate compliance with the obligations and requirements established by the LFPDPPP.
4. Facilitates those responsible and charged with the fulfillment of their obligations in
5. security matter of personal data.
6. Help reduce the impact in terms of implementation costs of the LFPDPPP.
7. SAW. Enriches the purpose of binding self-regulation schemes in terms of personal data protection.
8. Help those responsible and managers demonstrate to the Institute the compliance with the obligations set forth in the LFPDPPP.

Figure 1 Equivalence Table

The privacy notice in the modalities to which it refers, in the following cases:

1. When the personal data is obtained personally from the owner, the person in charge must make available the integral privacy notice;

2. When the personal data is obtained directly or indirectly from the owner, the person in charge may make the integral or simplified privacy notice available to them.

3. III.When the space used to obtain personal data is minimal and limited, so that the personal data collected or the space for the dissemination or reproduction of the privacy notice are also used, the notification modality may be used. short privacy.

The provision of the simplified or short privacy notice does not exempt the person responsible for their obligation to provide the mechanisms so that the owner can know the content of the integral privacy notice. The person in charge will not be able to establish a charge for the owner for the use of these mechanisms.

The person in charge may opt for any of the three modalities referred to in the Eighteenth of these Guidelines for making his privacy notice available, in accordance with the conditions set forth in this guideline, regardless of whether he is obliged to have the comprehensive privacy notice.

Mechanisms for the owner to know the integral privacy notice.

The simplified privacy notice should indicate the mechanisms that the person in charge has implemented so that the owners can know the integral privacy notice.

For the election of these mechanisms, the person in charge must choose those that are easily accessible to the holders and with the greatest possible coverage, considering their profile and the way in which they maintain contact with the person in charge; free; that they are duly enabled and available at all times, and that they make access to information simple.

When the simplified privacy notice is made known to the owners by remote or local means of electronic communication, optics or other technology, by that same means should be made available the comprehensive privacy notice.

The short privacy notice must contain, at least, the following information elements, in accordance with the provisions of the guidelines of this Section:

1. The identity and address of the person responsible;
2. The purposes of the treatment, and
3. The mechanisms that the responsible person offers so that the owner knows the integral privacy notice.

The immediate disclosure of the aforementioned information does not exempt the person responsible for the obligation of provide mechanisms so that the owner knows the content of the comprehensive privacy notice.

Conclusions

Regardless of the fact that it is about complying with a series of legal provisions to avoid possible sanctions to the Responsible, the most important thing is to consider that both the physical and moral persons who handle personal data, compliance with this Law provides them with a competitive advantage over the others, and as today some companies emphasize the importance of being socially responsible, or in their case ecological organizations; it is propitious that they can indicate as added value that they adequately protect the personal data of their clients, workers, suppliers and the general public.

The importance that responsible treatment of personal data has gained, even more so in this era in which the technological revolution has meant that they have a pecuniary value for certain companies, which use them for marketing or commercial purposes.

The Federal Law on Protection of Personal Data in Possession of Private Parties, published in the Official Gazette of the Federation on July 5, 2010, obliges all those responsible for the processing of personal data to comply with various obligations, in order to achieve a transparent, responsible and informed management of them.

It is important for companies to be updated and comply with the requirements of the Law, as this provides benefits that have been exposed in this guide.

References

IFAI. (2010). tabla de equivalencia funcional de estándares en materia de medidas de seguridad en el marco de la LFPDPPP. Mexico City: IFAI.

NYCE, (2010) Desarrollo Conceptual del Modelo de Certificación en materia de Protección de Datos Personales, en el marco de la LFPDPPP y demás normatividad aplicable en la materia, Mexico City NYCE

Secreteria de Economia, (2013) Lineamientos del Aviso de privacidad, Mexico City, Secretaria de Economia