

# Technical Summary

---

## Toolkit para empresas en Materia de Seguridad de la Información



## INTRODUCTION

The Information Systems Safety Company Toolkit arises as an imperative need to support and guide individuals and corporations obliged under the terms of the Personal Data Protection Withheld by Individuals Federal Act, to safeguard, and in general, carry out personal data processing in a safe way.

It is addressed to the people responsible for processing personal data within the private sector -independent of their industry- and its aim is for the user, even without any knowledge whatsoever of the content of the Personal Data Protection Withheld by Individuals Act (LFPDPPP by its acronym in Spanish) to be able to perform Control Enhancing Mechanisms within their organization, in such a way that the data being processed is relevant, correct, and updated, according to what the hereinabove mentioned Act states.

It is a tool that allows thorough compliance with the Personal Data Protection Withheld by Individuals Act (LFPDPP), by achieving:

1. To explain what personal data is.
2. To distinguish personal data from sensitive data, as well as other type of information.
3. To be able to publish the obligations as someone responsible of personal data being processed.

4. Writing the corresponding proprietary Privacy Notice, as applicable in each the industry or commercial sector.
5. Form your Personal Data Department, according to your organization's profile and train your personnel to comply with the Personal Data Protection Withheld by Individuals Act, in a preventive manner, or before an ARCO rights exercise, and before requirements or verification visits from IFAI (Access to Information and Data Protection Federal Institute by its acronym in Spanish).
6. To define the volume of personal data being processed and evaluate if they are being duly protected.
7. To take the corresponding safety measures to protect the personal data you manage.
8. To implement a continuous self-evaluation mechanism, thus being always in compliance with the Personal Data Protection norms.

The aforementioned, to comply with the Liability Principle, stated in Article 14 of the Personal Data Protection Withheld by Individuals Act.

To develop this group of tools, international standards and principles in the subject-matter were taken into consideration, as well as the national applicable legislation.

## **CONSERVATION PERIOD AND DUTY IN THE FEDERAL REGULATION**

### **Legal Grounds**

LFPDPP Regulation .- Article 37: *"The personal data conservation period should not exceed the necessary to comply with the purposes which justified processing, and should follow the applicable provisions in the subject-matter in questions, as well as **taking into consideration the data administrative, accounting, fiscal, juridical, and historical aspects**. Once the processing objective(s) have been complied with, and whenever there is no existing legal or regulatory provision establishing the contrary, the person who is responsible shall proceed to cancel the data in possession after their being blocked for later deletion".*

### **Basic Information or Principles for Development**

The purpose and liability principle were taken into consideration, since the personal data should be kept in observance to what is foreseen by any and all regulation deemed applicable, even after the purpose for which the personal data has been complied with.

Also, obligation to confidentiality was taken into consideration, which is addressed in diverse regulations, such as in the case of the Health sector.

### **Impact and Usefulness**

Knowing the established conservation periods in diverse regulations would allow those responsible and the owners to know how long said personal data ought to be preserved as per the law, which shall have to be considered within the blockage

periods under the terms of the right to cancellation exercise, or else whenever the purpose of collection for said personal data is fulfilled.

In the same way, those responsible shall allow compliance with the data conservation legal obligations as per the stated corresponding periods, and avoid being sanctioned for noncompliance in the care of the corresponding competent authorities in the subject-matters in question.

### **Challenges**

A detailed analysis of all the federal regulation was carried out, including that issued by the Congress of the Union, as well as the regulation issued by the President, and the regulation stated in the Mexican Official Norm (NOM by its acronym in Spanish).

The criteria used in the search served the terms: personal data, personal data, private life, privacy, confidentiality, conservation, and storage.

Although much of the information did not through any results, i.e. provisions in data conservation subject-matter, much of it threw information regarding information confidentiality.

Without a doubt, this section shall be of great use for those responsible of processing the data, as well as for the owners, since the personal data protection issue must be addressed from an integral point of view serving any and all regulation which may result applicable and not only the Personal Data Protection Withheld by Individuals

Act and its Rules, in order to avoid those responsible of being sanctioned, even by different authorities other than the IFAI.

## **DATA STRATIFICATION AND VOLUME**

The Data Stratification and Volume stage is a tool that allows an effective and efficient identification, as well as the type and volume of the data processed by a company.

The tool contains a list of data that the entrepreneurs should select, according to the data requested to employees, clients, providers, and visitors. Such listing is based upon experience, which indicates the data is the most common requested to that kind of people.

In the same way, the results to be thrown are valuable data for the company, since when knowing the type of data and volume being processed could, in later stages, carry out a better privacy notice, since it shall be known if financial or sensitive data is used, and which shall ask for processing in writing.

When carrying out this exercise, the user shall have an inventory of the data he processes, therefore complying with the legal requirement for data safety, as stated in Article 61, Section I of the Personal Data Protection Withheld by Individuals Act Regulation.

As we can observe, the Data Stratification and Volume stage is of great use for the user, since apart from knowing the status in which the company is regarding the type and volume of data it processes, it can also be used to comply with one of the most important legal requirements in Personal Data safety subject-matter.

## **RISK ANALYSIS AND SAFETY MEASURES**

The Toolkit is a tool that supports organizations to define the measures to be implemented to protect personal data as stated in Article 48 of the Regulation. Said measures ought to consider privacy policies and programs, training, update and personnel awareness, supervision systems, and internal surveillance, external audits or verifications, allocate resources, take care of the risk of personal data, review safety policies and programs, receive and answer doubts or claims, issue sanctions in case of noncompliance, establish measures for personal data assurance and its traceability.

As part of the measures, it is necessary for organizations to define a strategy with the safety actions for the required personal data and the possibility to implement a Personal Data Management System.

The Toolkit is a support for the organizations to carry out the activities that follow, and therefore achieve compliance with Article 61 of the Regulation:

1. Carry out a personal data inventory by category and type of collected datum.

There is a format to support the organizations in the structure of its inventory.

2. Identify the involved treatment systems in any phase of the personal data life cycle, from the formats provided in the Toolkit. The organization shall be able to identify the systems, or the media where they are processed, storage, or used for required personal data transfer by the organization to render the services or sell the products.
3. Determine the functions and obligations of the people in the organization who are involved in any stage of the personal data processing stage.
4. Carry out a risk analysis consisting of the identification of risks, and estimating the possible risks to personal data. The Toolkit includes a list of threats and vulnerabilities proposed that may be deemed by the organization to define its own scenarios. Once identified, the criteria is established based upon the volume of personal data, its sensibility by type, exposure, and traceability of the data.

To evaluate the risk, and as a result of such analysis, the organization shall identify from a quantitative scale easily understood, those high risks that menace the safety of personal data and which require immediate attention for processing. To carry out this analysis, the Toolkit provides a series of formats which shall help to gather and analyze the information.

5. Perform a gap analysis regarding the controls established in the Guide to Implement a Personal Data Safety Management System, a document issued

by the IFAI. In addition to the format for the analysis to be carried out, a control map ins provided for the following documents:

- a. SGSDP Guide.
- b. ISO/IEC ISO 27001:2013 Standard.
- c. MIPYMES Guide.

As a result of the risk and gap analysis, the organization may perform a work plan to implement the lacking safety measures, and therefore include in the Annexes the norms, standards, recommendations, and guidelines that may be consulted, in addition to the support information which shall help select the necessary controls to mitigate the risks and close the identified gaps.

Performing these activities shall allow the organization to implement a Personal Data Management System formed by the stages established in the Recommendations regarding personal data safety, and which are hereinbelow presented:

- **PLAN:**
  1. Establish the scope and objectives.
  2. Carry out a personal data management policy.
  3. Establish functions and obligations for those who process personal data.

4. Carry out a personal data inventory.
5. Carry out the personal data risk analysis.
6. Identify the safety measures and gap analysis.

- **IMPLEMENT/OPERATE**

7. Implement the applicable safety measures to personal data.

- **MONITOR/REVIEW**

8. Reviews and audit.

- **IMPROVE**

9. Continuous improvement and training

**PRIVACY NOTICE**

### **Legal Grounds.**

According to Article 12 from the Personal Data Protection Withheld by Individuals Federal Act (LFPDPPP by its acronym in Spanish), the person responsible shall be obliged to inform the data owners which information is collected from them and for what purpose through the Privacy Note. Article 16 of the same Code of Laws lists the elements said Notice should include. Additionally, the SECRETARIA DE ECONOMIA published the document Privacy Notice Guidelines describing at more detail the characteristics and elements of the Notice.

### **Basic Information or Principles for Development.**

Basic documents for the present section were the Personal Data Protection Withheld by Individuals Federal Act, its Regulation and the Privacy Notice Guidelines.

### **Impact to the Final User.**

The final user, entrepreneur, or professional service provider, requires instruments and tools that help him develop its own Privacy Notice. It is not just about having a tool automatically developing the Notice, it is about the individuals to be conscious of what it is, why it is necessary, and each one of its elements. Correct training in data protection subject-matter results inviable for many individuals processing them. However, they can duly comply with the LFPDPPP is they see a direct application into their specific case.

Additionally, we consider the individual, i.e., the person responsible for processing the personal data should be conscious of the sanctions that he may be imposed.

The Act, as it has explicit sanctions, as well as a specific sanctioning procedure, it becomes tangible. It is less probable that a person commits an infraction to a law if he knows the direct consequence.

Lastly, it is undeniable that those responsible, just as it happens with all companies, they modify their activities, processes, and internal norms. Privacy Notices should be updated according to the modifications that take place. At first glance, a tool that generates a Privacy Notice is enough, however, the concrete instructions shall make those Responsible to identify the concrete changes that should be known by the individuals whose personal data is being processed.

**Brief explanation of the challenges faced when developing it, and in some way make shine their contribution.**

The biggest challenge of this activity has definitely been to think about the wide range of existing companies. All individuals, while they are not making purely use of the personal data they have in their power, they are obliged to have a Privacy Notice. Therefore, a standardized Privacy Notice shall take into consideration the different industry branches. We believe there may not be only one format for all those Responsible of personal data to adopt. It is them who should adapt the support formats as it best serves their activities.

**PERSONAL DATA PROTECTION DEPARTMENT**

Article 30 of the Personal Data Protection Withheld by Individuals Federal Act states that those Responsible for processing personal data are obliged to designate a person or department in charge of personal data.

In accordance with the Personal Data Protection Withheld by Individuals Federal Act, the functions of said personal data officer or department shall be the following:

- Process the personal data holders' requests to exercise the rights to which reference is made in the Law, and
- Promote personal data protection within the responsible person's organization.

The IFAI recommends that these functions are carried out by the person responsible himself, or else, by a person designated thereof whenever considered or foreseen that the amount of requests made by the personal data holders regarding their access rights, rectification, cancellation, and opposition (ARCO), and, in general, personal data, as well as compliance with the obligations stated by the Law, and commitments acquired around the personal data itself, to be duly dealt with.

Also, the personal data protection functions may be in charge of one person whenever the capacity of the person responsible does not allow him to designate greater resources to deal with these tasks, in which case, it shall be important for the person responsible to evaluate if it is convenient to implement procedures that allow more efficiency in his functions to avoid any noncompliance with the Law.

The functions recommended in right request attention subject-matter are the following:

- a. Establish and manage the procedures to receive, process, follow up, and timely assist the requests to exercise the rights to access, rectify, cancel, and oppose, as well as to assist on claims or requests presented by the holders, and which are related to the policies and/or practices for personal data protection developed by the organization, and
- b. Monitor the progress or changes in legislation in personal data privacy and protection subject-matter that may impact the guiding principles and actions developed in this subject within the organization, making the necessary adequacies.

Regarding the promotion or personal data within the organization, the functions recommended by the IFAI are the following:

1. To design and execute policies and/or practices for personal data protection within the organization, or else, to adapt and improve the existing practices within the provisions of the Law;
2. To align these policies and/or practices -including its objectives, strategic actions, action lines, general and specific roles and responsibilities assigned, and an implementation procedure and period- for the internal processes of the organization that demand or enjoy personal data;

3. To develop a mechanism to evaluate effectiveness and efficiency of the policies and/or practices;
4. To monitor and evaluate the organization's internal processes linked to obtaining, using, exploiting, conserving, enjoying, cancelling, and transfer personal data in order to be sure the information is protected and processed in accordance with and observing the Act;
5. To participate and coordinate actions with other areas of the organization, such as Legal, Information Technologies, Information Safety, Marketing, Customer Support, Human Resources, among others, in order to assure due compliance with the privacy policies and/or practices in its internal processes, formats, notices, resources, and management carried out;
6. To assure compliance with the Act and other applicable regulation of the personal data protection policies and/or practices;
7. To spread and communicate the implemented personal data protection policies and/or practices within the organization, as well as to train all personnel on them;
8. To promote a personal data protection culture oriented to increasing the personal and involved third party awareness, such as managers, in processing personal data;
9. To monitor compliance of subsidiary or affiliate partnerships' personal data protection policies and/or practices under common control of the organization or any partnership of the same group operating and to which these practices may be applicable;

- 10. To identify and implement the best practices regarding personal data protection;
- 11. To promote adopting self-regulating schemes, and
- 12. To be the organization's representative in personal data protection before other entities.

Regarding the options the person responsible has to form his personal data department, are the following:

<b>Individual:</b>	Should perform by himself the personal data protection functions.	
<b>MiPyME (micro, small and medium enterprise):</b>	Should decide if one of the following is designated:	
	<b>1) A person</b> part of the structure or business of the responsible entity (employee or company executive).	<b>2) A department</b> in the organization: <ul style="list-style-type: none"> <li>a. Formed by different areas of the company, or</li> <li>b. with people who shall only have the task of managing said department.</li> </ul>
	<b>3) A manager</b> (individual or legal entity who solely or jointly with other ones processes the personal data on behalf of the responsible entity) other than the organization performing said task.	

