



# Information Technologies Industry Development Project

**PROJECT:  
DEVELOPMENT OF SELF-MANAGEMENT MANUALS THAT  
PROMOTE THE DUE PROTECTION OF PERSONAL DATA AT  
CORPORATIONS**



This document is the **EXECUTIVE SUMMARY** of the Project entitled “Development of Self-Management Manuals that promote the due Protection of Personal Data at Corporations” developed – in five stages or deliverables – by the Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI, Mexican Chamber of the Telecommunications Electronics and Information Technologies Industry) upon instructions of the Ministry of Economy and Prosoft 2.0, with the purpose of developing an assurance culture to contribute to self-management of corporations in order for them to comply properly with the *Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Federal Law on Protection of Personal Data held by Private Parties)* and its related regulations, registered in the Project of the World Bank, *Component F: Institutional Strengthening and improvement of the legal and regulatory framework*.

It is a project that is closely related to one of the most important legal advances in Mexico and that allows for offering legal certainty in the use of the Information Technologies (IT) to the consumers and other economies, such as the publication of the Mexican Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP in Spanish) on July 5, 2010, in the *Diario Oficial de la Federación (DOF, Official Gazette)*; of its Regulation (RLFPDPPP in Spanish) on December 21, 2011, as well as the Privacy Notice Guidelines and the Parameters for the proper development of the binding self-regulation systems described in article 44 of the LFPDPPP in the DOF on January 17, 2013.

## I

In the two first stages of the study, the work consisted of researching the models and procedures that may be used as reference by the companies in relation to the treatment of personal data, but that may also be useful to guide the preparation of Manuals that will eventually concentrate and orient the efforts of the key personnel regarding the mechanisms to be applied to achieve the adequate protection of information, the access to ARCO rights, the implementation of security measures, and the verification of the compliance with the above.

The third and fourth stages of the project included the analysis of recommendations and the development of forms with the purpose of creating an environment of suggestions and questions to determine a self-management framework for the proper alignment of corporate practices with the Mexican laws regarding personal data protection, to end with the preparation of a self-management manual that promotes the due protection of personal data at corporations.

## II

**First Deliverable: First Advance** covered "the research of the successful organization models of the companies in the IT sector regarding personal data processing". In this stage, international relevant models were researched based on the following four criteria: 1) that they have been issued by public and private government agencies with long personal data protection tradition and that are representative of the various systems in the subject, such as Canada, the United States of America, the European Union and the Asia-Pacific Region (APEC); 2) that they are used to present Mexican companies as safe harbors for data processing; 3) that they have been issued, as the case may be, as recently as possible to be aligned with the new world standards; and 4) that their standards or good practices have the highest possible incidence on the Mexican case in regard to the preparation of future self-management manuals.

Furthermore, the selection of countries and personal data protection models made is based on the relevance of the influence of each country regarding personal data protection. That is, considering the various existing international models of or approaches to personal data protection, such as the United States of America, Canada, the European Union or the APEC, representative countries or instruments (guidelines, manuals, etc.) have been chosen with the purpose to make the self-management manual the result of an extensive analysis of the best practices followed worldwide.

From the point of view of the best practices and gained experience, the chosen countries and instruments are the ones that, in view of the existing Mexican systems and instruments, are considered the most relevant ones by virtue of the practices followed in each case, as well as the experience gained in the application of regulations on personal data protection by the organization or *Data Protection Authority (APD, in Spanish)* in each case.

As to the diversity of the personal data protection practices, upon choosing countries from different geographical regions, it was also intended to enrich the set of personal data protection practices, which is reflected in the self-management manual through the applicable practical recommendations. It is in this way that the choice of countries allows for the contribution of diversity.

Thus, the chosen countries are those that are considered more relevant for the preparation of the self-management manual because of their relevance, experience and best practices regarding personal data protection.

According to such criteria, 34 self-management models –in 7 different categories- consisting of guidelines, checklists or toolkits of 7 countries (United

Kingdom, Canada, United States of America, Spain, Mexico, Australia and the Netherlands) were studied, apart from the ones applied by several international organizations (HL7 and ISO). That is, instruments prepared by public and private entities were studied. All of them are well-known as reference for the proper compliance with personal data and privacy protection.

The chosen reference instruments were the following:

- 1) Management/Accountability: 1) A Guide for Businesses and Organizations - Your Privacy Responsibilities; 2) Cómo Proteger la Información Personal: Una guía para Negocios (How to Protect Personal data: A Guideline for Business); 3) Data Protection Good Practice Note: Training Checklist for Small and Medium Sized Organizations; 4) Getting Accountability Right with A Privacy Management Program.
- 2) PIAs/Privacy by Design: 1) Privacy Impact Assessment Handbook Version 2.0; 2) Privacy by Design: Essential for Organizational Accountability and Strong Business Practice; Privacy by Design (ICO); 3) Privacy Impact Assessment Guide.
- 3) Security and Audits: 1) A Practical Guide to IT Security- Ideal for the small business; 2) Guía sobre Seguridad y Privacidad en el Comercio Electrónico (Guideline on Security and Privacy in E-commerce) (INTECO); 3) Guía de Seguridad de Datos (Guideline to Data Security); 3) Guidance on Data Security Breach Management; 4) ISO/IEC 27001:2005; 5) ISO/IEC 27002:2005; 6) Audit: A Guide to ICO Privacy and Electronic Communications Regulations Audits; 7) Auditing Data Protection A Guide to ICO Data Protections Audits ; 8) Data Protection Audit Resource Version 1.0; 9) Key Steps for Organizations in Responding to Privacy Breaches; 10) Privacy Breach Checklist; 11) Privacy Audit Framework under the New Dutch Data Protection.
- 4) Transfers / Remittances: 1) Data Sharing Checklists; Processing Personal Data Across Borders Guidelines; 2) Outsourcing A Guide for Small and Medium Sized Businesses; 3) Model Checklist application for approval of Binding Corporate Rules.
- 5) Privacy Notice / ARCO Rights: 1) Guía Práctica para generar el Aviso de Privacidad (Practical Guideline to Create the Privacy Notice); and 2) Guía Práctica para la atención de las solicitudes de Ejercicio de los derechos ARCO (Practical Guideline to attend requests to exercise ARCO rights).
- 6) Digital Environment Services (Cloud Computing and On Line): 1) Guidance on the Use of Cloud Computing; 2) Personal data Online Small Business Checklist; 3) The Guide to Privacy and Electronic Communications

- 7) Sensitive Data: Health 1) HL7 Role-Based Access Control (RBAC) Role Engineering Process, V. 1.3; 2) Circle of Care; 3) Technical Guidance Note: Subject Access to Health Records by Members of the Public; 4) Estudio sobre la privacidad y la seguridad de los datos personales en el sector sanitario español (Study on personal data privacy and security of personal data in the Spanish Health Sector)

The studied systems are bases or guidelines for personal data controllers and processors to have references that allow them to establish the controls necessary to minimize the risk implied in all types of processing, guaranteeing a high level of protection and a corporate culture regarding the *habeas data* basic right. They are models useful for Mexico to be able to be considered as a country with a proper level of personal data protection, both for the system it has from the regulatory and compliance standpoint, and for the fact that its companies operating in the IT sectors or using the IT to provide goods or services, are true *safe harbors* prepared to compete at global level.

**Second Deliverable: The Second Advance** covered the "research of the procedures that are references for the companies in personal data processing within the digital environment". In this stage, legal texts of countries or regions that have given a relevant drive to personal data protection and with which Mexico has permanent commercial relations were studied.

The regulations of the Economies chosen have proven their usefulness in the personal data protection field, and also their efficiency in the development of secure platforms for commerce in its various forms, including the electronic commerce. For this, the review of their specific classes will allow for the design of self-management manuals that promote the due protection of personal data in the Mexican companies.

The research in this second stage was carried out in two parts: analysis of the laws or legal texts regarding personal data protection of the following countries or regions: Latin America (Colombia, Costa Rica and Peru); Asia-Pacific (APEC); Australia; Canada; the United States of America; Mexico; New Zealand; and the European Union (Spain, France and the United Kingdom). And the second part was the examination of self-regulation models that can be used as reference regarding privacy good practices, such as guidelines or codes in America (Canada, the United States of America and Mexico); Asia-Pacific (Australia, Japan and Singapore); and the European Union (Europrise, Spain and the United Kingdom).

**Third Deliverable: The Third Advance** consisted of the “Preparation of a guideline of recommendations for the companies regarding models of organization and procedures when they act as personal data controllers or processors within the digital environment or the IT’s”. The methodology of this stage took into consideration the findings obtained in the first two stages of the study, i.e., from the analysis of the self-management models and the most important guidelines or *toolkits* of Economies that are advanced in this subject, as well as the research of the best practices and controls to be implemented by the companies regarding personal data protection through the compliance with standards or self-regulation schemes.

Based on the above, “recommendations” aimed at having those who process personal data –whether a data controller or a data processor – may adopt measures (procedures or mechanisms) that enable them to control the risk implied in the processing of personal data, avoiding, to the extent possible, penalizations that would derive from a breach or an inadequate compliance with the regulations on personal data protection. In one word, the recommendations prepared in this third stage refer to the following areas related to personal data protection:

Personal data protection principles: the persons who process personal data must comply with the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability to guarantee legal and legitimate (lawful and loyal) processing of personal data. The above implies that those who process personal data take care of guaranteeing the personal data protection basic right of the owners of such data; however, it must be taken into consideration that these principles are not absolute.

The recommendations are general and basic, as the LFPDPPP, its Regulation and other applicable regulations integrate the general legal framework on personal data protection in such a way that it must be understood that there are concrete obligations or issues that may require, as the case may be, specific compliance, apart from other specific legal provisions that may rule over the activities of personal data controllers and/or processors or certain aspects of personal data. Then, those who process personal data are the ones who have to analyze the risk implied in personal data processing and adopt or implement the legal and technological measures, mechanisms or procedures they may deem convenient. And such principles must be complied with at all stages of processing: at the time personal data is collected; during the handling or use of personal data; and once the processing has finished. It is important to mention that many guidelines and/or recommendations by information protection authorities (IPAs) worldwide are made available to the persons responsible for complying with the

regulations on data protection. These guidelines and/or recommendations may be used, as the case may be, as reference or model to be taken into consideration by the personal data controllers or processors to develop their own procedures or policies regarding personal data protection. Last, the personal data protection procedures or policies developed by those who process information must cover, as the case may be, the company governance areas, regulatory and/or legal compliance, compliance assurance and training / awareness.

Duties regarding personal data protection: additionally to the principles mentioned above, it is necessary to take into account the duties that must be guaranteed in personal data processing and which are related to confidentiality and security measures. As to the confidentiality duty, those who process personal data must guarantee that the persons who access personal data, at any stage of the process, must keep it confidential, and this obligation will survive even the end of the relationship with the personal data controllers. In regard to the security measures, their aim is to avoid alterations, loss, unauthorized processing or use of personal data, in such a way that they guarantee the integrity, confidentiality and availability of such data. Concretely, according to the Regulation of the Law, the security measures may be administrative, physical and technical. Thus, whoever processes personal data must adopt such measures to guarantee information confidentiality, integrity and availability.

ARCO Rights: In respect to the exercise of the access, rectification, cancellation and objection (ARCO) rights, and particularly in the case of Mexico, it is possible to follow the guidelines prepared and published by the IFAI (Instituto Federal de Acceso a la Información y Protección de Datos, Federal Institute for Access to Information and Data Protection), in such a way that when associated with the articles of the LFPDPPP and its Regulation, they rule the exercise of these rights. Now, it is important to discuss some general issues related to such exercise, the ownership or the persons entitled to exercise them and the contents of the applicable request. In any case, those who process personal data must make sure to establish a procedure that enables attending and responding on due time and form the requests to exercise the ARCO rights made by the interested parties. Concretely, an ARCO rights management procedure must include the following: 1) Request reception; 2) Review for requirement compliance (form and contents); 3) Answer to the request; 4) Attention (in a certain period of time) regarding the applicability of the request, and 5) Solution of enquiries / complaints. In relation to each one of the ARCO rights, the specific issues about the requirements of the exercise request in question must be taken into consideration. Last, companies must contemplate both the possibility of the exercise of the rights by electronic means, ensuring the due accreditation of identity by using advanced electronic

signatures or other ID proving electronic means, and the possibility of contracting a third party, that would become, as the case may be, a personal data processor, to attend the ARCO rights exercise requests.

Procedures to attend complaints or resolve disputes: These procedures are necessary because, with them, it is intended – if necessary – to gain and keep the confidence of the information owners fostering and making transactions easier to perform. As applicable, those who process personal data can either choose to adopt or adhere to procedures to attend and answer complaints or solve disputes, considering the traditional conflict solution systems such as the Online Dispute Resolution (ODR) which may be filed in Mexico, or systems already existing worldwide in relation to personal data protection. In any case, the procedures must be effective in such a way that they allow attending the complaints and/or enquiries properly, avoiding other risks inherent to the persons who process personal data.

Adhesion to self-regulation schemes: People who process personal data must take into consideration adopting or adhering to a binding self-regulation scheme, studying which binding self-regulation scheme is more adequate for the personal data processes they perform, and using the binding self-regulation parameters, such as: deontological codes, good professional practices codes, privacy policies, corporate privacy rules, trust seals, certifications and other schemes.

Compliance audit mechanisms: people who process personal data must take into consideration that compliance auditing must be an independent procedure. It can be performed by both the internal or external audit function, *a priori* or *a posteriori*, including the data protection and privacy policies and programs, as well as the procedures and controls established or adopted, and, covering the principles, rights, duties and other issues regarding information protection followed by the company.

Conclusively, those who process personal data must adopt measures and procedures to guarantee legal and/or regulatory compliance regarding personal data protection.

**Fourth Deliverable: The Fourth Advance** covered the “design of audit models or review guidelines for the security measures implemented or that the companies must implement in the digital environment to comply with the LFPDPPP”. In the case of the companies that do not have security measures, this stage of the project has the purpose of preparing a guideline that enables them to know the security measures they must implement in order to comply with the

LFPDPPP based on an audit model or a checklist of the implemented measures or the measures to be implemented in the digital environment. The proposal is associated to the observance of **the eight principles** of personal data protection (legality, consent, notice, quality, purpose, fidelity, proportionality and accountability); the **duties** of confidentiality and security measures; and the implementation of **procedures** that allow the personal data owners to exercise their access, rectification, cancellation and objection rights (ARCO rights).

To that end, the guidelines, checklists and toolkits prepared by the IFAI in Mexico and other information protection authorities (IPAs) and well-known organizations worldwide were studied in the first advance of this project. The audit model or verification guideline was divided into five parts: 1) the first describes briefly the elements included in the design of an audit; 2) the second evaluates the compliance with the principles set forth in the LFPDPPP and its Regulation, 3) the third evaluates the compliance of the confidentiality duties and security measures; 4) the fourth reviews the existence of procedures in the companies to exercise the ARCO rights; and 5) the fifth reviews the obligations to be complied with in case of personal data transfers.

For each one of the parties related to the compliance audit model or review guideline, a series of questions oriented to review (formularies) were prepared that enable “measuring” the extent of compliance with the Law and the Regulation, as well as correcting the non-contemplated or non-complied with terms within the management model implemented by the personal data controllers or processors in the digital environment or the IT environment. As exhibits to the above mentioned fourth report, an audit document form was proposed to integrate the information to be requested and questions to be made for each database that is subject to an audit or review; and the minimum elements of the audit report were proposed.

The last part of the project (**Fifth Delivery: The Fifth Advance**) summarizes the findings of the above listed deliverables and gathers them in a Compliance Manual: Self-Management Manual that promotes the due Protection of Personal Data at Corporations, aimed at explaining clearly the regulatory obligations and principles for the companies to adopt good practices and build a culture of responsibility regarding personal data protection processing.

### III

Upon preparing the Manual, it was considered important to underline the fact that for the digital economy to grow in Mexico, it is necessary to have public policy that fosters the knowledge each company must have about its strengths and weaknesses, as well as its values, responsibilities and better ways to be

competitive in the new global environments, the cross-border flow of information, the cloud computing and digital environment.

Within this context, *self-management* becomes a valuable corporate self-analysis mechanism applicable to each one of the corporate areas, and even more so now when a new list of duties for the private parties that process personal data has come up. All the above is derived from an increasingly more developed regulatory framework at international and domestic levels.

It is important to mention there is a study entitled *Estudio de Protección de Datos Personales entre Usuarios y Empresas* (Study on Personal Data Protection among Users and Companies), prepared by the Asociación Mexicana de Internet (AMIPCI, Mexican Internet Association) in 2012. Here, the following information is provided: 28% of the surveyed companies do not know what personal data is; 44% does not have the necessary knowledge about the LFPDPPP; three out of every ten companies do not know what actions they must perform to comply with the law; five out of every ten companies do not have sufficient knowledge about the access, rectification, cancellation and objection rights (ARCO).

To respond to these challenges, it is basic that there is a preventive manual or guideline for the companies to determine by themselves their extent of compliance of the rules set forth in the Mexican Constitution and the LFPDPPP, as well as the regulations, guidelines, parameters or guides derived from them, taking into consideration references and regulations of other countries or regions.

As to the digital environment, self-management and self-regulation are preventive alternate mechanisms, especially if we take into consideration that personal data is the basic raw material of economic activities, and that the personal data databases are a significant part of the intangible assets of many companies. Thus, the due protection of such data is a component of the value of all economic units.

According to the Terms of Reference of this project, the purpose of the Manual is to create a document that enables “concentrating and orienting clearly the efforts to be made by the key personnel regarding the mechanisms and procedures to be followed in order to guarantee proper information protection, access to ARCO rights, implement security measures and verify their compliance.”

Consequently, the Manual is intended to be a guideline or a set of guidelines for the personal data controllers and processors to establish – through self-management – the controls necessary to minimize the risks implied in all personal data processing, guaranteeing a better protection level, in order to develop a corporate culture regarding the basic right to protect personal data.

The self-management manual proposed herein will enable various types of companies to adopt their own measures and/or procedures to minimize the risk associated with personal data processing, avoiding any penalizations. Besides, the manual includes specific recommendations, for example, the processing of sensitive personal data, as well as any treatments in relevant specific sectors within the IT's field, such as cloud computing and marketing.

Organizing the analysis described herein according to criteria such as invoicing or employee number was not viable, as the regulations on personal data protection are aimed to a wider range of data controllers. That is, the regulations are applicable to an individual or a multi-national corporation that process personal data, without any distinction. Further, actually such criteria may not be relevant, for example, in the case of a data controller that, independently from its invoicing volume and/or number of employees, has entrusted personal data processing to another data controller.

Making some distinctions according to certain criteria may provoke a misinterpretation and improper practical application of the regulations by personal data controllers and/or processors. That is, compliance requirements are the same for both, and each one of them makes their own decisions about the measures and/or procedures they use. As an example, we can mention the fact that the legislative Committee Report of the LFPDPPP, when referring to the persons subject to compliance, states that "the exception of private groups or categories processing information, particularly the information considered especially protected, is not justified when there is no regulation that sets forth the guaranties of the owners of such information in the current laws." That is, the Law does not include any specific provisions beyond the subjects expressly exempted from the compliance with the LFPDPPP and of the sensitive personal data such as the one requiring additional measures regarding the compliance of principles to guarantee the owners' fundamental right to have their personal data protected.

Developing the Manual according to specific criteria may pose a problem regarding its practical application by the personal data controllers. Examples of certain measures may be found worldwide, such as the obligation to appoint a Data Protection Officer (DPO) in the case of companies with more than 250 employees discussed in the light of the amendment to Directive 95/46/CE that has been criticized in several public forums, because such measure may not respond properly to the actual reality. As, should a physician that handles the highly sensitive personal data of his patients not have such an officer, and not only a simple employee, due to the nature of the personal data he handles?

Thus, the criteria may become somewhat arbitrary in the practice, as for example a small company with less than 250 employees may be dealing with *big data* or sensitive personal data and be exempted from this obligation, while a technological company with over 250 employees that does not process any sensitive personal data would be subject to comply with the data protection officer obligation. This is a specific comment the ICO has published in its Proposed New EU General Data Protection Regulation: Article-by-article Analysis Paper published in February 2013.

Conclusively, the recommendations of this study are addressed to the PyMEs (Small and Medium-sized Companies in Spanish). It also offers specific recommendations in the cases of processing that requires additional measures, such as the sensitive personal data, in such a way that the Manual is fully practical and enables each data controller to adopt the measures he considers convenient and necessary to comply with the regulations according to the risks he finds. Moreover, the Manual is addressed to Mexican PyMEs, which means a universe of 5.1 million economic units: out of which 95.2% are micro-companies, 4.3% are small companies, .03% are medium-sized companies, and the rest are large companies. All of them have a poor privacy culture and, consequently, a poor personal data protection culture.

#### IV

The main document of this project is the **Self-Management Manual that promotes the due Protection of Personal Data at Corporations** conceived as a compliance manual or a set of guidelines derived from compared research, which has been divided in two sections: a section that presents the basic concepts to the users, that is, the companies that process personal data, and a second section integrated by recommendations and self-management formularies (guiding questions or checklists).

The conceptual part includes the description of the basic guidance elements for the users of the Manual to understand the recommendations and formularies section. This item considers the results of the above mentioned surveys to foster the personal data protection culture in the companies similar to the ones used by the Ministry of Economy in February 2011 and the AMIPCI in 2012, whose results revealed a gap in the knowledge about the topic. For this, it is justified that the Manual contains basic elements to understand the *habeas data* from the corporate point of view, not only as a simple compliance guideline or a local corporate compliance guideline, but also as a tool for the Mexican economic units to follow to the world trends in this topic.

Besides, the Manual contains a Self-Management Guideline to Comply with the Principles, Duties and Rights for the Protection of Personal Data Held by Private Parties. This Guideline includes accurate recommendations and formularies (guiding questions) that promote the self-management regarding: principles of data protection; traceability of data and compliance with principles; information protection duties (security measures and confidentiality); domestic and international transfer of personal data; specific personal data processing (cloud computing, advertising and commercial research); and personal data protection rights.

As support tools and exhibits, the Manual also includes: A guideline for the preparation of self-management audits or reviews regarding personal data protection, a regulations catalogue, and a glossary of terms.