Analysis of IT companies regarding personal data security to foster the role of the data processor according to the Federal Law on Protection of Personal Data Held by Private Parties

EXECUTIVE SUMMARY

July, 2012

INDEX

INTRODUCTION 3
I. STUDY SCOPE (Universe of Companies in the IT Industry and Survey) ... 7
I.1 Sample of the companies in the IT Industry.- 7
I.2 Questionnaire for the Survey.- 9
I.3 Performance of the Online Survey.- 10
I.4 Analysis of the information obtained from the Survey.- 11
II. IDENTIFICATION OF BEST PRACTICES 17
III. RECOMMENDATIONS AND CORRECTIVE ACTIONS 27
III.1 Recommendations.- 27
III.2 Corrective Actions.- 29
III.3 Public Policy.- 34

INTRODUCTION

After several years of analysis by the Mexican Congress, the ***Ley Federal de Protección de Datos Personales en Posesión de los Particulares*** ("**LFPDPPP**", Federal Law on Protection of Personal Data Held by Private Parties) was published on the *Diario Oficial de la Federación (Official Gazette)* on July 5, 2010, and later, its Regulation was issued by the President of Mexico on December 21, 2011. This represents a significant advance in the protection of the information privacy and self-determination constitutional rights, while fostering a framework that provides legal certainty to consumers and other economies in the use of Information Technologies (IT).

The Ministry of Economy has not overlooked the fact that with this new legal framework, there are great challenges to divulge the rights, obligations and duties that now the private parties and the companies of the IT industry that possess personal data of individuals must assume in order to guarantee its legitimate, controlled and informed treatment.

Truly, the LFPDPPP identifies as data controller for the treatment of information as the private individuals or companies that decide on how to treat the personal data, that is, any information about an identified or identifiable individual, and sets forth various basic principles, such as: the principle of accountability, according to which the data controller shall take care of complying with the personal data protection principles set forth in the Law, and must carry out the actions necessary to apply them.

The above, even when this information is treated by a third party upon request of the data controller. For this, the data controller must take the necessary and sufficient actions to guarantee that the privacy notice given to the owner of the personal data is respected at all times by him or third parties with whom he

has any legal relationship. Moreover, the LFPDPPP also defines the role of the **data processor** as the individual or company that by himself/itself or together with other individuals treats personal data on behalf of the data controller.

Within this context, it is relevant to mention that a significant number of IT-related companies act as data processors. For this, it is important to develop programs that drive the implementation of internationally well-known standards or practices in the subject of security, in order to promote reliability in their contracts and to foster the protection of personal data in the organizational practice.

For that, based on the provisions of the PROSOFT 2.0 and Component F of the World Bank Project (Loan 7571-MX), it has been entrusted to the *Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información ("CANIETI", National Chamber of the Electronic, Telecommunications and Information Technologies Industry)* to develop the project entitled **"ANÁLISIS DE EMPRESAS DE TI EN MATERIA DE SEGURIDAD DE DATOS PERSONALES PARA FOMENTAR LA FIGURA DEL ENCARGADO DE ACUERDO A LA LFPDPPP"** (Analysis of IT companies regarding personal data security to foster the role of the data processor according to the Federal Law on Protection of Personal Data Held by Private Parties), intended to foster, in the IT Industry, the importance of implementing security measures for the protection of personal data.

Furthermore, the **general object** of the project is: "To develop the skills and drive the use of good personal data security practices in the information technologies industry in order to offer certainty to the companies that subcontract them as data processors as described in the LFPDPPP", with the following **particular objects**:

a) Identify the domestic and international skills and practices regarding data security for IT companies.
b) Assess the extent of the current use of personal data security practices in IT companies in Mexico.

c) To issue recommendations and corrective measures for an effective practice of security measures to protect personal data in the IT companies.

Once the 5 stages of the Study (deliverables) have been completed, this **EXECUTIVE SUMMARY** was prepared containing a brief description of the first findings, as well as the recommendations for the effective practice of security measures on personal data protection in the IT industry.

Delivery	Contents	Activities
1st Delivery: First Advance	Report of a and b activities	a) Define the sample of the IT Industry companies (out of the 2,700 economic units), considering their specific characteristics and the number of companies in several states of the Republic. b) Determine the type of information to be requested from the IT industry companies to develop the online survey tool. It is recommended to use at least the following information: a. The company's main activity (software development, IT services, BPO, call center, etc.) b. Within its activities, does it process, store or safeguard any type of personal data? c. Does it offer *outsourcing* services to treat personal data?

Delivery	Contents	Activities
		d. Does it have any security measures in place? e. Which are the standards and/or norms used to implement internal security measures? f. Does it have any procedure in place in case there is a security breach?
2nd Delivery: Second Advance	Report on Activity C	c) Identify the best practices regarding personal data security, as well as the requirements of the legal framework provided by the LFPDPPP.
3rd Delivery: Third Advance	Results and documentation related to Activity D	d) Perform the survey of the sample of IT industry companies.
4th Delivery: Fourth Advance	Report on Activity E	e) Analyze the information obtained to project a descriptive statistical scheme on the existence, type, practice, effectiveness and problems of the implementation of the security measures to protect personal data.
5th Delivery: Fifth Advance	Report on Activity F and final document	f) Prepare the recommendations and corrective measures for an effective practice of the security measures regarding personal data protection in the information technologies industry to comply with the LFPDPPP.

I. STUDY SCOPE (Universe of Companies in the IT Industry and Survey)

This section summarizes the results of deliverables (advances) 1, 3 and 4, as they are closely linked to determine the universe of companies to be analyzed in order to determine their type of activity, what kind of data they process, which are the security measures they apply, etc., all through an online survey.

I.1 Sample of the companies in the IT Industry.- Based on the methodology established, the first part of the study covered the activities to define the sample of companies of the IT Industry (out of the 2,700 economic units), taking into consideration their specific characteristics and the number of companies in different states of the Mexican Republic, as well as to determine the type of information to be requested from the IT industry companies to develop the online survey tool.

First, all the companies that perform any of the following economic activities were considered as companies in the IT Industry:

a) Development of bundled software
b) Development of system software and tools to develop application software
c) Development of application software
d) Software consulting services
e) Computer system analysis services
f) Computer system design services
g) Computer system programming services
h) Data processing services
i) Database design, development and management services
j) Computer system implementation and testing services
k) Computer system integration services
l) Data processing services

m) Security services for computer and data processing systems
n) Services of analysis and risk management of computer and data processing systems
o) Business processes based on the use of computer and communication systems
p) Added value analysis, design, development, management, maintenance, testing, security, implementation, maintenance and support services for computer systems, data processing and business processes
q) Training, consulting and evaluation services to improve human skills, quality assurance and processes of the IT industry companies
r) Business processes management services based on information technologies that include, among others, call centers, contact centers, payroll management, portfolios, collection, production lines, etc.
s) Embedded software development
t) Interactive means based on information technologies:
   I. Development or creation of interactive entertainment
   II. Design specialized services
   III. Animation
   IV. Digital compression technologies
   V. Visual effects
   VI. Interactive television, and
u) Any other technology determined by the Board of Directors.

Based on the economic activities listed in the 2011 Rules of Operation of PROSOFT 2.0, a universe of 12,200 companies was considered to determine the sample that would represent such industry in order to carry out an online survey.

The probability random sample design considered a basic sample of 530 companies surveyed around the Mexican Republic that, thanks to the participation, allowed this number to increase to 564 companies. The reliability level of this online survey was 95%.

I.2 Questionnaire for the Survey.- 22 questions were prepared for the survey divided into five main sections:

Introduction.- This section briefly describes the program that the Federal Government, through the Ministry of Economy, fosters to promote the growth of the IT services industry. The main objects of the program are to strengthen the institutions and to improve the regulatory legal framework and the sector policies. Moreover, this section was used to present and/or reinforce among the participating companies the contents of the LFPDPPP in relation to the treatment of personal data as well as the role of the data processor.

Classification.- This section groups the different companies in the industry that offer IT services for which the application of the LFPDPPP is relevant, according to their nature of the operation, mission, vision and values. On one hand, a classification of the participating staff was made to guarantee that the point of view about the problems takes into consideration the implications of the business and the technological environment. Moreover, the number of employees of the companies and their annual sales were identified. On the other hand, it was sought to find the existence of companies in Mexico that offer outsourcing services for the treatment of personal data. A company with this profile may cover the characteristics and requirements of the data processor role.

Information Security and Privacy Organization Practices.- With this group of questions, it was sought to determine the type of practices of management and operation related to information security and privacy of the companies that together with their operation nature may help determine the opportunity areas in themselves when complying with the LFPDPPP.

Information Security and Privacy Management covering the main topics of the processes, roles and responsibilities, as well as the security of the information assets.- The main object of this section is to determine the way in which the organizations have assigned information security responsibilities, as well as the technical, operation and process control mechanisms to achieve the level of security and privacy required by the operation. Through these controls, it will be possible to identify the administrative, technical and physical security measures that the organizations have in place.

Data treatment in the so-called Cloud Computing.- This section tried to identify the control mechanisms that the organizations have implemented now to deliver and use services in a computer system of this kind. In this way, it may be determined whether the industry is prepared to comply with the LFPDPPP, keeping the level of privacy of the persons' information.

I.3 Performance of the Online Survey.- After the questionnaire was approved, on April 9, 2012, the electronic invitation was launched to 12,200 companies that were in the databases of the AMITI, the CANIETI, the AMIPCI and the surveying company.

The original period considered was four weeks, i.e., from April 9 to May 4, 2012. However, in order to get the sample that would represent the companies subject matter of this survey, such period was extended, so the online survey was opened from April 9 to May 31, that is, approximately eight weeks.

The electronic invitation was opened by 4,373 companies, out of which 1,385 participated and only 564 answered the survey.

I.4 Analysis of the information obtained from the Survey.- In regard to the economic activities that integrate the IT industry, it was found that less than 5% of the surveyed companies provide some kind of outsourcing.

As to the company size, it was observed that about 80% of the surveyed companies are within the micro and small company classification.

Now, regarding personal data processing, storage or safeguard – internal or of the clients -, the following ranges were obtained:

- From 41% to 45% of the companies evaluated process personal data.
- From 30% to 31% store personal data.
- Only 25% safeguards this kind of data.

Organizational information privacy and security practices.- It is relevant to mention that 26% of the surveyed companies do not know which regulations and/or reference frameworks are used to implement information security. Only 39% mentioned the Federal Law on Protection of Personal Data Held by Private Parties as a regulation mechanism.

Type, Existence and Practice of Security Measures.- 27% of the companies have a central policy and auxiliary standards on information security; 22% consider human resources security as the most relevant topic; 15% use the compliance control objectives; and 11% consider the management of information security incidents as the most important issue.

55% of the surveyed companies does not have a Security Committee that supervises the compliance, monitoring and improvement of the policies in place.

36% of the companies have not defined any contract agreements or clauses with their clients or suppliers about the responsibility of processing and exchanging information and personal data.

35% of the companies do not have in place formal indicators of the effectiveness of information security evaluation. Now, those companies that have such mechanisms prepare incident reports, IT general control evaluations, technical vulnerability solution reports and/or classification of the events identified by the infrastructure.

Information identification and classification.- In this activity, only 29% of the surveyed companies identifies and classifies information as a component of its security standard framework. Besides, 29% said that the area responsible for defining and managing the information classification criteria is the General Management; 26% said that the responsible for such classification is the security department; and only 8% of the companies assigns such activity to the personal data area.

It is important to mention that in 27% of the cases, there are no formal classification criteria.

Awareness, education and training of the personnel on personal data protection.- The results of this survey show that 33% create awareness in their staff through e-mails, brochures, printed means, etc.

53% said that education and training activities are carried out at least once a year in their organizations. However, it is important to mention that 35% of the companies do not remember when they have had their last training on information security and privacy.

Physical security measures.- The physical security measures have been defined by the companies according to their control goals:

- Physical and facilities security (25%)

- Information assets inventory (17%) or asset management

Technical security measures.- The surveyed companies have defined the technical security measures within the following control goals:

- Computer operations (22%)
- Logical access control (20%)
- Application development security (16%)
- Telecommunications operation (13%)

Problems in the implementation of security measures to protect personal data.- For the companies of the IT services industry to achieve the adoption of personal data privacy mechanisms in their information security systems – that comply with the LFPDPPP, adding value to their business processes – the following root causes of the gaps and shortcomings observed in the results of the survey must be solved:

- 80% of the IT companies are classified as micro and small companies; consequently, they have not achieved the capacity to implement the security measures to protect personal data. This lack is due mainly to scarcity of economic and human resources.

- The information security function has been conceived and assigned permanently to a technological context developed through isolated or specific assurance efforts, based on specific security tools. In many of these cases, the main assumption is to meet any auditing or evaluation requirements, or to solve the specific problems.

- A lack of experience in the IT services industry is recognized for the assimilation of the privacy regulations on the information security scope, as well as to recognize the responsibilities of each actor described in the LFPDPPP and its Regulation.

- The protection approach that has been developed is based on the technological infrastructure, and not on the sensitivity, critical condition or significance of information for the business, and even less from the standpoint of personal data protection.

- Limited budgets and resources are assigned to implementing the initiatives on information security and personal data privacy. This lack is due to a certain competition with other priorities of the organizations. Priorities that are derived frequently from the budget assigned to the IT function. Hence, the security and privacy alternatives cannot be developed due to the organizational requirements.

- Resource restrictions have resulted in the majority of the surveyed organizations not performing basic controls regarding security, e.g., risk analysis, security strategy, training and awareness strategy on security and privacy, security incident management or ongoing improvement of information security.

- Solving these root causes does not come from only one or limited solution, but from a permanent process of the organization to incorporate the issues of security, privacy and compliance with the LFPDPPP and its Regulation as part of an organizational culture.

Treatment of Personal data in the so-called Cloud Computing.- The survey found that 53% of the companies offer or use cloud computing services.

The aspects of the Regulation related to the companies that offer cloud computing services were reviewed. It was found that the majority of the

providers do not know or fulfill the aspects and mechanisms that the Regulation sets forth to guarantee the due protection of personal data.

General Conclusions from the Survey.- Based on the answers of the surveyed companies on information and personal data security, it is possible to reach the following conclusions:

- The percentage of the participation of micro and small companies may indicate that there is true concern about the security and privacy scopes and requirements in the industry in regard to the efforts to be developed in order to comply with such concepts.
- In the case of the participation of micro companies, due to their income level, it is important not to restrict the budget to implement control mechanisms to help them comply with the Law. The personal data privacy and security commitment does not depend on the size of the business, but on the type and sensitivity of the information managed in their processes.
- The personal data treatment outsourced services are identified as a business opportunity area for the IT industries companies in Mexico, as only 31% of such companies offer those services.
- Although the companies understand fairly some of the key components to comply with the LFPDPPP, they are not being carried out at present.
- The surveyed companies perceive the topic of personal data security as an issue to be solved by an information technology (IT) area.
- The organizations have worked on the implementation of preventive technical controls and controls to detect security gaps, but not within a context of personal data privacy.
- The implementation of the current controls is based mainly on the experience of the persons in charge of the IT area.
- The majority of the budgets for security and privacy initiative efforts derive from the IT budgets.
- The effectiveness of the security and privacy functions is not monitored, evaluated and supervised in any way whatsoever.

- From some of the opinions of the survey participants, it is possible to identify that the companies consider that this kind of regulations only apply to large companies.
- At present, the companies do not have an incident response team or a control log of the activities of the processing, applications, information and personal data infrastructure, that allow them to have a formal control of such activities. For this, it would be complicated to provide evidence in a legal action related to security breaches and damages to personal data.
- Taking into consideration the nature of their services and their operation inertia, the cloud computing sector must carry out efforts to review their adhesion contracts regarding the characteristics of service delivery and their operation systems, in such a way that they adapt to the requirements the Regulation of the LFPDPPP sets forth in Article 52.
- It is important to mention that the companies that do not recognize the usefulness of Risk Analysis base their information security policies on specific remedial efforts of deviations or the subjective decisions of the persons in charge of such functions.
- Article 20 of the LFPDPPP and Articles 63 to 66 of its Regulation, recognize as a priority the management of information security incidents. Consequently, another opportunity area to achieve the compliance with the LFPDPPP is the low percentage of organizations that have worked on their management of information security incidents.
- Training on information security and privacy represents one of the most relevant efforts to be made by the IT services industry. For this, the organizational nature of personal data privacy in the Regulation of the Law includes active training of the personnel of the organization that treats with personal data.

II. IDENTIFICATION OF BEST PRACTICES

The object of the second report of this Study was to "Identify the best practices of personal data security and the requirements of the regulatory framework contained in the LFPDPPP".

The best practices and standards analyzed were the following:

CMMI (Capability Maturity Model Integration)

- Set of best practices that provide the elements to have effective processes that help improve the efficiency, effectiveness and quality within the work groups, projects and divisions. In other words, it contributes to the improvement of all the areas of an organization.
- Information security may be conceived within the CMMI model of development and services as a type of requirement. However, the SSE-CMM (System Security Engineering Capability Maturity Model) establishes it specifically in its 11 areas of security engineering processes.

CobiT (Control Objectives for Information and Related Technology)

- Set of practices to improve information management both in the financial and technological areas. It is a reference framework to set a safe and reliable roadmap for information technologies, as well as a tool that supports top management to reduce the gap between the control needs, the technical issues and the particular risks of businesses.
- Within the benefits of CobiT, it was found that the security and privacy requirements will be identified more easily and their implementation may be monitored through the dominions established in CobiT: Planning and Organizing (PO), Acquiring and Implementing (AI), Delivery and Support (DS), and Monitor and Evaluate (ME).

ISO 27001

- It is the international information security management standard that allows an organization to evaluate its risk and implement appropriate controls to preserve information confidentiality, integrity, and availability at an adequate level.

- Its Exhibit A summarizes the control objectives and controls the ISO 27002:2005 developed in order to be chosen by the organizations for the development of their Information Security Management Systems (ISMS).

- In the ISO 27000 series, the ISO/IEC 27017 is in the development stage. It will consist of a security guideline for Cloud Computing, and the ISO/IEC 2703 that will consist of a guideline on Cyber-security.

- Taking into consideration that the ISO/IEC 27001 is the information security international standard, we will find the personal data protection applicability criteria in all the dominions. It is important to mention that in Dominion A.15 Compliance, Object of Control "compliance with the legal requirements" we found, specifically, control 15.1.4 related to data protection and personal data privacy.

- The ISO/IEC 27001 is the certifiable information security standard. For this, the IT companies that wish to be considered reliable suppliers must take it into account for their information security strategy.

- The ISO/IEC 27005:2011 is an essential standard for those who need to manage their risks effectively and, in particular, to comply with the security information management through standard ISO/IEC 27001.

ITIL (Information Technology Infrastructure Library)

- Set of guidelines (best practices) and modules through which it can be established a better use of the information resources of an entity or organization from the point of view of services. ITIL has set the road of "how" to derive more benefits from the information technologies.
- Considering that the ITIL covers the IT services in all their stages, the 5 books that integrate it contain useful procedures applicable to information protection.

NIST (National Institute of Standards and Technology)

- Its mission is to promote industrial innovation and competition in the United States of America.
- The NIST laboratories are focused on three areas: measurement science, technology (information technologies, engineering) and facilities of domestic users.
- The publications on information security and information technology are the specials ones of the 800 series.
- Within the 800 series, the most relevant ones on the topic of security and personal data are:

Issue Number (Date)	Title	Content
NIST SP 800-12 (October 1995)	An Introduction to Computer Security: The NIST Handbook	It is focused on security controls according to their nature, i.e., it establishes a classification of such controls (administrative, operation and technical controls).
NIST SP 800-14	Generally Accepted Principles and Practices	Description of 8 security principles and 14 security

Issue Number (Date)	Title	Content
(September 1996)	for Securing Information Technology Systems	practices.
NIST SP 800-39 (March 2011)	Managing Information Security Risk	It provides the organizations with a guideline on information security risk management establishing its components (risk identification, evaluation, response to and monitoring).
NIST SP 800-122 (April 2010)	Guide to Protecting the Confidentiality of Personally Identifiable Information	It suggests categorizing the level of impact of Personal Identifiable Information (PII) in low, moderate and high, and based on the potential damage that may be caused to the owners of the information and/or the organization if it were violated, used or disclosed improperly. Additionally, it provides that the PII must be protected through a combination of measures, including operation safeguards, specific privacy safeguards and security controls.
NIST SP 800-144 (December 2011)	Guidelines on Security and Privacy in Public Cloud Computing	It offers a general overview of the public cloud computing services and their security and privacy challenges. It also describes the usage models (public cloud, private cloud, community cloud and hybrid

Issue Number (Date)	Title	Content
		clouds) and gives recommendations on security and privacy and the activities to be performed when contracting outsourced cloud computing services.

PCI/DSS (Payment Card Industry Data Security Standard)

- International standard that sets information security requirements to protect the cardholders' data.
- The companies that process, keep or transmit the cardholders' data must meet the standard. If they do not, they may lose their operation permits (franchise loss).
- The information provided by the cardholders to manage the credit and debit cards is personal (identification, financial and property data). For this reason, each one of the control objectives and requirements of this standard apply to personal data protection.

Spain

- The Agencia Española de Protección de Datos (AEPD, Spanish Information Protection Agency) is the institution in charge of taking care and fostering the privacy and protection of personal data in Spain. The Iberian Peninsula belongs to the European Union, thus, it must abide by its criteria in general.

- The AEPD is a public legal entity with its own legal capacity and full public and private authority according to Royal Decree 428/1993 dated March 26, 1993.

- Article 9 of Organic Law 15/1999 (LOPD in Spanish) dated December 13, 1999, sets forth that both the data collector and the data processor must adopt technical and organizational measures to guarantee the security of the personal data to avoid its modification, loss, or non-authorized treatment or access.

- The Regulation of the LOPD sets forth that the security measures required from the databases and their treatment must be classified in three levels: basic, intermediate and high.

- The AEPD has issued a document called "Guía de Seguridad de Datos" (Data Security Guideline) which covers several best practices on personal data protection.

- The classification of the security levels is made according to the nature of the treated information and the need to guarantee the confidentiality and integrity of information.

- The security measures are accruable.

- The Guideline contains a security document whose content is structured as follows:

    - Application field of the document,

    - Measures, standards, procedures, rules and standards to guarantee the required security levels,

    - Information and the staff's obligations,

    - Incident reporting, management and response procedures, and

    - Review procedures.

- The Regulation of the LOPD sets forth in articles 96 and 110 that from the intermediate level of security required, the databases must be subject to an internal or external audit at least every two years. The audit will result in a report that will be delivered to the person responsible for the database and be available to the inspection of the AEPD or the control authorities of the autonomous entities.

- The Asociación Española de Normalización y Certificación (AENOR, Spanish Standardization and Certification Association), has published among other standards related to information security, the following:

    - Since November 28, 2007: ISO/IEC 27001 as UNE-ISO/IEC 27001: 2007

    - Since December 2009: ISO/IEC 27002 as UNE-ISO/IEC 27002: 2009

United Kingdom

- The United Kingdom, through the Data Protection Act 1998, sets forth that -when there is a data processor to treat personal data-, a data processor that provides sufficient guaranties about its security measures to protect the processing that will perform on behalf of the data controller must be chosen. It must be reviewed that those security measures are being applied and there must be a written contract that sets forth the data processor's obligations. There is a model contract published by the European Standardization Committee.

- The Information Commissioner Office (ICO) is an independent authority in the United Kingdom that was created to defend the rights of public interest information, and to promote the opening of public entities and the privacy of the information of individuals.

- In relation to security measures, the DPA has established the following: "Principle 7: Proper technical and organizational measures must be taken against the unauthorized or illegal processing of personal data, as well as against accidental loss, destruction or damage of personal data.

- It is suggested to design a security organizational model, according to the type of personal data they possess and according also to the information security breach contingencies.

- The ICO has designed good practices notes and codes, shown below:

    - Data Protection Good Practice Note Security of Personal Information

    - Data Protection Good Practice Note (List of training for small and medium-sized companies)

    - Data Sharing Code of Practice

    - Personal information online code of practice

    - Cloud computing

- The ISF (Information Security Forum) researches, clarifies and solves key issues about information security and risk management through the development of good practices.

- The 2011 Good Practices Standard covers the corporate perspective on information security and it is divided in four main categories:

    - Security governance

    - Security requirements

    - Control framework

    - Security monitoring and improvement

The United States of America

- In the field of personal data protection in possession of private parties, the United States of America has regulations on privacy and security measures mandatory for the data controllers and data processors of personal data, both at industry and state levels.

- At federal level:

    - The 1974 Privacy Act sets forth a code of fair practices that regulate the collection, maintenance, use and disclosure of the information of individuals in the recording systems of the federal agencies of the United States.

    - The United States Code (USC) is the coding by topics of the general and permanent acts of the United States of America and it is divided in comprehensive topics divided in 50 titles. It is published by the Legislative Review Office of the House of Representatives of the United States.

    - Under title 15 "Commerce and Business", Chapter 24 of the USC, we find the topic of personal information privacy. It discusses the disclosure of private personal information and fraudulent access to financial information.

    - Section 1173(d) of the Health Insurance Portability and Accountability Act of 1996 "Security Standards for Health Information" sets forth that the Department of Health and Human Services shall adopt security standards that take into consideration the technical capacity of the registration systems used to keep health information; the costs of security measures; the need to train people who have access to health information; the value of audit tracking in computerized recording systems;

and the needs and capacities of small health care providers and health care rural providers.

- At state level:
    - The state of Massachusetts has a regulation called 201 CMR 17.00: Standards for the Protection of Personal Information of the Commonwealth Residents.
    - The objects of the above mentioned instrument are: to guarantee the security and confidentiality of client information according to the standards of the industry in question; to protect information against foreseen threats or risks; and to protect against non-authorized access to or use of information that may result in damage or discomfort to any consumer.
    - In the Nevada Revised Statutes (NRS), Chapter 603A deals specifically with personal information security. The "Regulation of Business Practice" in articles NRS 603A.200 and NRS 603A.210 establishes the destruction of certain records and security measures, respectively.
    - Article NRS 603A.215 sets forth that the responsible parties that accept payment cards must comply with the current version of standard PCI/DSS. In case the responsible party does not carry out this practice, he has the obligation not to transfer personal information by electronic transmission or no-voice transmission other than facsimile machine unless the information is encrypted[1] in order to guarantee the security of the electronic transmission.

[1] Encryption means "the protection of data in electronic or optic form, in storage or in transit, using an encryption technology that has been adopted by an established standards setting body including, but not limited to, the Federal Information Processing Standards issued by the NIST, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data." NRS 603A.215, http://www.leg.state.nv.us/nrs/nrs-603a.html, revised on February 21, 2012, , 20:00 hrs.

- It is important to mention that other states such as California, Hawaii, Illinois and Vermont have laws on the subject of privacy.

- There are several government and private organizations that publish models, best practices and standards on information security in the United States, such as the Carnegie Mellon University (Software Engineering Institute), CMMI, ISACA, CobiT or NIST.

III. RECOMMENDATIONS AND CORRECTIVE ACTIONS

The fifth and last Deliverable focused on the preparation of "… recommendations and corrective actions for an effective practice of security measures for the protection of personal data in the information technologies industry to comply with the LFPDPPP".

III.1 Recommendations.- To ease the adoption of control mechanisms that each organization will require from its specific analysis, as well as its operation characteristics to meet the requirements of the LFPDPPP that were proposed under the section "Reference practical framework of control mechanisms for information security and privacy management", it is important to take into account the following additional recommendations:

- The effort to estimate the acceptable risk level and the combination of security and privacy controls in the organization may be based on the document references of the experience of other countries with similar regulations and which have been included in this research. The use of these references does not imply copying or adapting the elements that have been developed, rather, it is necessary to favor the creation of alternatives adequate to the operation reality of the organization.

- The IT industry companies must work to redefine their services for final customers, taking into consideration the operation and technological implementation mechanisms within which their IT services are created,

and the service legal and quality elements agreed upon with the suppliers and customers. All this in such a way that the operation model meets these requirements naturally, and the information security and data privacy become natural characteristics of each service offered. This recommendation implies the change of the current infrastructure management approach to an integral approach of information services management.

Moreover, it is recommended that within the commercial areas of the company, all things related to the data processor are defined according to the LFPDPPP including, but not limited to, the following:

- Object
- Technical activities to be performed
- Benefits
- Requirements

- A positive way to drive the efforts to increase information security and privacy is that the organization enforces its control initiatives within an industry reference framework that may be evaluated independently (certification), and a reasonable guarantee of the effectiveness of security management is attained considering the privacy requirements of the interested parties.

- To support the monitoring and evaluation activities related to the effectiveness of the security function within the risk and privacy parameters, it is recommended that the organizations can implement a self-regulation mechanism from a compliance point of view independent from the infrastructure and security operations, that facilitates supervision and ongoing improvement in a short term and, at the same time, enables preparing the security and privacy framework for an

external review that determines the compliance with the LFPDPPP in the natural maturity of the regulation.

III.2 Corrective Actions.- As recommendations regarding the corrective actions for an effective practice of security measures regarding personal data protection in the IT industry to comply with the LFPDPPP, the most significant corrective actions are listed below:

Information Security and Privacy Organizational Practices

General Status	Corrective Actions
• The companies of the IT industry acknowledge certain mechanisms as the basis to make decisions on the level of information security and data privacy, such as: risk analysis, compliance with auditing exercises, supplier recommendations, vulnerability technical analyses, etc. However, their application is not formalized or is recognized as an organizational component with a multi-discipline participation. • In this sense, the organizations have begun to implement information security mechanisms based on regulations and specific requirements.	• Security and Privacy Risk Analysis and Evaluation must be established as a formally defined process within the organizational practices to adjust the business operation and the quality of services to clients based on identifying the priorities of protection with a strict sense of business. • Upon identifying the protection and privacy priorities, the organizations must assign specific budget lines to develop the security and privacy projects as part as a budget planning strategic exercise that corresponds to the level of participation of all the areas of the organization in the use of these controls in their processes.

General Status	Corrective Actions
• For this reason, the budget allotments are limited and there are only, to a large extent, allotments for specific isolated projects. • The performance of these security and privacy controls projects are made as part of the responsibilities of the Systems / Informatics / IT functions of the business, without including an integral approach and performance. • The organizations identify the general areas of control to be considered to develop specific protection and privacy mechanisms; however, not all have been implemented.	• The organizations must extend the roles and responsibilities of security and privacy to all the areas and functions of their structures to be recorded and performed formally. • A security and privacy strategy procedure must be defined to take advantage of the results of the risk analysis and evaluation, for making decisions on the control issues to be developed in the organization based on the priority, feasibility and benefits of such controls.
Information security and privacy management **"Processes, roles and responsibilities"**	
• It was found that there is an Information Security Committee that supervises the activities of assurance of and compliance with the privacy of information	• The organizations must establish formally (as part of the effort of assigning roles and responsibilities) a multi-discipline group that has responsibilities about determining the

General Status	Corrective Actions
within the organization. • Moreover, the participation of strategic roles has increased in the classification of information (protection type and priority). • The organizations have not made ongoing efforts regarding personnel training on information security and privacy topics. • Likewise, no systems have been developed to measure the effectiveness of the security and privacy function. For this, there are only operation metrics or occasional technical evaluations. • The implications of the privacy requirements have not been taken into account in the agreements with suppliers, business partners or customers.	acceptable risk level, the definition of the security strategy, the measurement of the security effectiveness and the direct operation of controls. • The organizations must include the commercial, operation and legal areas in the definition of security and privacy roles and responsibilities, with the specific assignment of the determination of legal agreements and terms, service levels and deviations related to breaches of security and incidents with suppliers, business partners and customers. • In the first effort of control mechanisms, the organizations must define and perform an integral strategy of awareness about information security and privacy, within the corporate parameters of institutional communication. • As part of the controls related to the incident and breach management, effectiveness measurement components of the security function must be derived, considering actively the acceptable level of risk, and the

General Status	Corrective Actions
	level of security that prevails in the organization, based on measuring the risk components and the management of security breaches.
Information security and privacy management **"Security of the Information Assets"**	
• To a large extent, the IT industry companies are responsible for their own facilities where the technological infrastructure to process information is located. • The protection approach has been focused on securing the infrastructure and not on the type of information processed by the organization. • It was found that there is a considerable advance in the protection mechanisms related to the networks of telecommunications, platforms and final user equipment. • The current security control efforts have not been developed	• Perform a detailed review of the characteristics of the computer facilities to make sure that they comply with the industry requirements (according to applicable standards). • Or, request the supplier of the computer equipment that it delivers periodical results of any reviews or evaluations of such equipment. • Develop an information security and privacy strategy based on preventive, detection and corrective controls whose implementation takes into account policies, procedures and technical mechanisms that aid to the compliance with the LFPDPPP, and help reaching the operation level required by the organization (the specifications recommended for these

General Status	Corrective Actions
with privacy requirements. • The assumption of the selection and characteristics of the security control mechanisms is the subjectivity / experience of the personnel responsible for the security function in the organization. • There are initial efforts about preventive security monitoring based on the generation, preservation and exploitation, and for this, they do not contribute to generating effectiveness metrics of the security function.	controls can be found in the "Practical Reference Framework of Information Security and Privacy Management Control Mechanisms"). • Develop a component to measure the effectiveness of the information security function. First, it may take into account the self-regulation capacities and gradually reviews by third parties.
Information Treatment in Cloud Computing	
• The organizations that offer or consume cloud computing services consider their implications within their own security and privacy standards framework. • However, the suppliers of cloud computing services do not know fully the implications of the	• Develop an information security and privacy strategy based on preventive, detection and corrective controls, whose implementation takes into account policies, procedures and technical mechanisms that help the compliance with the LFPDPPP and help them reach the operation level required by the organization (the

General Status	Corrective Actions
privacy regulation on the management of their services from the operation, service level and legal point of view in case of a breach or deviation from contract provisions.	specifications recommended for these controls can be found in "Practical Reference Framework of Information Security and Privacy Management Control Mechanisms"). • The organizations must include the commercial, operation and legal areas in the definition of security and privacy roles and responsibilities, with the specific assignment of the determination of legal agreements and terms, service levels and deviations related to breaches of security and incidents with suppliers, business partners and customers.

III.3 Public Policy.- The activity f) of the title Work Methodology of item 5 (Technical Specifications) of the Reference Terms was added the provision of paragraph c) of item 4 (Scope of the study, counseling or research): "c).- The recommendations and corrective actions must take into consideration actions of the public policy, as well as of the company".

In this respect, such report 5 puts in context the legal and scheduling framework required to establish a special public policy on the topic of security regarding the IT industry companies that deal with personal data as "data processors" according to the LFPDPPP. Although it is true that in this regard the 2007-2012 Economy Sector Program is not specific, its objectives work as a framework to promote mechanisms or measures to increase the competitiveness of the companies by fostering the use of the IT in the subject.

It is understood that this Program did not determine comprehensive action lines for the economy in general, or for the digital theme in particular, as it was issued in May 2008. Mexico did not have then the Federal Law on Protection of Personal data held by Private Parties, enacted in 2010.

As **public policy** or specific scheduling scheme, to be guided by the public power, the following objects with their respective lines of action were proposed in this project:

General Object.- To drive the knowledge of good domestic and international practices regarding data security for the IT industry.

Object 1. To generalize the use of good practices of personal data security in the IT industry, to be able to offer certainty to the companies and individuals that subcontract them as data processors according to the LFPDPPP.

Object 2. To develop skills on domestic and international practices on data security for individuals or companies related to the IT industry that operate as data processors to manage personal data held by private parties.

Object 3. To promote recommendations and corrective actions for an effective practice of security measures to protect personal data in the IT companies by individuals or companies that operate as data processors in treating personal data held by private parties.

It is important to mention that the success of the Public Policies promoted to drive the knowledge of good domestic and international practices on personal data security for the IT industry, with the above objects and their respective action lines, lies on the existence of the human, organizational and material infrastructure, financial resources, and especially, that the target entities, in this case the private parties that work as data processors in the treatment of personal data, have the proper incentives to become aligned under the standards, good practices, and mainly, the institutional expectations of the industry and of the owners of such information.

For that purpose, the government agencies must consider within their own annual expense budget, lines to promote within their sector of influence according to the Organic Law of the Federal Public Administration, the use of good practices on personal data security in the IT industry to be able to offer certainty to the companies and individuals that subcontract them as data processors as set forth in the LFPDPPP, together with the IFAIPD; as well as to establish an administrative unit that attends the issues of protection of personal data held by private parties from the sector point of view.

As **policy instruments**, the following have been recommended: a National Information System on norms, standards and good practices on personal data security in the IT industry, whose object will be to guide and inform the companies and individuals that subcontract data processor treatment services as set forth in the LFPDPPP. And a National Inventory of IT companies within the Sistema de Información Empresarial Mexicano (SIEM, Mexican Company Information System).

And finally, on the topic of **institutional parties responsible for enforcing this public policy**, it was underlined that according to the Mexican law on federal public administration, there are 19 public institutions (Ministries, the General Attorney's Office and the Legal Counseling Department), with the participation of the IFAIPD, that cover the field of regulations on privacy. Thus, these 20 entities must be considered as the parties responsible for guiding harmoniously the applicable Public Policy.

PROJECT PREPARED FOR THE CÁMARA NACIONAL DE LA INDUSTRIA ELECTRÓNICA, DE TELECOMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN (CANIETI, MEXICAN CHAMBER OF THE ELECTRONIC, TELECOMMUNICATIONS AND INFORMATION TECHNOLOGIES INDUSTRY)

BY PIVOTAL SERVICIOS, S. DE R.L. DE C.V.

www.pivotalmexico.com

flor.hernandez@pivotalmexico.com

2011-2012