



EXECUTIVE SUMMARY



TABLE OF CONTENTS

Objectives of the Study.....	2
Study Methodology.....	2
Universe.....	3
Determination of sample size.....	3
Statistical reference frame.....	3
Main Results	4
Profile of the respondent	4
Types of data handled by the Company.....	5
Figures and procedures defined within the Company	5
Security measures.....	6
Privacy Notice	7
Quality Principle	8
Purpose Principle	8
Principle of Loyalty	9
Principle of Responsibility	9
Service provider (data treat collected for the company).....	9
Processing of Personal Data in the Cloud	9
Recommendations for Business and Administration	10
1.-Raise awareness in the Mexican Population rights conferred by the LFPDPPP and more effort to create awareness of the obligations imposed on private sector companies.	10
2.-Implementation LFPDPPP private sector where he focused the study (SME's)	12
3.-Professional security (consulting)	14
Conclusions.....	15
Analysis of the institution's Strengths, Weaknesses, Opportunities and Threats (SWOT). 17	

Objectives of the Study

Identify the level of culture and current practices on Protection and Processing of Personal Data in Private sector companies. With particular focus on IT Companies.

Under the following objectives:

To measure the level of understanding and compliance LFPDPPP.

Identify the procedures implemented within the Company in terms of protection of personal data based on the statement of the LFPDPPP, considering technical, organizational, operational and legal terms.

Study Methodology

To achieve the objectives of the study, to analyzed sources of information regarding to the Protection of Personal Data.

We conducted a thorough investigation about the path of personal data privacy in those countries that already have a law on protection of personal data. In this way, were reviewed specialized laws about IT area and were taken expert opinions / Privacy professionals.

Surveys were focused at private sector companies for determine the level of culture, that them have.

The surveys were conducted in 10 minutes by the following via:

- Electronic questionnaire by internet
- By telephone interview

Information Gathering:

September to October, 2012

Universe

The universe was taken on based on 3,237 Mexican companies of Private sector, related to the sector of information technology nationwide. (According to INEGI Economic Census 2009). Also have been considered other Business sectors in the survey, with the purpose to get a better level of significance

Determination of sample size

The selection method is statistical sample, determining the size thereof by the formula corresponding to a finite population, which has been estimated margin of error of + / - 5% for a confidence level of 95%.

Universe or sampling units = 3,237

Tolerable error = 5%

Confidence level = 95%

Expected error = 10%

Size of the Sample = 191

Distribution of the Size of Sample

The segmentation was performed the following way by Federal Entities, Sector, Sales amount or incomes, business activity and number of employees; with the purpose of identify the business size and location of itself.

Statistical reference frame

The study was conducted through descriptive statistics that deals with the design of sampling plans, procedures to summarize data, draw graphs and compute measures that help to describe some findings derived from a data set

Objects were drawn from the quantitative analysis, supplemented with qualitative analysis.

Main Results

Profile of the respondent

Participation of respondents by State is as following:

- 52% was participation by Business City
- 48% was participation the other states.

The business sector with more participation was:

- Servicios with a 52%,

The rest of the business sector was:

- Trade Sector 34%
- Industry Sector 14%

According to the positions held by respondents are the highest percentages are:

- The 26% holds the position of General
- A 20% belongs to analysts.

Depending on the size of the companies surveyed the most part in the survey was:

- Microenterprises with 66% of participation , which generates less than \$ 4 million dollars annually to the value of his sales

The business activity, with highest participation in the survey was:

- The IT sector with 24%, also Other services provided by the same percentage, however the latter encompasses multiple services, not specified in the survey, therefore can't be considered of the same magnitude the IT

Types of data handled by the Company

According to the classification of the Types of data established in the Act, The data that most companies handle are:

- Basic Data , Financial and Property Data is a 65%

By size of company that has greater data handling are:

- Microenterprises with 37.95% between Basic data, Financial and Property.

As for storage of data:

- The 53% of the business have data stored in paper.
- The 45% of the business have data stored in electronic means

Figures and procedures defined within the Company

Surveyed Company.-

- 69% have some figure or procedure defined.
- A 31% do not have any figure or procedure defined.

The main reasons that 31% do not have any figure or procedure defined is:

- Ignorance of the Law and its Regulations with a 27.1%.

The business activity with more figures or procedures defined in accordance with the requirements of Law is:

- IT with a 24.17% compliance

Security measures

Of the companies surveyed than have a responsible for developing security measures for the protection of data.-

- The 54% have a Responsible either internal staff or external to the company.
- The 46% has not a Responsible

The most important factors to consider companies to develop security measures are:

- risks inherent by personal data type
 - 20% Responsible
 - 17% External Moral Person
 - 23% Internal Person
- Technological development
 - 19% Responsible
 - 27% External personal of company
 - 7% Internal Person

The main actions considers the responsible for security measures are.-

Develop an inventory of personal data and Treatment Systems

- 29% Responsible
- 24% External Person of the company
- 25% Internal Person

Determine the roles and responsibilities of persons processing personal data.

- 25% Responsible
- 18% External Person of the company
- 25% Internal Person

The Responsible has a procedure for notifying Vulnerabilities

- 51% If you have
- 49% No account with that procedure.

As for the type of consent for treating personal data

- Collects 80% tacit consent for all data types (Basic Data , Financial and Property , Data sensitive)

Privacy Notice

Of the participating companies:

- The 27% has with Privacy Notice
- The 73% do not have Privacy Notice

Based on the above, the following results are derived from 27% claiming to have a Privacy Notice.

As for business activity, companies that meet Privacy Notice are:

- 11.76% the Technology Information meet the privacy notice
- Consultant at Legal and Business meet a 3.17%

Privacy Notice type showing Companies at the time of data collection:

- The 47% Unveils the Privacy Notice (subject to the Act)
- The 53% Unveils the Privacy Notice incomplete (missing elements)

The media most used by companies to publicize your Notice of Privacy are:

- The 28% Unveils Privacy Notice visually
- The 25% for a digital medium

Quality Principle

Companies that adopt mechanisms to ensure the Principle of Data Quality:

- 53% The data conform to data they provide the owner and are only updated at the request of the same
- 45% obtained objective evidence (Official Documentation)
- The remaining 2% used other mechanisms

Purpose Principle

The following results are for 27% of companies claiming to have Privacy Policy.

Companies that clearly mentioned on your Notice of Privacy the Purpose for which the information collected:

- 87% mentioning the purpose the treat of data in your Notice of Privacy
- 3% says no mention the purpose treat of data in your Notice of Privacy

The Companies that says to mention in your Notice of Privacy that data is treating for the Advertising, Marketing and / or Commercial purposes are:

1. The 21% is clearly indicated in its Notice of Privacy
2. The 6% does not indicate the end of Advertising, Marketing and / Commercial
3. The 6% not treat data for the purpose of Advertising, Marketing and Sales Prospecting:
 - The 2% indicate in the Privacy Notice other purpose for which they seek to data
 - The 4% not indicate the purpose the collecting of data.

Principle of Loyalty

Mechanisms used by the companies surveyed to ensure the principle Loyalty:

- The 64% have Policies and control procedures for the security of personal data
- A 23% has staff trained on the Law
- The remaining 13% used other mechanisms

Principle of Responsibility

Of the companies that have a responsible person

- 60% of those responsible has security measures that mention in Article 48 of the Regulation to ensure the Principle of Responsibility
- The 40% do not apply any of the measures provided in Article 48 of Regulation

Most Maintainers who have implemented some of the measures to ensure the principle of Responsibility, states that its primary activity has been to develop policies and programs mandatory and enforceable privacy within the company

Service provider (data treat collected for the company)

Of the companies surveyed:

- a 33 % has providers who treat personal data collected for the company
- 67% do not have a providers who treat personal data collected for the company

Processing of Personal Data in the Cloud

Of the companies surveyed, those who have service in the Cloud

- 39% companies surveyed its service providers in the cloud has any of the requirements established in Article 54 of Regulation.
- 61% companies surveyed mentioned that your service provider in the cloud not meet any of the requirements established in Article 52 of the Regulation, for the treatment of data in the cloud.

Recommendations for Business and Administration

Considering the results of the study, we suggest the following recommendations for action, set in 3 axis impact attack aimed deficiencies facing the implementation of the LFPDPPP and Regulations on Private Sector Companies in Mexico.

1.-Raise awareness in the Mexican Population rights conferred by the LFPDPPP and creates greater awareness effort of the obligations imposed on private sector companies.

2.-Implementation LFPDPPP private sector where he focused the study (SME's)

3.-Security Professionals (Consulting)

Note: It is important to mention that the regulatory authority is the Secretaria de Economía and the Guarantor is the Instituto Federal de Acceso a la Información y Protección de Datos

1.-Raise awareness in the Mexican Population rights conferred by the LFPDPPP and more effort to create awareness of the obligations imposed on private sector companies.

According to the results of the study conducted, we found the biggest problems this is the ignorance and understanding of the law, although our study was applied only to private companies, clearly establish that the general public is unaware of this right under the Act (for protection of their personal data), and that is why Mexican society has not demanded their rights to the Companies, therefore the Companies have ignored these obligations, it has against holders that have data

The IFAI have publicity campaigns which force to Private Firms in the compliance the Privacy notices, but not have informational on how to meet, from which comes this new right of protection for personal data, which are sanctions, and most important a privacy notice; IFAI broadcast a single message "on notice no deceit" and all it establishes is a warning of the Act for breach of something not set or defined. Therefore, we Speculate that company not understand law, due to lack of information by the guarantor authority.

Recommendations:

We recommend a two-way action, first awareness among companies and on the other hand the awareness of the population and that through their knowledge, they themselves will be able to demand their rights against companies that collect your data, which represent immediate action by the Company to comply with the law.

For awareness among private company

We made it clear that not only the commercial broadcast media generate awareness of this Act, the IFAI has developed courses on its website and practical guides for at companies, which effectively help meet Act, stating that the information if it exists, what is needed is the spread it all private companies, to create an effective knowledge in companies to comply with their obligations under the Act

It is recommended improve the advertising content, the basic information must be more complete and needed for the companies to let them know of their obligations and sanctions that exist if do not comply with the law.

Improve campaign strategy on the mass media.

It is up to the authorities to determine the strategy to generate the impact, we only emit recommendations on the for missing information in the advertising.

For awareness of Population

We propose that IFAI campaign must be generate awareness for the people on the value of their personal data, showing the obligations of companies and rights that has the population, which is why it is recommended that the campaign will cover the follow points as measures to raise public awareness:

1. Knowledge of rights conferred by this Act
2. Explain to the Population what is it a personal data
3. Which value have personal data for companies
4. Educate the population on what is a Privacy Notice, your minimum requirements established by Law for the companies.
5. Educate the population on what are the Rights Arco
6. Knowledge of the Authority to which holders can go in the event that the Company does not guarantee their rights.

We emphasize that we only emit recommendations, authorities will be responsible of developing an effective campaign and generate than the necessary impact is sought.

2.-Implementation LFPDPPP private sector where he focused the study (SME's)

The SME's not considered that by not implementing the measures necessary to comply with the provisions of the Act could be subject to fines ranging from six thousand to 38 million pesos, representing a risk for business stay , non-compliance can be very costly to them and compromise their freedom.

Also have not Emphasized that regardless of the fines that may be subject, there are other hazards that may put the company in Situations: such as stealing sensitive information subject which may be due to lack of Security measures to data protection, the effect on the reputation of the company for not being subject to the law , loss of contracts with other companies for noncompliance, and distrust of their customers.

Recommendations:

Empowering Business by the Guarantor

the training have to be the spread the knowledge of this law among the companies. therefore We leave at the discretion of the guarantor authority the type of means to carry it out, either through internal campaigns within the companies, make deeper campaigns in the mass media (most complete), through more guides focused on issues not yet addressed etc.

We recommend the following topics for training:

1. Brief Overview of the LFPDPPP and Regulations
2. what is it a personal data ,how is classified, how is data collecting, type of consent obtained as provided by law
3. Profile to be met Responsible for data
4. Procedure for the Exercise of the Rights Arco
5. Minimum security measures to be applied for the treatment of the data
6. General guide and easy , procedures that must be met by all the Companies on the law the protection of personal data

7. Explain the difference between giving personal data and transfers.
8. The sanctions that will have the Companies by breach of law.

Within Companies

We must not forget the most important in the fulfillment of the Law and this Regulation is:

- Verify that the processes are functioning properly
- Implement training of staff on the protection of personal data

For this reason we recommend

1. **Raise awareness** in the staff on the importance and risk of handling of personal data in the work of each of those who work within the company and also outside as holders, in order to achieve a culture of protection of personal data and prevent for any inconvenience. We recommend establishing this culture of personal data protection as a general principle of the company.
2. **Provide training to the staff**, whether through courses, presentations etc. also give follow-up to training, through the elaboration of questionnaires, in order to determine the level of comprehension that has been captured in employees and focus on what was not understandable to correct it immediately.

3.-Professional security (consulting)

Aware that in Mexico the protection of personal data is a recent creation the law and Obligatory for the private companies, its implementation is immediate and necessary, companies seeking to adhere to the guidelines of the law seek to find consultants, professionals in the field to help them comply with the law.

The reality is that there are few professionals in the field; they are based on European models, since Europe has more than 20 years implementing this law.

There are the false Messiah: consulting without the minimum knowledge in the matter, have implemented the law in large institutions, but have done so incorrect and incomplete, exposing their poverty before the subject, and demonstrating that its implementation does not have livelihood, nor with the capability of supporting a true audit of data protection , which puts at risk the personal information of its customers and employees.

Recommendations:

We propose a certification by for the guarantor authority, for consultants who so wish, on the issue of privacy, training with qualified personnel in this field, either through agreements with countries that already have experience in this subject for example the European Union or OECD.

We propose certifications to ensure that consultants will do to a good job in companies that will require their services. The certifications have to be backed by certification of a competent authority such as IFAI.

Conclusions

Cannot be said, that all the companies are in a similar state of ignorance of the law; because our study spanned only 221 companies, and there is a wide range of circumstances between different companies surveyed; from which not have heard of the law and the companies that your know they exist.

Companies that even though they know that it exist the law, not aware of their obligation, not know how to apply the law, not aware the sanctions can face that in the event of non-compliance.

The situation of 221 companies surveyed, reflect a low level of culture that is has about the LFPDPPP and their Regulation (Two years ago the law came into force)

The vast majority of participants in the survey shows ignorance of the law, while those companies that if they have knowledge of the regulations and is implementing it, is being applied incorrectly

Companies currently don't value the importance and need to protect the personal data, being these the company's fixed assets, so it must be protected.

There is a reluctance to change by the Companies for the LFPDPPP adaptation, represents a change in the Organization of the information, which involves costs, personnel training, process adaptation.

In the case of companies that are implementing law in your organization this has implemented inadequately, the most significant reason would be their lack of knowledge on the subject of privacy; this is factor that hinders the fulfillment of the norm.

Therefore companies consider the implementation of the Act as an imposition and not as a value for the company

The Implementing of Law by the Companies will be beneficial for your own image, generating a competitive advantage.

Increase the intensity of the actions of dissemination, awareness, awareness, and the benefits that generates the implementation of the law to mitigate the low level of knowledge and application of the rules on data protection.

Generate support programs for micro and small enterprises, it will generate a greater commitment by enterprises, since many of them, does not have sufficient resources to implement the requirements of law.

Analysis of the institution's Strengths, Weaknesses, Opportunities and Threats (SWOT).

	STRENGTHS	WEAKNESSES
Internal Analysis	<ul style="list-style-type: none"> • Ensures Privacy • The right to informational self-determination of people • Constitutional basis in Article 16 ° as an individual guarantee • Increased public confidence by safeguarding your data • Cost reduction of security incidents casus 	<ul style="list-style-type: none"> • Ignorance or lack of awareness of the importance of consent.. • Loopholes in the law, need to define more terms of Act, etc.. (Lack of Legislation) • Bad Faith of Entrepreneurs by offering products in exchange for personal data vulnerable population (children, youth, etc..) • Lack of regulation of the internet (for computer crimes))
	OPPORTUNITIES	THREATS
External analysis	<ul style="list-style-type: none"> • There is a good level of commitment by the IFAI and the SE to spread campaigns on data protection in the mass media. • The recent entry into force of the Act, creates opportunities to take steps to create a level of awareness • Increased quality and accuracy of information. Better flow of information on citizens. 	<ul style="list-style-type: none"> • External fraud (hacker) • Cost for Implementation of the Law • Low security Mediated due to Lack Of Interest By The Address. • Information Exchange to 3rd and / or outsourcing