Information Technologies Industry Development Project

STUDY ON SELF-REGULATION REGARDING PRIVACY AND PERSONAL DATA PROTECTION WITHIN THE INFORMATION TECHNOLOGY ENVIRONMENT

Executive Summary

Introduction

As corollary of the **STUDY ON SELF-REGULATION REGARDING PRIVACY AND PERSONAL DATA PROTECTION WITHIN THE INFORMATION TECHNOLOGY ENVIRONMENT** related to the powers of the Mexican Ministry of Economy (SE in Spanish) according to article 43 (section V) of the Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) (Federal Law of Protection of Personal Data in Possession of Private Parties) to issue parameters – together with the Instituto Federal de Acceso a la Información y Protección de Datos (IFAIPD, Federal Institute of Information Access and Data Protection) – for the proper development of the self-regulation mechanisms and actions described in article 44 of the same Law, this executive summary contains the most relevant items of the study, as well as the conclusions and proposals that the Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) (National Chamber of the Electronics, Telecommunications and Information Technologies Industry respectfully makes.

1) General Concepts.- A first basic issue that the "collaboration" SE-IFAIPD must understand in the preparation of one (or several) parameters about self-regulation within the personal data protection is the consensus about the definition of the wide array of concepts involved in the universal digital world and, in particular, for the Information Technologies in Mexico.

2) Concept of parameter.- In this study, a certain notion of parameter has been used. For this purpose, "parameter" is herein understood as the set of general standards or factors determined by the Ministry of Economy together with the Federal Institute of Information Access and Data Protection that work as reference to establish or value the applicability and proper development of the mandated self-regulation mechanisms and actions regarding the protection of personal data in possession of private parties adopted by the persons responsible and persons in charge in order to complement the provisions of the Federal Law of Protection of Personal Data in Possession of Private Parties, its Regulation and the provisions issued by the government agencies to develop such mechanisms and actions and within the sphere of their respective jurisdiction.

As a parameter issued by SE-IFAIPD will be general, the Federal Law of Administrative Procedure opens the possibility of registering it in the "analogous" provisions. For this, such parameters must be published in the Diario Oficial de la Federación (Government Gazette) and be subject to the validation procedures with the Comisión Federal de Mejora Regulatoria (COFEMER) (Federal Regulatory Improvement Commission).

3) Concept of Information Technologies. As an IT industry, the collaborating agencies propose to consider it as the group of companies and/or enterprises whose main economic activity is to design, develop, produce, exploit, give maintenance and/or commercialize products, technologies and services associated to data processing and information custody and management, as well as any economic units related to the development of software and hardware, IT services, Business Process Outsourcing (BPO), digital creative mans, networks, applications or any other information technology that enable the digital exchange, storage and/or processing or by physical means of data.

4) Types of Self-regulation.- In compared law, there are for types of self-regulation: 1.- Mandated self-regulation, where a private organization or a group of private individuals is appointed to set and apply standards within a group generally established directly by public powers; 2.- Sanctioned self-regulation, where the standards are prepared by their receivers, and adopted finally by the public powers; 3.- Coerced self-regulation, where the standards are adopted autonomously when faced with the threat of an eventual public regulatory intervention; and 4.- Voluntary self-regulation, where there is no public intervention addressed to imposing or fostering, directly or indirectly, self-regulation.

In relation to the treatment of personal data and the self-regulation mechanisms or systems, from what was studied, it was found that there are at least three regulatory models that several countries have adopted: hetero-regulation systems, pure self-regulation and integrated or mixed self-regulation.

5) Experiences with the Self-regulation Models.- Although there are countries, like the United States of America, where pure self-regulation (not mandated) exists, i.e., without the intervention of the authority, there is hetero-regulation of the protection of personal data in possession of private parties regarding telecommunications and genetic information within the working environment. Besides, due to their federal character, there are several local laws that cover the topic.

Pure self-regulation tends to be replaced by a higher participation of authority, as it does not cover the expectations of the authority or the consumers. For this, the White House issued recently the results of a study called “Consumer Data Privacy in a Networked World: a Framework for protecting Privacy and Promoting Innovation in the Global Digital Economy”. It includes the Consumer Privacy Bill of Rights that are principles to protect personal data and are intended to be submitted to the Congress to become a law, or to

work as the basis to create conduct codes consolidated through public surveys according to the Consumer Privacy Bill of Rights.

The Canadian Model Code for the Protection of Personal Information proposed according to the principles contained in the national standards may be taken as a point of reference by organizations to create and operate their own Codes for the Protection of Personal Information with the minimum requirements set forth in such model code.

The first problem Canadian authorities had to face when implementing the Personal Information and Electronic Documents Act (PIPEDA) was to limit the scope of application of the act. This led to asking what the personal information that should be included under the protection of the act should be, making a difference between personal information and commercial activity. For that purpose, the protection of this act has been extended to photographs, business e-mail addresses, identification numbers linked to employees and IP addresses (computer Internet Protocol).

As to Mexico, it must be said that on February 22, 2012, the Permanent Mission of Mexico before the Organization of American States (OAS) submitted to the OAS the answers of a questionnaire about legislation and privacy and information protection practices “to get input that contribute to comply with the mandates contemplated n Resolution AG/RES. 2661 (XLI-011) dated October 6, 2011”, and acknowledged that in Mexico, only exist the self-regulation personal information models, the AMIPCI trust seal, the Code of Ethics of BBVA Bancomer and the Code of Conduct of NOVARTIS pharmaceutical group.

6) The Mixed or Integrated Self-Regulation Personal Information Model.- Within a third group of self-regulation systems, there is a clear trend of the countries towards a model that includes laws about personal information protection containing self-regulation models (*mixed or integrated model*). Mexico is in this category. Other countries that have adopted a similar approach are Germany, Argentina, Australia, Cyprus, Spain, Greece, Ireland, Italy, Japan, Luxembourg, Peru, Uruguay and the European Union.

7) The Deontological Codes.- Compared law shows that the privacy codes are the most usual self-regulation mechanism set forth until now by legislation. It has several names (codes of good practices, codes of conduct, deontological codes, type codes, etc.), and virtually all of them refer to behavior standards adopted by the persons to whom such provisions are addressed: industries, union associations or professional associations. Some of these codes are contained in the Law and others are made and enforced by the companies, representative associations or industries themselves.

This study underlined the main characteristics of the codes: representativeness, complementarity, advertising and registration, review, revocation, contents, evaluation, temporality and scope, and costs of preparation and adoption, with the idea of being integrated to a future institutional parameter in the subject.

In Spain, in spite of showing a low participation, there is a favorable issue that is worthy taking into consideration: the adoption of codes of conduct by the associations or groups that include several small or medium-sized companies. Thus, the participation is through collective representatives.

Another positive issue that can be rescued from the Spanish case is the (relatively) high level of participation of the entities responsible for dealing with personal information considered sensitive. They are associations that have shown some interest in leaving a record about treating properly this kind of information.

The only relevant code of conduct that promotes the use of a trust seal among its members is “Confianza Online”. This seal is addressed to the service providers of the information community, and covers aspects additional to the mere protection of personal information: consumer protection, online advertising and protection of minor children.

As to institutional codes of conduct, that is, the codes designed and promoted by a national authority, the ones issued by the English ICO represents a noteworthy example regarding the segments or principles covered. But once again, these codes do not address all the issues regulated by the personal information protection laws, or cover all the sectors that deal with personal information in their day-to-day operations.

The United Kingdom case is significant as to its extent of participation, because in spite of its system allowing for the adoption of a code for a profession or industry and the preparation of codes by the authority, there is only one code of conduct adopted by an industry, the others are codes that have been analyzed and identified in the study.

The situation of the United Kingdom is repeated in the European Union, where until now there is only one code of conduct regarding personal information protection that has a community validity scope.

8) Trust Seals, Trademarks or Marks.- From the review made until now, it was found that there are only a few mechanisms of certification similar to the approach intended to be adopted in Mexico. Although there are “Trust Seals”

(actually only one, the AMIPCI's), these have been mainly prepared by private entities (companies, associations, etc.) according to their own standards.

About this topic, it is recommended to read the study performed by Proyecto i+Confianza in 2002[1] to compare 19 trust brands or seals: L@belsite (France), Trusted Shops (Germany), Comercio Certificado (Argentina), e-com-quality mark (Italy), DIN Tested Website (Germany), Qweb (Italy), Trust-e (EE.UU.), Squaretrade (EE.UU.), Webassured (EE.UU.), Consumer Trust (Singapore), Health On the Net (Switzerland), BBBOnline Trust (EE.UU.), BBBOnline Privacy (EE.UU.), Confiar-e (Chile), [G] Garantía de Protección de Datos (Spain), AGACE (Spain), Bureau Veritas Web Value (France), IQA (Spain); and Marca AENOR de Buenas Prácticas Comerciales (Spain).

From the above seals, only half of them still exist: Trusted Shop, Qweb, Trust-e, Web Assured, Hon Code, Confiar-e, [G] now Confianza Online, AGACE y AENOR. BBBOnline Trust and BBBOnline Privacy merged into Better Business Bureau that has the "Business Seal for the Web".

Due to the fact that there is strong competition between the various trademarks, their commercial proposals to place trust seals have implied the presentation of the advantages and disadvantages of each seal. Thus, Trust-e qualifies itself as the best privacy seal, and claims that VeriSign Trust Seal, McAfee Secure Trustmark, Comodo HackerProof Seal or GeoTrust SSL Certificates are seals to guarantee security; and that the others are seals that only guarantee good commercial practices, such as BBB Accredited Business Seal, buySAFE Seal, Bizrate Customer Certified Seal or Shopping.com's Trusted Store Seal. What is important about such seals is that they participate as certifying agents of the Safe Harbor Privacy Principle and may be considered as relevant in building the Mexican models.

For the U.S. Department of Commerce, the trust seal granted to trans-border data flow between the U.S.A. and the European Union has been effective, as the persons that have such certification usually abide by it, but such fact is not an obstacle for the authority to file a legal action for breaching the model. However, a problem the U.S.A. authorities are facing is the misrepresentations of the companies, as the seal is only valid for one year,

[1] i+Confianza is a project promoted by the Asociación Española de Normalización y Certificación (AENOR), Asociación Española para el Derecho y la Economía Digital (AEDED), and Real e Ilustre Colegio de Abogados de Zaragoza (REICAZ) Fundació Catalana per a la Recerca (FCR). The document produced by this project is entitled "Libro Blanco sobre los Sistemas de Autorregulación, los Sellos de Confianza en Mercados Digitales y Códigos de Buenas Prácticas" (White Book on Self-regulation Systems, Trust Seals in Digital Markets and Good Practice Codes). AENOR, Spain, December 2002.

and the companies continue to use it after the expiration date. Perhaps for this reason, the European Union and the APEC are considering that the pure self-regulation trend must be replaced by a stronger participation of the authorities, as it does not meet the expectations of the authorities or the consumers.

The 2008 project called “Regional Trust Seal Pilot Project” continues to be on standby, as well as the proposals of the Red Iberoamericana de Protección de Datos (Data Protection of the Spanish-Latin American Network).

It is important to mention that the Trust Seals or Marks are generally signs granted when the companies or individuals have undergone an affiliation process to a deontological or good practice code and/or certification systems (verification, audit, etc.). If the seals European Privacy Seal (EuroPriSe) and Privacy Mark (Japan), there is no doubt that certification is essential to issue a seal. Moreover, if the above mentioned new proposals of APEC and the European Commission are reviewed, the trend is towards a certification-based self-regulation system.

9) Certification.- As discussed in this paper, the topic of certification is currently based on the Ley Federal sobre Metrología y Normalización (Federal Law on Metrology and Standardization), understood as the procedure through which it is ensured that a product, process, system or service complies with the standards or guidelines or recommendations of legal bodies dedicated to domestic and international standardization.

Within the systems of the Conformity Evaluation, certification is useful to determine the degree of compliance with the Mexican official standards or the conformity with the Mexican standards, the international standards or other specifications, prescriptions or characteristics. From a first analysis of these provisions, it can be inferred that the applicability of the certification notions (and even of accreditation) is focused on the procedures and methods set forth in the Mexican Official Standards (NOMs in Spanish), and/or by default, the international standards. Thus, it could be deduced *a priori* that they are not applicable to the parameter issue.

With a proposing intention, the accreditation described in the Regulation of the LFPDPPP may be defined with a practical sense to stimulate the adoption of self-regulation systems, especially if it is taken into consideration that the bottom line is that self-regulation is voluntary and that the IFAIPD does not lose – at any time – its powers to verify that the responsible entities or individuals comply with the law and its principles regarding the protection of personal information.

Attention must be paid to the fact that the European Commission recently said that it will explore the possibility of creating European systems to certify the procedures, technologies, products and services that conform to the privacy protection standards.

The privacy certification systems of the European Privacy Seal, the Japanese Privacy Mark and the APEC, whose standards are explained herein, have been found relevant for this essay.

10) Advantages of Self-regulation regarding Personal Information.- With the idea of describing the advantages of the self-regulation models regarding the protection of personal information, this study analyzed the most relevant ones for the industry, authorities and, particularly, the personal information subjects:

Prevention

- The establishment of self-regulation systems or models has a mainly preventive function, as they will enable mitigating or even establishing mechanisms to mediate among the parties and that the damages or injuries that certain actions may cause can be solved within a private environment.

Dispute Solution

- It allows for the establishment of forms of mediation or dispute solution through procedures *ad hoc* for each industry, taking into consideration the needs of a certain industry or the private sector.

- Effective procedures where analysis and solution times are short can be designed through the dispute solution mechanisms proposed by self-regulation.

- The procedures put in place in the self-regulation mechanisms to solve disputes may result in costs lower than the costs of the procedures where authorities participate.

- The mediation and dispute solution systems contributed by the majority of the organizations that promote self-regulation may be considered as part of the service performed by the responsible agents and the certifying organizations.

Reputation considerations

- It is thought that the adoption of a certain self-regulation mechanism contributes to a large extent to the image capital, as the users, parties, etc., will project an image of responsibility and respect to the protection of personal information.
- With the projection of a commitment and responsibility image regarding the protection of personal information, the individuals or companies that adopt a self-regulation model will achieve, to a certain extent, establishing a trust relationship with their customers or users.

Economic and competitive benefits

- The adoption of self-regulation mechanisms will not only represent benefits to the users, clients or parties, the individuals or companies that adopt them will represent economic benefits, as they will have more possibilities of establishing commercial relations at international level.
- One of the input products of digital economy is the personal information of users, customers or parties. For this, the adoption of the best practices regarding privacy will enable the healthy development of the domestic economy in general.
- It is very useful for the economic development to integrate to the legal system the standards that are actually necessary to organize and agree on good practices through deontological codes, without having to undergo the legislative process, while there is a coexistence and complementarity of the regulatory frameworks.
- The trust seals have achieved that a large group of users have created trust and increased participation throughout all their online channels, including websites, mobile applications, advertising, cloud services, business analysis and e-mail marketing.

Tailored Privacy

- An important advantage of the self-regulation models is that for their adaptation to reality or the needs of a certain sector, industry or company, it is not necessary to follow a complex procedure (such as in the case of any government regulation), which results in nimble processes.
- Self-regulation will allow for the application of legal demands in a simple way, attending the needs and realities of the various business models existing in the digital world.

- A big advantage is the flexibility with which the self-regulation mechanisms can be applied to technological changes that are adopted by several sectors.

- Through self-regulation, very specific and complex topics can be regulated, such as the protection of minor children's personal information.

- Several researchers state the advantages of self-regulation over Internet state regulation, claiming that self-regulation is faster, more flexible and more efficient; that the experience accrued by the industry can be used for these purposes, and the government resources are limited. Self-regulation allows for – if the parties are willing – regulation to be implemented more efficiently, regulation that includes penalization mechanisms within the private sector.

Complementarity

- The self-regulation mechanisms are intended to complement and make effective the application of law. In some cases, as observed in this study, such mechanisms tend to substitute the government regulation.

- Self-regulation is a way of promoting the best commercial practices regarding the protection of personal information as input of the digital economy and the domestic economic development as a whole.

- The codes of conduct prepared by the industry, commercial and professional organizations have been defined as "a bridge" between the substantive rules of the information protection laws and their implementation at operation level.

Trust

- The self-regulation models may be the way that enables the development of electronic commerce, allowing the creation of a trust environment between the users and the responsible individuals/companies, as the adoption of mechanisms will show commitment and responsibility regarding the protection of personal information.

- For the users, it has the advantage of being able to see which companies are parties of the self-regulation mechanism that meets their needs better.

- Self-regulation fosters mechanisms that eliminate the largest number of obstacles to the development of electronic commerce, such as the lack of trust of the consumers in websites that offer products or services.

- In cyberspace, the central object of self-regulation is to generate trust in the interaction of the users of Internet, and in this sense, the idea is to compare the actions and processes within an ethical framework to improve the quality of a service within the Internet world.

- With the proper framework, the verifications, balances, surveillance and control of self-regulation make it a more attractive route than the enactment of laws by the central government.

Social benefits

- The mass media such as radio, TV, written press, advertising and Internet already have self-regulation mechanisms, many times related to the methods and the selection of certain contents that may affect severely society or commercial practices.

- Frank Kuitenbrouwer states that self-regulation may aid several purposes in relation to the legislative process: self-regulation may be intended to avoid legislation; may be used to anticipate legislation; may be used to implement legislation; and may also be used to complement laws.

- Self-regulation allows for offsetting insufficiencies and limitations, favoring that its target activities are adjusted to its own values and standards. Thus, it is appropriate to consider it an adequate complement of regulation, mainly in the sectors where special conflicts exist regarding basic rights.

- It is possible to regulate every single area of cyberspace in order to gain the trust of users. The efforts to regulate the Internet, mainly regarding electronic commerce are, in the first place, justifiable as an alternative before the information society that lacks territory limits (hence, legal limits), but self-regulation is the ideal instrument to contribute to the government agencies being able to attend and solve problems derived from the Internet.

- For the APEC any protection system adopted, whether legislative, self-regulatory or of any other kind, should prevent the misuse of personal information and the damage that may be caused to private parties, always proportionately considering the probability and seriousness of the damage that may represent information collection.

- As to work matters, the good practice codes are useful as they achieve a certain balance between the legitimate expectations of employees about

the proper treatment of their persona information and the legitimate interest of their employers to carry out their own businesses within the legal framework.

- A proper procedure to grant trust seals is built on a solid base of transparency and accountability regarding the collection and use of personal information.

11) General and specific principles for Self-regulation regarding personal data protection.- As part of this study, some principles were proposed that must be taken into consideration in the initial or advanced stages of a mandated self-regulation system for the protection of personal information in possession of private parties.

As **General Principles**, the following are proposed:

a) All entities and/or companies of the IT industry must know and respect the principles that rule the treatment of personal information. For that purpose, the economic agents must guarantee the performance of training courses at all levels for the persons who deal with personal information because of their functions or responsibilities.

b) The confidentiality duty must be fostered as an unavoidable principle of anyone that due to his functions or responsibilities deals with personal information.

c) The respect of the rights of the personal information subjects, among other things, must be guaranteed through the due implementation of procedures to attend ARCO rights requests and the appointment of a person or department described in article 30 of the LFPDPPP.

d) The information systems that deal with personal information must be identified in order to find out whether they meet the security levels necessary for the type of information they deal with.

e) Internal actions of each organization must be adopted to allow programing, in the shortest time possible, the performance of the gap analysis described in article 61 (section V) of the Regulation of the LFPDPPP. The above, must be done apart from the need of taking into consideration any of the other actions listed in article 61.

f) As applicable, all the corrective actions necessary must be carried out for the information systems that deal with personal information to meet the actions to guarantee the security of personal information.

g) The “indefinite conservation” practice of the manual supports with which personal information is dealt with must be eliminated, and the periodical deletion of personal information treated through electronic devices must be fostered when in both cases the purpose for which the information was collected has been achieved and there are no legal regulations that provide for the conservation of such information for a longer period of time.

h) As long as its activities allow it, the IT industry must implement a “paperless office” within its own activities.

i) All organizations are responsible for any data transfers (domestic and international) to be carried out in the regular course of their activities. As applicable, the lawfulness of the transfer must be ensured, if it is made for purposes other than the ones that originated the data collection.

j) No website owned by the companies who participate in the IT industry may lack of a Privacy Policy and, as the case may be, of Privacy Notices legally enforceable if personal information is collected through such sites.

As **Particular Principles**, the following are proposed for some sectors especially relevant for the treatment of personal information in the digital environment.

Companies devoted to the design, development, production, exploitation, maintenance and/or commercialization of products, technologies and services associated to data processing and information custody and management:

a) All companies that process, takes care of or manages personal information for third parties is a **person in charge** according to the definition of article 3 (section IX) of the LFPDPPP and article 49 of its Regulation. Such companies must regulate such treatment by adopting the contract provisions (or any other legal instrument) set forth in article 51 of the Regulation of the LFPDPPP.

b) The persons in charge (*encargados*) must comply with all the enforceable security measures according to the type of personal information they deal with or according to the purpose of such treatment. No person in charge must deal with personal information if his products, technologies or associated services do not meet such security measures.

c) The employees of the persons in charge (*encargados*) must be conscious about the confidentiality duty they assume when dealing with personal information.

Software and hardware development companies:

a) The companies that develop software to be used to treat personal information must make sure that their products will allow their users to comply with the enforceable security measures according to the type of personal information to be treated or in relation to the purpose of such treatment.

b) The manufacturers of hardware must make sure that their products guarantee the availability, accessibility and integrity of the information treated in them.

Companies providing IT Services or Business Process Outsourcing (BPO)

a) If the service performance includes the treatment of personal information, these companies will be acting as persons in charge (*encargados*) and, consequently, they must abide by the provisions of the LFPDPPP and its Regulation.

b) In one word, they must regulate the relationship with their clients by adopting the contract provisions (or another legal instrument) described in article 51 of the Regulation of the LFPDPPP.

c) The employees of this kind of companies must be conscious of the confidentiality duty they assume when dealing with personal information.

Digital creative media, networks, applications or any other information technology that allows for information exchange, storage and/or processing or through information physical means:

a) The companies devoted to these activities must make sure that the technologies used ensure the integrity of the personal information exchanged.

b) They must also guarantee that, during information transfer, no person that is not duly authorized can have access to such information.

c) In case these companies perform electronic communications registration, they must make sure that they have the consent of the information subjects for that purpose or, otherwise, that there are laws that authorize such registration.

Children and Teenagers.- Following the policy of the United States of America, the Children's Online Privacy Protection Act (COPPA) was enacted

in 1998, and the Children's Online Privacy Protection Rule became effective on April 21, 2000, both with the purpose of protecting personal information of children under 13 years of age obtained through the Internet.

For that, the service providers must join a FTC-approved self-regulated model. Websites get a trust seal with which they can obtain personal information of the minor children with an authenticated permit of the parents.

Trans-border Data Flow.- A principle in this area is derived from Directive 95/46/EC of the European Union. According to this Directive, data exchange may only be made with countries that have similar laws that guarantee the proper protection of personal information. For such purpose, the Safe Harbor Privacy Principles between the European Union and the U.S. Department of Commerce were agreed. Consequently, the companies that meet these requirements may apply for a trust seal to such Department in order to perform trans-border data exchange for one year. At present, over 2,700 companies belong to the trans-border data flow program with the European Union.[2]

Reference must be made to the case of the new U.S. framework that calls the industry to increase its efforts to educate consumers regarding privacy and the tools available to demand their rights. For this, there are additional principles that we must discuss, such as:

The **simplified option** is a principle that permeated in the United States of America in order for the companies to simplify the consumer's options.

Other principles derived from the *habeas data*:

a) Foster a policy addressed to the companies consisting in "Do not track".
b) Improve the **privacy policies in mobile devices**, as in the last few years their use and capacity have increased.
c) Invite the data brokers to **comply with the privacy standards** to increase the transparency of their services.
d) Extend the work to the **great platform providers**, such as Internet service providers, operation system developers, browsers and social networks in order to increase their privacy levels in favor of consumers.
e) **Promote self-regulation with the creation of enforceable codes.-** In regard to this issue, the U.S. Department of Commerce, supported by the main actors of each industry, started a project to facilitate the development of **codes of conduct for specific sectors.** The Commission has seen this effort favorably and has invited the self-regulation companies,

2 See White House, note 1 *supra*, page 33

associations and firms to adopt the principles contained in the regulatory framework.

12) Parameter Proposal (structure).- A way to summarize or condense the findings of the works to compare the self-regulation models on privacy and protection of personal information within the specific area of the IT, as well as to create concrete recommendations on the subject, is to prepare a first draft to be used as the basis or guideline to issue the so-called "*parameters for the proper development of the self-regulation mechanisms and measures".*

It is important to mention that with that purpose, it has been necessary to determine first the method to write the *parameters*, that is, their "format", as these regulatory models do not appear in any kind of text known formally until now, at least from the point of view of a standard that has general effects with such a name. Thus, several systems have been explored to achieve this purpose, and it was found that the best format is something similar to an administrative regulation.

Another relevant issue to be considered is the material environment of validity and application of the parameters, especially if this study has focused on the digital environment or the environment of the IT as expressed in the Reference Terms.

Taking into account that there are connection points in the physical world and the digital environment that the parameters may include, it was thought to respectfully propose a bill that is not limited to one or the other environment, but that has a general approach, and that the parameters become gradually specialized according to the various sectors.

It is very important that the material field of the parameters clearly defined in such parameters, that is, that a specific difference is clearly drawn between each one of the self-regulation mechanisms contemplated by the LFPDPPP and its Regulation (deontological codes, good professional practice codes, trust seals, privacy policies, corporate privacy rules, and other mechanisms that include specific rules or standards), in order to avoid confusions between the private parties and the authorities.

The certification of the responsible persons (*responsables*) is an issue that requires definition as a tool to guarantee the proper development of the self-regulation measures or mechanisms and, especially, the due legal consensus about whether the parameters 1) will refer to the Law of Metrology and Standardization regarding accreditation / certification, 2) will extend to the

provisions of that Law, or 3) a *sui generis* or *ad hoc* framework will be created for this issue, must be reached.

A) TYPE OF LEGAL INSTRUMENT

It is proposed to write an AGREEMENT through which the parameters for the proper development of the enforceable self-regulation systems described in article 44 of the Mexican Federal Law for the Protection of Personal Information in Possession of Private Parties are announced.

B) CONTENTS

BACKGROUND

This section must contain the bases of the administrative act consisting of the agreement that announces the parameters linking it to the 2007-2012 National Plan of Development and Economy Sector Program.

CHAPTER I
GENERAL PROVISIONS

This first article must define the object of the parameters and their application field, as well as the basic definitions to understand them properly. Likewise, it must contain the characteristics of the enforceable self-regulation systems.

CHAPTER II
SELF-REGULATION SYSTEM TYPES

The main elements of the various systems (means and mechanisms) of self-regulation mentioned in the LFPDPPP and its Regulation must be described: deontological codes, good professional practice codes, trust seals, privacy policies and other mechanisms.

CHAPTER III
CONTENT OF THE SELF-REGULATION SYSTEMS

This section is very important to develop the minimum mandatory contents of the various self-regulation systems that may be registered by the IFAIPD, as well as their application field. Here rules are set

about complementarity, mechanisms to measure the efficiency of the system adopted, consequences and corrective measures in case of non-compliance, identification of the responsible persons, supervision and surveillance systems, training, concrete measures taken regarding the protection of special information subject categories (*minors, disabled people or non-Spanish speaking persons*), domestic and international transfer of personal information, system administration, procedures to protect information and alternative mechanisms to solve disputes.

CHAPTER IV
CERTIFICATION

The purpose of this chapter is to set forth the framework about accreditation and certification in order to set its object, characteristics, functions of the accrediting and certifying agencies, certifying procedures and types of certificates. This chapter must also contain the obligations of the individuals or corporations that are recognized as certifying agencies for the protection of personal information, under the principles of independence, objectivity, confidentiality and verification. This chapter approaches also the topics related to validity, renewal and revocation of accreditation.

CHAPTER V
SELF-REGULATION SYSTEMS NOTIFICATION

This section contains the general requirements to perform the procedure to notify the self-regulation systems that are convenient for the private parties according to the first paragraph of article 44 of the LFPDPPP with the applicable sector authorities and the Institute, which may be in writing or through the IFAIPD website.

CHAPTER VI
REGISTRATION

It only states that the notified self-regulation systems will be registered in the Registro de Esquemas de Autorreglación Vinculante de Protección de Datos Personales en Posesión de Particulares (Registry of Enforceable Self-regulation Systems for the Protection of Personal Information in Possession of Private Parties) under the charge of the Institute, provided that the requirements set forth in these Parameters and the parameters set forth in the Reglas para el Registro de Mecanismos y Medidas de Autorregulación (Rules to Register Self-regulation Mechanisms and Measures) in the subject.

PROVISIONAL ARTICLES

This section sets forth that the parameters will be effective as of the day following their publication in the Diario Oficial de la Federación (Government Gazette) and that, for the purposes of its implementation, the coordination with several agencies of the Federal Public Administration will be established upon a call of the head of the Ministry of Economy

13) Final Considerations.- Although it has not shown been a model with high participation, self-regulation must continue to be considered an alternative to promote better personal information protection practices.

Those who adopt a self-regulation model promote in their organization or the organization of their affiliated companies an intense reorganization of their information security systems and a change of culture in the personnel that deal with personal information, things that are indispensable to reach the protection levels that the majority of the laws demand for the treatment of this kind of information.

On the other hand, and taking as a reference point the demands of the European Union, it is indispensable to take into consideration that this region demands that the transfer information outside the European Economic Space must be done towards countries or responsible persons (*responsables*) that guarantee a level of protection of personal information equivalent to the level provided in that region.

In this sense, the adoption of self-regulation systems may be a distinctive element to increase the competitiveness of the IT industry against other market options, as the actors of this industry that offer services such as hosting or call centers are highly required by European companies.

It is important to mention that the adoption of self-regulation mechanisms or measures with added value (such as government support or certification) may increase trust in electronic commerce, within an environment that has not yet exploited all the capacity of that commercialization means.

It is perceived that the extent of participation of the competent authorities is an important factor for the success of the self-regulation systems, because they are the ones that may foster their adoption by means of divulgation actions or a positive distinction in favor of those responsible persons who have adopted them.

For the above, it is recommended to analyze the possibility of creating a strategy addressed to the implementation of a self-regulation system with high participation of the authorities in charge of driving the productive development of specific sectors of economy, with the institutional support of the Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAIPD) Federal Institute of Access to Public Information and Information Protection.

The above mentioned strategy must define also whether it drives and implements a system that promotes the adoption of pure and simple codes of conduct or codes that grant added value to their adoption by granting duly promoted and supported trust seals or marks.

Project prepared for:

Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI)
(National Chamber of the Electronic, Telecommunications and Information Technologies Industry)

By:

CGMPS Consultores Especializados, S.C.

www.cgmps.com.mx