THIRD SECTION
EXECUTIVE BRANCH
MINISTRY OF THE ECONOMY

REGULATIONS to the Federal Law on the Protection of Personal Data Held by Private Parties

In the margin, a seal with the National Coat of Arms that reads: United Mexican States.- Office of the President of the Republic.

FELIPE DE JESUS CALDERÓN HINOJOSA, President of the United Mexican States, in the exercise of the power vested in me by Article 89(I) of the Constitution of the United Mexican States, pursuant to Article 34 of the Federal Public Administration Organizational Law and Articles 3(X), 18, last paragraph, 45, last paragraph, 46, second paragraph, 54, last paragraph, 60, last paragraph, and 62, last paragraph, of the Law on the Protection of Personal Data Held by Private Parties, hereby issues the following:

REGULATIONS TO THE FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES

Chapter I
General Provisions

Purpose

Article 1. The purpose of this law is to regulate the provisions of the Federal Law on the Protection of Personal Data Held by Private Parties.

Definitions

Article 2. In addition to the definitions established in Article 3 of the Federal Law on the Protection of Personal Data Held by Private Parties, for the purposes of these Regulations, the following definitions shall apply:

I. Departments: Those indicated in Article 26 of the Federal Public Administration Organizational Law;

II. ARCO rights: The rights of access, rectification, cancellation and objection;

III. Digital environment: The environment made up of the combination of hardware, software, networks, applications, services, or any other technology of the information society that allows for the exchange or computerized or digitalized processing of data;

IV. Exclusion list: Database intended to record free-of-charge the refusal of the data subject to have his personal data processed;

V. Administrative security measures: Combination of actions and mechanisms to establish the management, support, and review of the security of information at an organizational level, the identification and classification of information, as well as the creation of an awareness by personnel and their education and training in the area of protection of personal information;

VI. Physical security measures: Combination of actions and mechanisms, whether or not using technology, intended to:

a) Prevent unauthorized access or damage to or interference with physical installations, critical areas of the organization, equipment and information;

b) Protect mobile, portable, or easily removable equipment located inside or outside installations;

c) Provide maintenance to equipment containing or storing personal data so as to ensure their availability, proper working order, and integrity, and

d) Guarantee the elimination of data in a secure manner;

VII. Technical security measures: Combination of activities, controls, and mechanisms with measurable results that use technology to ensure that:

a) Access to logical data bases or to information in logical format is by identified and authorized users;

b) The access referred to in the previous paragraph is only so that the user may carry out the activities required by his position;

c) Actions to acquire, operate, develop, and maintain secure systems are included, and

d) The management of communications and computerized resources used in the processing of personal data is carried out

VIII. Identifiable individual: Any individual whose identity can be determined, directly or indirectly, by any information. An individual will not be deemed identifiable when to obtain the identification, disproportionate periods of time or activities are required;

IX. Transmission: Communicating personal data between a data controller and a data processor, within or outside of Mexico;

X. Electronic media: Storage medium that can be accessed only by means of the use of a device with electronic circuits that processes its contents in order to examine, modify or store personal data, microfilms included;

XI. Physical media: Storage medium intelligible by sight, in other words, which does not require any device to process its content in order to examine, modify or store the personal data, and

XII. Suppression: Activity consisting in eliminating, erasing, or destroying personal data, once the blocking period has elapsed, under security measures previously established by a data controller.

Subject Matter

Article 3. These Regulations apply to the processing of personal data found on physical or electronic media that make possible, access to personal data according to specific criteria, regardless of the form or method of its creation, type of media, processing, storage, or organization.

These Regulations do not apply when, in order to obtain access to personal data, disproportionate periods of time or activities are required.

Pursuant to Article 3(V) of the Law, personal data may be in numerical, alphabetical, graphic, photographic, acoustic or other any other form, concerning an identified or identifiable individual.

Territorial Scope

Article 4.

These Regulations will be obligatory for all processing when:

I. It is carried out in an establishment of the data controller located in Mexico;

II. It is carried out by a data processor, regardless of its location, on behalf of a data controller established in Mexico;

III. The data controller is not established in Mexico but is subject to Mexican laws as a consequence of entering into a contract or under international law, and

IV. The data controller is not established in Mexico and uses media located in Mexico, unless such media are used only for transit purposes that do not involve processing. For purposes of this subsection, the data controller shall provide the media necessary to comply with the obligations imposed by the Law, its Regulations, and other applicable rules and regulations with respect to the processing of personal data. For this purpose, it shall designate a representative or implement the mechanism that it considers appropriate, provided that by means of this, it is ensured that the data controller will be able to effectively comply with the obligations that are imposed by law on individuals and corporate bodies that deal with personal data in Mexico.

When the data controller is not located in Mexico, but the data processor is, the latter shall be subject to the provisions related to the security measures contained in Chapter III of these Regulations.

In the case of individuals, the establishment shall mean the location of their main place of business or that used to perform their activities or their home.

In case of corporate bodies, the establishment shall mean the location of the principal management of the business; in case of corporate bodies residing abroad, the location of the principal management of the business in Mexico, or in the absence thereof, that designated by them or any stable installation that allows actual or real performance of an activity.

Information About Individuals Carrying on Business and Data About Their Representatives and Contacts

Article 5. These Regulations shall not be applicable to the following information:

I. With respect to corporate bodies;

II. With respect to individuals as businessmen and women and professionals, and

III. With respect to individuals who provide services for a corporate body or individual engaged in business and/or providing services consisting only of their first names and surnames, the position or post they hold, as well as some of the following employment data: physical address, electronic address, telephone and fax numbers; provided that this information is used only for purposes of representing the employer or contractor.

Processing Arising from a Legal Relationship

Article 6. When the processing has as its purpose that of complying with an obligation arising from a legal relationship, it will not be considered as for exclusive personal use.

Public Access Source

Article 7. For the purposes of Article 3(X) of the Law, the following shall be considered as a public access source:

I. Remote or local electronic, optical and by other technological means of communication, provided that the location of the personal data is intended to facilitate providing information to the public and is open for general consultation;

II. Telephone directories as provided in applicable rules and regulations;

III. Official newspapers, gazettes and/or bulletins as provided in applicable rules and regulations, and

IV. Social communication media.

For the cases listed in this Article to be considered public access sources, it will be necessary for them to be able to be consulted by any person not prevented from doing so by any rule or regulation, or without any requirement other than, if applicable, the payment of consideration, a fee or charge.

A public access source shall not be considered as such when the information contained in it is illicit or has an illicit origin.

The processing of personal data from a public access source shall respect the reasonable expectation of privacy to which Article 7, third paragraph, of the Law refers.

Groups Without Legal Status
Article 8. Those forming part of a group that acts without legal status and that deals with personal data for specific purposes or for purposes of the group shall also be considered as data controllers or data processors, as the case may be.

Chapter II
Principles of Protection of Personal Data

Section I
Principles

Principles of Data Protection
Article 9. Pursuant to Article 6 of the Law, data controllers shall comply with the following principles governing the protection of personal data:

I. Legitimacy;

II. Consent;

III. Information;

IV. Quality;

V. Purpose;

VI. Loyalty;

VII. Proportionality, and

VIII. Accountability.

In addition, the data controller shall observe the duties of security and confidentiality to which Articles 19 and 21 of the Law refer.

Principle of Legitimacy
Article 10. The principle of legitimacy requires the data controller to ensure that processing follows and complies with the provisions of Mexican and international law.

Principle of Consent
Article 11. The data controller must obtain consent for the processing of personal data unless it is not required under Article 10 of the Law. The request for consent shall refer to a specific purpose or purposes, contemplated in the privacy notice.

When personal data are obtained personally or directly from the data subject consent shall be prior to the processing.

Characteristics of Consent
Article 12. Obtaining consent, tacitly or explicitly, shall be:

I. Free: without error, bad faith, violence or fraud that may affect the expression of the will of the data subject;

II. Specific: refer to one or several specific purposes that justify the processing, and

III. Informed: the data subject must previously know from the privacy notice, the processing to be done with his personal data and the consequences of granting his consent.

Express consent must also be unequivocal, in other words, that there are elements that unquestionably demonstrate that it was given.

Tacit Consent
Article 13. Unless the Law requires the express consent of the data subject, tacit consent will be valid, as a general rule, pursuant to Articles 12 and 13 of these Regulations.

Request for Tacit Consent
Article 14. When the data controller seeks to collect personal data directly or personally from the data subject, it shall previously make available to the data subject a privacy notice which shall contain a mechanism by which, as the case may be, the data subject may state his refusal to allow the processing of his personal data for purposes different from those that are necessary and that create a legal relationship between the data controller and the data subject.

In those cases in which personal data is obtained indirectly from the data subject and cause a change in the purposes that were consented to in the transfer, the data controller shall make available to the data subject a privacy notice prior to using the personal data. When the privacy notice is not brought to the notice of the data subject directly or personally, the data subject shall have a period of five day to state, as the case may be, his refusal to allow the processing of his personal data for purposes which are different from those that are necessary and that create a legal relationship between the data controller and the data subject. If the data subject does not state his refusal to the processing of his data in accordance with the foregoing, it shall be understood that he has given his consent to the processing of the same, unless there is evidence to the contrary.

When the data controller uses remote or local electronic, optical or other technological means of communication mechanisms that allow personal data to be obtained automatically and simultaneously at the time the data subject has contact with the mechanisms, at the same time the data subject must be informed of the use of such technology, that through these mechanisms personal data will be obtained, and of the manner in which this can be disabled.

Express Consent
Article 15. The data controller must obtain the express consent of the data subject when:

I. It is required by law;

II. In the case of financial or property data;

III. In the case of sensitive data;

IV. It is requested by the data controller to prove the same, or

V. It is so agreed by the data subject and the data controller.

Request for Express Consent
Article 16. When express consent is required by law, the data controller shall provide the data subject with a simple and free-of-charge means of stating this, if he so wishes.

Exceptions to the Principle of Consent
Article 17. As provided in Articles 10(IV) and 37(VII) of the Law, tacit or express consent will not be required for the processing of personal data when this arises from a legal relationship between the data subject and the data controller.

The previous paragraph shall not apply when the processing of personal data is for purposes different from those that are necessary and create the legal relationship between the data controller and the data subject. In this case, to obtain tacit consent, the data controller shall observe the provisions of Article 8, third paragraph, of the Law and Articles 11, 12, and 13 of these Regulations, and with respect to sensitive, financial, or property data, it shall obtain express consent, or as required by the Law, express and written consent.

Verbal Consent
Article 18. It is considered that express consent was given verbally when the data subject gives it orally to the data controller in the latter's presence of by the use of any technology that permits oral dialogue.

Written Consent
Article 19. It will be considered that express consent was given in writing when the data subject provides it in a document bearing his hand-written signature, fingerprint, or any other mechanism authorized by law. In a digital environment, an electronic signature may be used or any mechanism or procedure that is established for this purpose and permits the identification of the data subject and the obtaining of his consent.

Proof of Obtaining Consent
Article 20. To show that consent has been obtained, the burden of proof always rests upon the data controller.

Withdrawal of Consent
Article 21. At any time, the data subject may revoke his consent for the processing of his personal data and the data controller shall establish simple and free-of-charge mechanisms to permit the data subject to revoke his consent using at least the same media that he used to provide it, provided that the law does not prevent this.

The mechanisms or procedure established by the data controller to deal with consent revocation requests may not exceed the period contemplated in Article 32 of the Law.

When the data subject requests confirmation that the processing of his personal data has stopped, the data controller shall expressly respond to such request.

If the personal data has been transmitted prior to the date of the revocation of consent and continue to be processed by the data processor, the data controller shall bring the revocation to the attention of the data processor so that he takes the necessary steps to deal with it.

Procedure in the Case of a Refusal to Stop Processing
Article 22. In case of refusal by the data controller to stop the processing of personal data in the event of a withdrawal of consent, the data subject may file with the Institute the complaint to which Chapter IX of these Regulations refers.

Principle of Information

Article 23. The data controller must bring to the attention of the data subject the information related to the existence and main characteristics of the processing to which his personal data will be submitted, through a privacy notice, pursuant to the Law and this Regulations.

Characteristics of the Privacy Notice

Article 24. The privacy notice must be simple, with the necessary information, written in a clear and understandable language, and with a structure and design that facilitates its understanding.

Means of Divulging

Article 25. For the divulging of privacy notices, the data controller may use physical or electronic formats, verbal means or any other technology, provided it complies with the duty to inform the data subject.

Contents of the Privacy Notice

Article 26. A privacy notice must contain the items referred to in Articles 8, 15, 16, 33, and 36 of the Law, as well as those established in the guidelines referred to in Article 43(III) of the Law.

Privacy Notice to Obtain Personal Data Directly

Article 27. As provided in Article 17(II) of the Law, when personal data is obtained directly from the data subject, the data controller must immediately provide at least the following information:

I. The identity and address of the data controller;

II. The purposes of the processing, and

III. The mechanisms offered by the data controller so that the data subject will be aware of the privacy notice in accordance with Article 26 of these Regulations.

The immediate divulging of the above information does not exempt the data controller from the obligation to provide mechanisms for the data subject to become aware of the content of the privacy notice, pursuant to Article 26 of these Regulations.

Privacy Notice in Formats with Limited Space

Article 28. The data controller may bring a privacy notice to the attention of the data subject, as provided in the previous Article, when it obtains personal data by printed means, provided the space used to obtain the personal data is minimal and limited so that the personal data obtained is also the minimum.

Privacy Notice to Obtain Persona Data Indirectly

Article 29. When personal data is obtained indirectly from the data subject, the data controller must observe the following in order to bring the privacy notice to the attention of the data subject:

I. When the personal data are processed for the purpose contemplated in the consent to transfer or have been obtained from a public access source, the privacy notice shall be made known in the first contact with the data subject, or

II. When the data controller wishes to use the data for a purpose different from that consented to, in other words, there will be a change of purpose, the privacy notice must be made known prior to the use of the data.

Processing for Marketing, Advertising, or Commercial Exploration

Article 30. Among the purposes of processing referred to in Article 16(II) of the Law, as applicable, there must be included those concerning processing for marketing, advertising, or commercial exploration.

The above is without prejudice to current law which regulates processing for the purposes set out in the previous paragraph when this contemplates higher protection for the data subject than that provided in the Law and these Regulations.

Proof of Privacy Notice

Article 31. To show that a privacy notice has been given in accordance with the principle of information, the burden of proof shall always rest upon the data controller.

Compensatory Measures

Article 32. In accordance with Article 18, third paragraph, of the Law, when it is impossible to communicate the privacy notice to the data subject or this requires disproportionate efforts given the number of data subjects or the age of the data, the data controller may implement compensatory measures using mass communication media in accordance with the guidelines issued by the Institute and published in the Federal Official Gazette under which it is possible to use the measures established in Article 35 of these Regulations.

The cases not included in the guidelines issued by the Institute shall require the express authorization of the latter, prior to the implementation of the compensatory measure, in accordance with the procedure established in Articles 33 and 34 of these Regulations.

Request for Authorization of Compensatory Measures

Article 33. The procedure to obtain authorization from the Institute for the use of compensatory measures using mass communication media to which the previous Article refers, shall always be initiated at the request of the data controller.

The data controller shall submit the request directly to the Institute or by any other means that the latter has authorized for this purpose. The request shall contain the following information:

I. The name of the data controller making the application, and as applicable, of its representative, as well as a copy of the official identification proving legal status and the original for comparison. In the case of a representative, a copy of the document proving his right to represent the data controller must be submitted, as well as the original for comparison;

II. Address to receive notifications and name of person authorized to receive them;

III. The processing to which it is intended to apply the compensatory measure and its principal features, such as purpose; type of personal data processed; if transfers are to take place; details of the data subjects, among them age, geographic location, educational and socio-economic level, among others;

IV. Causes or justification for the impossibility of bringing a privacy notice to the attention of the data subjects or the disproportionate efforts that this would require. The data controller shall state the number of data subjects involved, age of the data, whether or not there is direct contact with the data subjects, and their economic situation;

V. Type of compensatory measure sought to be used and for what period of time it will be published;

VI. Proposed text for the compensatory measure, and

VII. Documents that the data controller considers necessary to submit to the Institute.

Procedure for Authorization of Compensatory Measures

Article 34. The Institute shall have a period of ten days following receipt of the request for compensatory measures to issue its decision on the matter.

If the Institute does not issue a decision within the period established, the compensatory measure request will be considered as authorized.

Once the request is submitted by the data controller to the Institute, the latter shall weigh the disproportionate efforts to make known the privacy notice, taking the following into account:

I. The number of data subjects;

II. The age of the data;

III. The economic situation of the data controller;

IV. The geographic area and sector in which the data controller operates, and

V. The compensatory measure to be adopted.

When weighing the request, if the Institute considers that the compensatory measure proposed does not comply with the principle of information, it may propose to the data controller the adoption of a compensatory measure different from that suggested by the data controller in its request.

The proposal of the Institute shall be brought to the attention of the data controller so that it may take such action as it considers appropriate within a period of no more than five days, calculated from the day following that on which it received notification.

If the data controller does not respond within the period mentioned in the previous paragraph, the Institute shall resolve the matter based on the file of the matter.

When the Institute decides that the data controller does not justify the impossibility of bringing the privacy notice to the attention of the data subject or that this requires disproportionate efforts, the use of compensatory measures shall not be authorized.

Any authorization given by the Institute shall be valid unless the circumstances under which the compensatory measure was authorized change.

Features of Compensatory Measures

Article 35. Mass communication compensatory measures must contain the information provided in Article 27 of these Regulations and shall be made known by means of privacy notices published in any of the following media:

I. Newspapers with national circulation;

II. Local newspapers or specialized journals when it is proven that the data subjects reside in a particular federative entity or are part of a particular activity;

III. Web site of the data controller;

IV. On a hyperlink on an web site of the Institute, set up for this purposes, when the data controller does not have its own web site;

V. Informational posters;

VI. Information spots on the radio, or

VII. Other alternative mass communication media.

Quality Principle

Article 36. The personal data processed by the data controller will meet the principle of quality when they are exact, complete, pertinent, correct, and up-to-date as required to comply with the purpose for which they are processed.

Personal data are presumed to comply with quality when they are directly provided by the data subject until he declares and proves otherwise, or the data controller has objective evidence contradicting this.

When the personal data were not obtained directly from the data subject, the data controller must take reasonable measures for it to meet the principle of quality in accordance with the type of personal data and the processing conditions.

The data controller must adopt the mechanisms that it considers necessary to ensure that personal data dealt with are exact, complete, pertinent, correct, and up-to-date so that the truth of the data are not altered and the data subject thereby prejudiced by this.

Preservation Periods

Article 37. The preservation periods for personal data may not exceed those necessary to achieve the purposes that justify the processing and shall comply with the law applicable to the subject matter involved and take into account the administrative, accounting, tax, legal, and historical aspects of the information. After the purpose or purposes of processing have been achieved, the data controller must cancel the data in its collection after blocking them for subsequent suppression.

Procedure for Preserving, Blocking, and Suppression of Personal Data

Article 38. Data controllers must establish and document procedures for the preservation, and if necessary, blockage and suppression of personal data, including periods of preservation thereof, in accordance with the previous Article.

Proof of Compliance with Preservation Periods

Article 39. The data controller must show that personal data is preserved, or if applicable, blocked, suppressed, or cancelled in accordance with the periods set out in Article 37 of these Regulations or taking into account a request of the right to cancelation.

Principle of Purpose

Article 40. Personal data may be processed only to comply with the purpose or purposes set out in the privacy notice, as provided in Article 12 of the Law.

For purposes of the previous paragraph, the purpose or purposes set out in the privacy notice shall be determined, something which will be achieved when with clarity, and without giving rise to confusion and in an objective manner, the purpose for which personal data will be processed is specified.

Differentiation of Purposes

Article 41. The data controller shall identify and distinguish in the privacy notice between the purposes that give rise to and are necessary for the legal relationship between the data controller and the data subject from those that are not.

Objection to Processing for Different Purpose

Article 42. The data subject may refuse or revoke his consent, as well as object to the processing of his personal data for purposes different from those that are necessary or that gave rise to the legal relationship between the data controller and the data subject, without this having as a consequence, the termination of the processing for the latter two purposes.

Processing for Different Purpose

Article 43. The data controller may not carry out processing for different purposes that are not compatible or analogous to those for which the personal data was originally collected and which were mentioned in the privacy notice unless:

I. A law or regulation explicitly permits it, or

II. The data controller has obtained consent for the new processing.

Principle of Loyalty

Article 44. The principle of loyalty establishes the obligation to process personal data giving priority to the protection of the interests of the data subject and the reasonable expectation of privacy, as provided in Article 7 of the Law.

Misleading or fraudulent means may not be used to collect and process personal data. It will be considered that the behavior is fraudulent or misleading when:

I. There is fraud, bad faith or negligence in the information provided to the data subject about the processing;

II. The reasonable expectation of privacy of the data subject referred to in Article 7 of the Law is violated, or

III. The purposes were not established in the privacy notice.

Principle of Proportionality
Article 45. Only personal data that are necessary, appropriate, and relevant in connection with the purposes for which they were obtained may be processed.

Principle of Minimization
Article 46. The data controller must make reasonable efforts to limit the personal data processed to the minimum necessary in accordance with the purpose of the processing taking place.

Principle of Accountability
Article 47. Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to protect and be responsible for the processing of personal data found in its custody or in its possession or for those it communicated to a data processor, whether or not the latter is located in Mexico.

To comply with this obligation, the data controller may use standards, best international practices, corporate policies, self-regulation arrangements, or any other mechanism that it determines is adequate for such purpose.

Measures for the Principle of Accountability
Article 48. Pursuant to Article 14 of the Law, the data controller must adopt measures to guarantee the proper processing of personal data, giving priority to the interests of the data subject and the reasonable expectation of privacy.

The measures that may be adopted by the data controller include at least the following:

I. Prepare privacy policies and programs that are binding and enforceable within the organization of the data controller;

II. Implement a program of training, updating, and raising the awareness of personnel about obligations in matters of protection of personal data;

III. Establish an internal supervision and monitoring system, as well as external inspections or audits to verify compliance with privacy policies;

IV. Dedicate resources for the implementation of privacy programs and policies;

V. Implement a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies and business models, as well as to mitigate them;

VI. Periodically review the security policies and programs to determine modifications required;

VII. Establish procedures to receive and respond the questions and complaints of data subjects;

VIII. Have mechanisms to comply with privacy policies and programs, as well as sanctions for a breach thereof;

IX. Establish measures to protect personal data, in other words, a group of technical and administrative actions that will allow the data controller to ensure compliance with the principles and obligations established by the Law and these Regulations, or

X. Establish measures to trace personal data, in other words, actions, measures, and technical procedures that will allow the tracing of personal data while being processed.

Data Processor
Article 49. The data processor is the individual or corporate body, public or private, not a part of the organization of the data controller, that alone or together with others, processes personal data on behalf of a data controller as a result of a legal relationship linking the same and setting out the scope of service to be provided.

Obligations of the Data Processor
Article 50. The data processor shall have the following obligations with respect to the processing carried out on behalf of the data controller:

I. Process personal data only according to the instructions of the data controller;

II. Not to process personal data for a purpose other than as instructed by the data controller;

III. Implement the security measures required by the Law, these Regulations, and other applicable laws and regulations;

IV. Maintain confidentiality regarding the personal data subject to processing;

V. Eliminate personal data that were processed after the legal relationship with the data controller is concluded or upon instructions of the data controller, provided there is no legal requirement for the preservation of the personal data, and

VI. Not to transfer personal data unless the data controller so determines, the communication arises from subcontracting, or if so required by a competent authority.

The agreements between the data controller and data processor related to the processing of personal data must be in accordance with the corresponding privacy notice.

Relationship between the Data Controller and Data Processor

Article 51. The relationship between the data controller and data processor must be established by contract or other legal instrument decided upon by the data controller and that permits its existence, scope, and contents to be proven.

Processing of Personal Data in Cloud Computing

Article 52. For the processing of personal data in services, applications, and infrastructure in what is called "cloud computing," in which the data controller adheres to the same by general contractual conditions or clauses, such services may only be used when the provider:

I. Complies at least with the following:

a) Has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;

b) Makes transparent subcontracting that involves information about the service which is provided;

c) Abstains from including conditions in providing the service that authorize or permits it to assume the ownership of the information about which the service is provided, and

d) Maintains confidentiality with respect to the personal data about which it provides the service, and

II. Has mechanisms at least for:

a) Disclosing changes in its privacy policies or conditions of the service it provides;

b) Permitting the data controller to limit the type of processing of personal data about which it provides the service;

c) Establishing and maintaining adequate security measures to protect the personal data about which it provides the service;

d) Ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it, and

e) Impeding access to personal data by those who do not have proper access or in the event of a request duly made by a competent authority, so inform the data controller.

In any case, the data controller may not use services that do not ensure the proper protection of personal data.

For purposes of these Regulations, cloud computing shall mean the model for the external provision of computer services on demand that involves the supply of infrastructure, platform, or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared.

Regulatory agencies, within the scope of their authority, and assisting the Institute, shall issue guidelines for the proper processing of personal data in what is called "cloud computing."

Transmission of Personal Data

Article 53. National and international transmissions of personal data between a data controller and a data processor need not be informed to the data subject or his consent obtained.

The data processor shall be considered as a data controller, together with its own obligations, when it:

I. Uses the personal data for a purpose different from that authorized by the data controller, or

II. Makes a transfer without complying with the instructions of the data controller.

The data processor will not be held responsible when, at the express indication of the data controller, it transmits the personal data to another data processor designated by the latter, to which it had entrusted the performance of a service, or transfers the personal data to another data controller pursuant to these Regulations.

Subcontracting Services

Article 54. Any subcontracting of services by the data processor implying the processing of personal data must be authorized by the data controller and shall be made in the name and on behalf of the latter.

After obtaining authorization, the data processor must formalize the relationship with the subcontractor by contract or other instrument that permits its existence, scope, and contents to be proven.

The subcontracted individual or corporate body will assume the same obligations that are established for the data processor under the Law, these Regulations, and other applicable laws and regulations.

The data processor shall have the obligation of proving that the subcontracting was done with the authorization of the data controller.

Subcontracting Authorization
Article 55. When the contract or legal instruments that have formalized the relationship between the data controller and the data processor contemplates that the latter may subcontract services, the authorization referred to in the previous Article will be understood to be given through the stipulations in those.

If subcontracting is not contemplated in the contract or legal instruments to which the previous paragraph refers, the data processor must obtain authorization from the data controller prior to subcontracting.

In both cases, the provisions of the previous article must be observed.

Section II
Sensitive Personal Data

Situations Giving Rise to the Creation of Sensitive Personal Databases
Article 56. Pursuant to Article 9, second paragraph, of the Law, databases containing sensitive personal data may be created only when:

I. The law so requires;

II. It is justified under Article 4 of the Law, or

III. The data controller requires it for legitimate, concrete purposes in accordance with its explicit activities or purposes.

Chapter III
Security Measures for Processing Personal Data

Scope
Article 57. The data controller, and as applicable, the data processor, must establish and maintain administrative, physical, and if applicable technical, security measures for the protection of personal data pursuant to the Law and this Chapter, regardless of the processing system. For the purposes of this Chapter, security measures mean security control or group of controls to protect personal data.

The above is without prejudice to the laws and regulations in force with respect to security issued by the competent authorities in the corresponding sector when they contemplate greater protection for data subjects than that provided in the Law and these Regulations.

Reduction in Penalties
Article 58. Pursuant to Article 65 (III) of the Law, whenever there is a breach of personal data security, the Institute may take into consideration compliance with its recommendations in determining a reduction in a penalty.

Security Measures
Article 59. To establish and ensure effective security measures, the data controller may take its own security measures or may contract these to an individual or corporate body.

Factors to Determine Security Measures
Article 60. The data controller shall determine the security measures applicable to personal data, taking into account the following factors:

I. The inherent risk by type of personal data;

II. The sensitivity of the personal data processed;

III. Technological development, and

IV. The possible consequences of a violation for the data subjects.

In addition, the data controller shall try to take the following factors into account:

I. The number of data subjects;

II. The vulnerabilities previously encountered in the processing systems;

III. The risk as a result of the potential quantitative or qualitative value that the personal data may have to an unauthorized third party having possession of the data, and

IV. Other factors that may have an impact upon the level of risk or which result from other laws or regulations applicable to the data controller.

Actions to Take for the Security of Personal Data
Article 61. In order to establish and maintain the security of personal data, the data controller must take into account the following actions:

I. Prepare an inventory of personal data and processing systems;

II. Determine the duties and obligations of those who process personal data;

III. Have a risk analysis of personal data consisting of identifying dangers and estimating the risks to the personal data;

IV. Establish the security measures applicable to personal data and identify those implemented effectively;

V. Analyze the gap between existing security measures and those missing that are necessary for the protection of personal data;

VI. Prepare a work plan for the implementation of the missing security measures arising from the gap analysis;

VII. Carry out reviews and audits;

VIII. Train personnel who process personal data, and

IX. Keep a record of personal data storage media.

The data controller shall prepare a document setting out security measures arising from the previous paragraphs.

Updating Security Measures

Article 62. Data controllers must update the document setting out security measures when the following events occur:

I. Modifications to the security measures or processes are made for their continuous improvement, arising from revisions of the security policy of the data controller;

II. Substantial modifications are made in the processing arising from a change in the level of risk;

III. Processing systems are violated, as provided in Article 20 of the Law and Article 63 of these Regulations, or

IV. There is an impact upon the personal data other than the above.

In the case of sensitive personal data, the data controller shall review, and if necessary update the security document once a year.

Security Breaches

Article 63. Breaches of the security of personal data which occur in each processing phase are:

I. Loss or unauthorized destruction;

II. Theft, misplacement or unauthorized copying;

III. Unauthorized use, access or processing, or

IV. Unauthorized damage, alteration or modification.

Notification of Security Breaches

Article 64. The data controller must inform the data subject, without delay, of breaches that significantly prejudice the property or non-pecuniary rights of the data subjects upon confirming the breach and having taken action to trigger an exhaustive review of the magnitude of the breach so that the prejudiced data subjects may take the appropriate measures.

Minimum Information for Data Subject in the Event of Security Breaches

Article 65. The data controller must inform the data subject of at least the following:

I. The nature of the breach;

II. The personal data compromised;

III. Recommendations to the data subject concerning measures that the latter can adopt to protect his interests;

IV. Corrective actions implemented immediately, and

V. The means by which he may obtain more information in this regard.

Corrective Measures in the Event of Security Breaches

Article 66. In case of a breach of the personal data, the data controller must analyze the causes of its occurrence and implement the corrective, preventive and improvement steps to make the security measures adequate in order to avoid a repetition of the breach.

Chapter IV
Transfers of Personal Data
Section I
General Provisions

Scope

Article 67. A transfer refers to the communication of personal data to a person other than the data subject, data controller or data processor, within or outside Mexico.

Conditions for a Transfer

Article 68. Any transfer of personal data, whether national or international, is subject to the consent of the data subject, with the exceptions provided in Article 37 of the Law; the data subject must be so informed by a privacy notice and the transfer be limited to the purposes that justify it.

Proof of Compliance with Transfer Obligations

Article 69. For purposes of demonstrating that the transfer, whether national or international, took place in accordance with the Law and these Regulations, the burden of proof in all cases rests upon the data controller that made the transfer and on the receiver of the personal data.

Transfers within the Data Controller's Group

Article 70. In the case of transfers of personal data among holding companies, subsidiaries, or affiliates under the common control of the same group as that of the data controller, or to a parent company or to any company belonging to the same group as that of the data controller, the mechanism to ensure that the receiver of the personal data complies with the provisions of the Law, these Regulations, and other applicable laws and regulations, may be the existence of internal rules to protect personal data whose observance is obligatory, provided that these comply with the requirements of the Law, these Regulations, and other applicable laws and regulations.

Section II
National Transfers

Specific Conditions Applicable to National Transfers

Article 71. To carry out a transfer of persona data within Mexico, it shall be necessary for the data controller to comply with the provisions of Article 36 of the Law and Article 68 of these Regulations.

Receiver of Personal Data

Article 72. The receiver of personal data will be subject to the Law and these Regulations as a data controller and shall deal with personal data in accordance with that agreed upon in the privacy notice communicated to it by the transferring data controller.

Formalization of National Transfers

Article 73. A transfer shall be formalized by a mechanism that allows it to be shown that the transferring data controller communicated to the receiving data controller the conditions under which the data subject consented to the processing of his personal data.

Section III
International Transfers

Specific Conditions Applicable to International Transfers

Article 74. Without prejudice to the provisions of Article 37 of the Law, international transfers of personal data will be possible when the receiver of the personal data assumes the same obligations as those of the data controller transferring the personal data.

Formalization of International Transfers

Article 75. For such purposes, a data controller that transfers personal data may use contracts and other legal instruments which contain at least the same obligations as those to which the data controller transferring personal data is subject, as well as the conditions under which the data subject consented to the processing of his personal data.

Opinion of the Institute Concerning Transfers

Article 76. Data controllers, if considered necessary, may request the opinion of the Institute as to whether an international transfer that they are carrying out complies with the Law and these Regulations.

Chapter V
Coordination among Authorities

Issuing Secondary Regulations

Article 77. When the competent government department or agency, responding to the needs of which it has become aware in the area it regulates, determines the need to regulate the processing of personal data held by private parties, within the ambit of its jurisdiction it may issue or modify specific regulations, in cooperation with the Institute.

Furthermore, when the Institute, as a consequence of the performance of its duties, becomes aware of the need to issue or modify specific regulations to regulate the processing of personal data in a certain sector or activity, it may propose to the competent department or agency the preparation of a preliminary draft.

Coordination Mechanisms

Article 78. For the preparation, issuance, and publication of the regulation referred to in Article 40 of the Law, the department or agency and the Institute shall establish the appropriate coordination mechanisms.

In all cases, the department or agency and the Institute, within their respective jurisdictions, shall determine the provisions of the regulation of the processing of personal data in the corresponding sector or activity.

Chapter VII
Binding Self-Regulation

Scope of Self-Regulation

Article 79. Pursuant to Article 44 of the Law, individuals or corporate bodies may agree among themselves or with civil or government organizations, national or foreign, on binding self-regulation arrangements in matters of personal data protection, complementing the provisions of the Law, these Regulations, and the regulations issued by departments or agencies in this matter and within their jurisdiction. Furthermore, through such arrangements, the data controller may prove to the Institute compliance with the obligations set forth in said regulations.

The above is in order to harmonize the processing carried out by those who become bound by the arrangements and facilitate the exercise of the rights of the data subjects.

Specific Objectives of Self-Regulation

Article 80. Self-regulation arrangements may be codes of ethics or of good professional practice, seals of confidence, privacy policies, corporate privacy rules, and other mechanisms, that include specific rules or standards and have the following main objectives:

I. Cooperate in compliance with the principle of accountability to which the Law and these Regulations refer;

II. Establish qualitative processes and practices in the field of protection of personal data to supplement the provisions of the Law;

III. Encourage data controllers to establish policies, processes and best practices for compliance with the principles of the protection of personal data, guaranteeing privacy and confidentiality of the personal data in their possession;

IV. Encourage data controllers to voluntarily keep records or certifications regarding compliance with the provisions of the Law, and show to data subjects their commitment to the protection of personal data;

V. Identify data controllers that have privacy policies aligned with the implementation of the principles and rights of the Law, as well as workforce competence for the proper performance of their obligations in this regard;

VI. Facilitate coordination among different self-regulation arrangements recognized internationally;

VII. Facilitate transfers among data controllers that have self-regulation arrangements such as safe harbor;

VIII. Promote the commitment of data controllers to render accounts and adopt internal policies consistent with external criteria, as well as to support mechanisms to implement privacy policies, including tools, transparency, continuous internal supervision, risk assessment, external inspections and remediation systems, and

IX. Channel mechanisms for alternative dispute resolution among data controllers, data subjects and third parties, such as conciliation and mediation.

These arrangements shall be binding upon those who join them; nevertheless, joining will be voluntary.

Incentives for Self-Regulation

Article 81. When a data controller adopts and complies with a self-regulation arrangement, this will be taken into consideration by the institute in deciding upon any reduction in a penalty in the event of a finding of a failure to comply with the Law or these Regulations. In addition, the Institute may decide upon other incentives for the adoption of self-regulation arrangements, as well as mechanisms to facilitate administrative proceedings before it.

Minimum Content of Self-Regulation Arrangements

Article 82. Self-regulation arrangements must take into account the parameters issued by the Ministry, in cooperation with the Institute, for the proper development of this type of self-regulation mechanisms and measures, considering at least the following:

I. The agreed upon arrangement, which may be ethics codes, good professional practice code, seals of confidence, or others that enable data subjects to identify the data controllers committed to protecting their personal data;

II. The extent of the application of the self-regulation arrangements;

III. The procedures or mechanisms to be used to ensure effective personal data protection by those adhering to them, as well as to measure such effectiveness;

IV. Internal and external systems to supervise and monitor;

V. Training programs for those processing personal data;

VI. Mechanisms to facilitate the rights of the data subjects;

VII. Identification of adhering individuals or corporate bodies to make it possible to recognize data controllers that meet the requirements of a given self-regulation arrangement and are committed to the protection of the personal data they hold, and

VIII. Effective corrective measures in case of a failure to comply.

Certification in Personal Data Protection
Article 83. Binding self-regulation arrangements may include the certification of data controllers in the area of protection of personal data.

If a data controller decides to submit to a certification process, this shall be granted by a certifying individual or corporate body apart from the data controller in accordance with the guidelines that the parameters referred to in Article 43(V) set for this purpose.

Accredited Individuals and Corporate Bodies
Article 84. The individuals and corporate bodies who are accredited as certifiers shall have as their principal duty that of certifying that the privacy policies, programs, and procedures voluntarily put into place by data controllers are followed in practice and ensuring proper processing and that the security measures adopted are adequate for their protection. For this purpose, certifiers may adopt mechanisms such as inspections and audits.

The procedure for accrediting the certifiers to which the previous paragraph refers shall be carried out in accordance with the parameters contemplated by Article 43 (V) of the Law. The certifiers shall guarantee their independence and impartiality in granting certificates, as well as compliance with the requirements and guidelines established in such parameters.

Self-Regulation Parameters
Article 85.
The self-regulation parameters referred to in Article 43 (V) of the Law shall contain mechanisms for the accreditation and revocation of the accreditation of individuals and corporate bodies as certifiers, as well as their duties; general guidelines for granting certificates in the protection of personal data, and the procedure for the notification of binding self-regulation arrangements.

Registration of Self-Regulation Arrangements
Article 86. The self-regulation arrangements notice of which has been given in accordance with Article 44, last paragraph, of the Law form part of a registry to be administered by the Institute and in which all those complying with the requirements established in the parameters contemplated in Article 43 (V) of the Law will be included.

Chapter VII
Rights of Personal Data Subjects and their Exercise

Section I
General Provisions

Exercise of Rights
Article 87. The exercise of any of the ARCO rights does not exclude the possibility of exercising another of them nor of this being a requirement to be fulfilled prior to exercising any of these rights.

Restrictions on the Exercise of Rights
Article 88. The exercise of ARCO rights may be restricted for reasons of national security, by laws and regulations of a public policy nature, for reasons of public health and safety, or to protect the rights of third parties in those cases and to the extent contemplated in the laws applicable to the matter, or by a decision of a competent authority well-founded in law and fact.

Persons Authorized to Exercise Rights
Article 89. ARCO rights may be exercised:

I. By the data subject, after proving his identity through the presentation of a copy of his identity document and having shown the original for comparison. Also admissible will be the electronic instruments by which it is possible to reliably identify the data subject and other authentication mechanisms permitted by law or previously established by the data controller. The use of an advanced electronic signature or the electronic instrument replacing it will exempt the data subject from the need to present a copy of the identification document, and

II. By the representative of the data subject, after proving:

a) the identity of the data subject;

b) the identity of the representative, and

c) the existence of the representation by means of a public instrument or simple power of attorney signed before two witnesses or by personal attendance by the data subject.

For the exercise of ARCO rights by minors or by a person under interdiction or without legal capacity, the representation rules of the Federal Civil Code shall apply.

Means to Exercise Rights
Article 90. For the exercise of ARCO rights, the data subject may submit, personally or through a representative, a request to the data controller using the means established in the privacy notice. For such purpose, the data controller shall make available to the data subject remote or local electronic communication means or such others as it considers appropriate.

In addition, the data controller may establish forms, systems, and other simplified methods to help data subjects exercise the ARCO rights and these must be mentioned in the privacy notice.

Customer Service

Article 91. When the data controller has customer service of any type or services for the resolution of claims related to the service rendered or the products offered, the data controller may resolve requests for the exercise of ARCO rights through such services, provided that the periods do not contradict those set out in Article 32 of the Law. In this case, the identity of the data subject is deemed proven by the means established by the data controller for the identification of the data subjects in providing its services or contracting for its products, provided that such means guarantee the identity of the data subject.

Specific Procedure for the Exercise of ARCO Rights

Article 92. When the law applicable to certain databases or processing establishes a specific procedure for requesting the exercise of ARCO rights, the provisions that offer the better guarantees to the data subject and that do not contradict the provisions of the Law, shall apply.

Costs

Article 93. The exercise of ARCO rights shall be simple and free-of-charge and the data subject need only pay expenses for shipping, reproduction, and if applicable, certification of documents, with the exception provided in Article 35, second paragraph, of the Law.

The costs of reproduction may not be higher than the costs of recovery of the corresponding material.

The data controller may not establish, as the only way to present requests to exercise ARCO rights, any service or means with a cost.

Address of the data subject

Article 94. For the purposes of Article 29 (I) of the Law, the request for access must show an address or some other means for notification of the response to the request. If this requirement is not complied with, the data controller shall deem the request not presented, and note this for the record.

Request Registry

Article 95. The data controller must process any request for the exercise of ARCO rights. The period to resolve the request will be calculated from the day it was received by the data controller and it will record the latter on the acknowledgement of receipt given to the data subject.

The period stated shall be interrupted if the data controller requires information from the data subject, as provided in the following Article.

Request for Additional Information

Article 96. If the information provided in the request is insufficient or inaccurate and so cannot be dealt with, or if the documents referred to in Articles 29 (II) and 31 of the Law are not attached, the data controller may ask the data subject once, within five days after receipt of the request, to provide the items or documents necessary for its processing. The data subject shall have ten days to attend to the request, calculated from the day following the date on which it was received. If no response is provided within this period, the request will be considered as not having been submitted.

If the data subject attends to the request for information, the period that the data controller has to respond to the request begins to run from the day following that on which the data subject attends to the request.

If the data controller does not request additional documentation from the data subject to prove his identity or the legal status of his representative, the same shall be considered as proven by the documentation provided by the data subject in his request.

Extension of Periods

Article 97. Pursuant to Article 32, second paragraph of the Law, if the data controller decides to extend the period to respond a request for the exercise of ARCO rights or the period for implementing the response, it must notify the applicant of the justification for the extension, within either of the following periods:

I. In the case of an extension of twenty days to communicate the decision adopted on the admissibility of the request, the justification for the extension must be communicated within the same period, calculated from the date the request is received, or

II. In the case of an extension of fifteen days to enforce the right in question, the justification of the extension must be communicated within the same period, calculated from the date of the notification of the admissibility of the request.

Response from the Data Controller

Article 98. In all cases, the data controller must respond the request for the exercise of ARCO rights that it receives, regardless of whether or not the personal data of the data subject appear in its databases, within the periods established in Article 32 of the Law.

The response from the data controller shall only refer to the personal data that have been specifically mentioned in the request and must be presented in a legible and understandable format with easy access. In case of the use of codes, initials, or keys, the corresponding meanings must be provided.

On Site Access to Personal Data

Article 99. When access to the personal data is on site, the data controller must determine the period during which the data subject may come to consult them, which may not be less than fifteen days. If this period lapses and the data subject has not come to obtain access to his personal data, it will be necessary to submit a new request.

Refusal by Data Controller

Article 100. A data controller must justify its refusal to grant the exercise of ARCO rights and inform the data subject of his right to request the commencement of proceedings for the protection of rights with the Institute.

Section II
Right to Access and its Exercise

Right of Access

Article 101. Pursuant to Article 23 of the Law, the data subject has the right to obtain his personal data from the data controller, as well as information regarding the conditions and general features of the processing.

Means of Complying with Right of Access

Article 102. The obligation to give access will be considered as complied with when the data controller makes available to the data subject personal data on site, respecting the period set out in Article 99 of these Regulations, or by issuing photocopies or using magnetic, optical, sound, visual, or holographic media, as well as other information technologies contemplated in the privacy notice. In all cases access must be granted in formats which are readable and comprehensive to the data subject.

When the data controller considers it appropriate, it may agree with the data subject upon reproduction media for the information different from that mentioned in the privacy notice.

Section III
Right to Rectification and its Exercise

Right to Rectification

Article 103. Pursuant to Article 24 of the Law, the data subject may request, at any time, from the data controller, a rectification or correction of his personal data that are inaccurate or incomplete.

Requirement to Exercise Right to Rectification

Article 104. The request for rectification must indicate to what personal data it refers, as well as the rectification or correction to be made, and must be accompanied by the documentation proving the admissibility of the request. The data controller may offer mechanisms for the benefit of the data subject to facilitate the exercise of this right.

Section IV
Right of Cancellation and its Exercise

Right of Cancellation

Article 105. Pursuant to Article 25 of the Law, cancellation means stopping the processing of personal data by the data controller, starting from their blockage and subsequent supression.

Exercise of Right of Cancellation

Article 106. The data subject may request, at any time, that the data controller cancel the personal data when he considers that they are not being processed in accordance with the principles and duties established by the Law and these Regulations.

The cancellation shall proceed with respect to all personal data of the data subject contained in a database, or only part thereof, as requested.

Blockage

Article 107. If the cancellation is warranted, and without prejudice to the provisions of Article 32 of the Law, the data controller shall:

I. Establish a blockage period only for the purpose of determining possible liability with respect to the processing, up to the legal or contractual limitation period, and so notify the data subject or his representative in the reply to the request for cancellation to be issued within the period of twenty days set out in Article 32 of the Law;

II. Take appropriate security measures for the blockage;

III. Put the blockage into effect within the period of fifteen days set out in Article 32 of the Law, and

IV. After the blockage period, carry out the supression using the security measures previously established by the data controller.

Purpose of Blockage

Article 108. Pursuant to Article 3 (III) of the Law, the blockage has as its purpose the prevention of processing, with the exception of storage, or possible access by any person, unless otherwise established by law.

The blockage period will be until the limitation period or contractual period.

Section V
Right of Objection and its Exercise

Right of Objection

Article 109. Pursuant to Article 27 of the Law, the data subject may, at any time, object to the processing of his personal data or require it to stop when:

I. There is a legitimate reason for doing so and his specific situation so requires, in which case, he must justify the fact that, even though the processing is lawful, it must stop in order to avoid its continuation causing prejudice to the data subject, or

II. He needs to state his objection to the processing of his personal data in order to avoid processing for specific purposes.

The exercise of the right to object may not be exercised in those cases where the processing is necessary to comply with a legal obligation imposed on the data controller.

Exclusion Lists
Article 110. In order to exercise the right to object, data controllers may prepare their own exclusion lists, including in them the data of the people who have stated their refusal to allow the processing of their personal data, either for their products or those of third parties.

Furthermore, data controllers may prepare common exclusion lists by industry or in general.

In both cases, the recording of the data subject in such lists must be free-of-charge and give to the data subject proof of being recorded on the list by the means established by the data controller.

Public Registry of Consumers and Public Registry of Users
Article 111. The Public Register of Consumers referred to in the Federal Law for Consumer Protection and the Public Register of Users referred to in the Law for the Protection and Defense of Users of Financial Services continue in force and will be governed in accordance with the laws referred to and any rules and regulations arising therefrom.

Section VI
Decisions Made without Human Intervention

Processing in Decisions Made without Human Intervention
Article 112. When personal data is used in decision-making without human intervention, the data controller must so inform the data subject.

In addition, the data subject may exercise his right of access in order to discover the personal data used as part of the decision-making process, and as the case may be, his right to rectification, when he considers that some of the personal data used are incorrect or incomplete so that, in accordance with the mechanisms implemented by the data controller for this purpose, he can request a reconsideration of the decision made.

Chapter VIII
Procedure for Protection of Rights

Initiation
Article 113. A request to begin proceedings for the protection of rights must be submitted by the data subject or his representative; either by a document in no particular format, on the forms set by the Institute, or through the system established by the latter, within the period contemplated by Article 45 of the Law.

Both the form and the system must be made available by the Institute on its website and in every one of the authorized offices as determined by it.

When filing a request for the protection of rights, the data subject or his representative must prove his identity or legal status, respectively, pursuant to Article 89 of these Regulations. In the case of the data subject, the latter may also prove his identity by electronic means or by other methods, as provided by applicable law.

The Institute may consider the identity of the data subject or the legal status of the representative as having been proven when the same has already been proven to the data controller upon exercising his ARCO rights.

Methods for Submitting a Request for the Protection of Rights
Article 114. A request for the protection of rights must be filed at the address of the Institute, in its authorized offices, by certified mail with acknowledgment of receipt, or in the system referred to in the previous Article, in the latter case, provided that the person has the certification of electronic identification referred to in Article 69-C of the Federal Law of Administrative Procedures. In any case, the applicant shall be given an acknowledgment of receipt showing in a legally acceptable manner, the date of filing of the request.

When the applicant files his request by electronic means through the system established by the Institute, it will be understood that he accepts that notices will be made to him through the same system or by other electronic media generated by this, unless he indicates a different means for notifications.

When the request is submitted by the data subject or his representative in an office authorized by the Institute, the latter shall certify the proof of identity or, as the case may be, the legal status of the representative, and may send or register by electronic means, both the request and the attached documents. In this case, the request will be taken as having been received, for purposes of the period to which Article 47 of the Law refers, when the Institute, using this same media, generates proof of receipt.

The foregoing is without prejudice to the authorized office sending to the Institute by certified mail, proof of the identity of the data subject or the document proving the legal status of the representative, as well as the request and attached documents, to be included in the file of the matter.

If the data subject sends the request and its attachments by certified mail, the period to which Article 47 of the Law refers shall be calculated from the date stated on the date or receipt stamp of the Institute.

Admissibility
Article 115. Proceedings for the protection of rights may be pursued when the data subject is not satisfied with actions or omissions of the data controller with respect to the exercise of ARCO rights when:

I. The data subject has not received a response from the data controller;

II. The data controller does not give access to the personal data requested or does so in a form that is not understandable;

III. The data controller refuses to make rectifications or corrections to personal data;

IV. The data subject disagrees with the information delivered because he considers that it is incomplete or does not correspond to what was requested or with the cost or type of reproduction;

V. The data controller refuses to cancel the personal data;

VI. The data controller persists in processing in spite of a proper request for objection, or refuses to deal with the request for objection, and

VII. For other reasons that in the opinion of the Institute are admissible under the Law or these Regulations.

Requirements of the Request for Protection of Rights
Article 116. The applicant must attach to his request for protection of rights, pursuant to Article 46 of the Law, the following information and documents:

I. A copy of the request for the exercise of rights in question, as well as a copy of the documents attached for each of the parties, if applicable;

II. The document proving that he acts on his own behalf or in representation of the data subject;

III. The document showing the response of the data controller, if applicable;

IV. If he challenges the failure by the data controller to respond, a copy of the acknowledgement or proof of receipt, by the data controller, of the request for the exercise of rights;

V. The documentary evidence offered to prove his claim;

VI. The document in which he indicates the other evidence offered by him, pursuant to Article 119 of these Regulations, and

VII. Any other document he considers ought to be submitted to the judgment of the Institute.

If the data subject cannot prove that he attended the data controller, either because the latter had refused to receive the request to exercise his ARCO rights or to issue a receipt, he shall bring this to the attention of the Institute by filing a document with it and this shall be given to the data controller for his response, in order to guarantee for the data subject the exercise of his ARCO rights.

Admission Order
Article 117. The Institute shall decide upon the admissibility of the request for protection of rights within a period of no more than ten days after its receipt.

After agreeing upon the admission, the Institute shall communicate this to the applicant, providing a copy to the data controller within a period no more than ten days, attaching all documents filed by the data subject, in order to allow the data controller to provide such response as it considers appropriate within a period of fifteen days from notification, with the obligation to offer the evidence it deems relevant.

Admission or Rejection of Evidence
Article 118. The Institute shall issue a decision to admit or reject the evidence, and if necessary, the evidence will be examined at a hearing, the place or media, date and time of which the parties shall be notified.

Submission of evidence
Article 119. The following may be produced as evidence:

I. Public documents;

II. Private documents;

III. Inspection, provided it is conducted through a competent authority;

IV. Legal presumptions, in its double aspect, legal and human;

V. Experts;

VI. Witness testimony, and

VII. Photographs, websites, documents, and other items provided by science and technology.

In the case of expert evidence or witness testimony, it shall be necessary to specify the facts they will deal with and indicate the name and address of the expert or the witnesses, producing the list of questions or the interrogatories, respectively, to prepare the same. Without these, the evidence will be deemed as not offered.

Conciliation

Article 120. After the request is admitted and without prejudice to the provisions of Article 54 of the Law, the Institute shall order conciliation between the parties according to the following procedure:

I. In the order admitting the request for protection of rights, the Institute shall require the parties to declare, by any means, their willingness to reconcile, within a period of ten days, calculated from the date of notification of the order. The order shall contain a summary of the request for protection of personal data and the response of the data controller, if any, indicating the common elements and the points in dispute.

The conciliation may be held in person, by remote or local electronic communication means, or by any other means as determined by the Institute. In any case, the conciliation shall be recorded using means that prove it took place.

The conciliation stage is waived when the data subject is a minor and any of the rights contemplated in the Law for the Protection of the Rights of Children and Adolescents, related to the Law and these Regulations, were violated, unless the minor has duly accredited legal representation.

II. If the parties accept the possibility of reconciling, the Institute shall indicate the place or means, day and time for the conciliation hearing which shall take place within twenty days after the Institute receives the declaration of the willingness of the parties to reconcile, attempting to reconcile the interests of the data subject and the data controller.

The conciliator may, at any time during the conciliation, require the parties to produce within a maximum period of five days, the evidence that they consider necessary for the conciliation.

The conciliator may suspend the conciliation hearing when he deems it appropriate or at the request of both parties, up to two times. If the hearing is suspended, the conciliator shall state the day and time for its resumption.

A record shall be made of any conciliation hearing, showing its result. If the data controller or the data subject or their respective representatives do not sign the record, this will not affect its validity, it being necessary to state the refusal.

III. If a party does not attend the conciliation hearing and justifies the absence within a period of five days, a second conciliation hearing will be called. If the party does not attend the latter hearing, the proceedings for the protection of rights will continue. If a party fails to attend a conciliation hearing without justification, the proceedings shall continue.

IV. In the absence of agreement in the conciliation hearing, the proceedings for the protection of rights will continue;

V. If reconciliation is achieved at the hearing, the agreement shall be put in writing and will be binding and shall state, if applicable, the period for it to be complied with, and

VI. Compliance with the agreement shall terminate the proceedings for the protection of rights; if not complied with, the Institute shall resume the proceedings.

The period referred to in Article 47 of the Law will be suspended during the period for compliance with the conciliation agreement.

The procedure established in this Article does not prevent the Institute, pursuant to Article 54 of the Law, from seeking conciliation at any time during the procedure for the protection of rights.

Hearing

Article 121. For the purposes of the penultimate paragraph of Article 45 of the Law, the Institute shall determine, if applicable, the place or means, date and time for the hearing, which may be postponed only for justified cause. At the hearing, evidence which by its nature so requires, shall be submitted and a record of this made.

Presentation of Arguments

Article 122. Once an order had been made recording that all evidence had been submitted, the file will be made available to the parties in order for them to formulate arguments, if they wish to do so, within a period of five days, calculated from the notification of the order referred to in this Article. At the end of this period, the proceedings shall be closed and the Institute shall issue its decision within the period established in Article 47 of the Law.

Interested Third Party

Article 123. If no interested third party has been indicated, a third party may appear in the proceedings by filing a document proving his legal standing to intervene in the matter and may do so up to the closing of the proceedings. Such party must attach to his document the document proving his identity when he does not act in his own name and the documentary evidence offered by him.

Lack of Response

Article 124. If the proceedings begin due to a failure of the data controller to respond to a request for the exercise of ARCO rights, the Institute shall send a copy to the data controller so that it may prove, as applicable, that it did respond the request, or in the absence thereof, issue a response and communicate this to the data subject with a copy to the Institute within a period of ten days from the notification.

If the data controller proves that it did respond the request for exercise of rights on time and in the proper form and had so notified the data subject or his representative, the proceedings for the protection of rights shall be dismissed for want of subject matter, in accordance with the provisions of Article 53 (IV) of the Law.

When the data controller proves that it did respond the request for exercise of rights on time and in the proper form and the request for the procedure for the protection of rights was not filed by the data subject within the period established by Law and these Regulations, the proceedings for the protection of rights shall be dismissed for being filed out-of-time, in accordance with the provisions of Article 53 (III) of the Law, as related to Article 52 (V) of the Law.

If the response was issued by the data controller during the proceedings for the protection of rights or was issued outside the period established in Article 32 of the Law, the data controller shall notify the Institute and the data subject of the response so that within a period of fifteen days from notification, the latter may take the appropriate steps to continue the course of the proceedings. If the data subject declares his satisfaction with the response, the proceedings shall be discontinued for want of subject matter.

When the data controller does not comply with the requirement referred to in the first paragraph of this Article, the facts declared by the applicant shall be deemed true and a decision made based on the items found in the file.

Decisions

Article 125. The decisions of the Institute must be complied with within the time period and in the terms stated in them and may be used as the basis for other proceedings contemplated in the Law.

Challenging a Decision

Article 126. Against a decision in the proceedings for the protection of rights, a nullity action may be filed with the Federal Tax and Administrative Justice Tribunal.

Renewal of Proceedings

Article 127. If the request for the protection of rights does not contain any of the causes for admissibility provided in Article 115 of these Regulations, but refers to the inspection proceedings contained in Chapter IX of these Regulations, the proceedings shall be referred to the competent department or agency, within a period of no more than ten days, calculated from the day on which the request was received.

Chapter IX
Inspections

Initiation

Article 128. The Institute, in order to prove compliance with the provisions of the Law or the regulations arising from it, may begin an inspection proceeding, requiring the data controller to provide the necessary documentation or visiting the establishment where the databases are located.

Basis for Admissibility

Article 129. Inspections may be initiated *ex officio* or at the request of a party, upon the instructions of the Plenum of the Institute.

Any person may file a complaint with the Institute about alleged violations of the provisions of the Law and other applicable laws and regulations, provided that they do not fall within the scope of the admissibility of a proceeding for the protection of rights. In this case, the Plenum will determine, upon proper grounds, the admissibility of beginning an inspection proceeding.

Certification

Article 130. While carrying out an inspection, the personnel of the Institute shall have official authority to certify the accuracy of facts related to the transactions they are carrying out.

Requirements of the Complaint

Article 131. The complaint must indicate the following:

I. Name and address of the complainant, or if applicable, the means of receiving notifications;

II. List of the facts on which the complaint is based, and if applicable, the evidence to prove the allegations, and

III. Name and address of the complainant, or if applicable, information on the complainant's location.

The complaint may be filed by the same means as is established for proceedings for the protection of rights.

When the complainant files his complaint by electronic means through the system established by the Institute, it will be understood that he accepts that notifications will be made to him by the same system or through other electronic means generated by this, unless he indicates a different means for notifications.

When the proceedings are carried out as a consequence of a complaint, the Institute shall acknowledge receipt of the complaint and may request the documentation it deems appropriate to carry out the proceedings.

Carrying Out the Inspection

Article 132. The inspection proceedings will have a maximum duration of one hundred and eighty days, calculated from the day the Plenum issues the decision to begin and shall conclude with a decision. The Plenum of the Institute may extend this term once for up to an equal period.

The Institute may carry out various inspections to gather the necessary evidence which inspections shall not take longer than a maximum of ten days for each one. Notice of this period must be given to the data controller or data processor, and if applicable, to the complainant.

Inspections

Article 133. The personnel of the Institute who carry out the inspections must have a legally proper written order bearing the handwritten signature of the competent official of the Institute, specifying the location of the establishment of the data controller or the location of the databases that are the subject of the inspection, the purpose and scope of the visit, and the provisions of the law upon which it is based.

Identification of Personnel

Article 134. When starting the visit, the inspector must show a valid credential with photograph, issued by the Institute, which accredits him to carry out such function, as well as the legally proper written order referred to in the previous Article, a copy of which must be left with the person visited.

Minutes of Inspection

Article 135. The inspection will conclude with the drawing up of the minutes of the inspection which shall indicate the steps taken during the inspection(s). The minutes will be drawn up in the presence of two witnesses proposed by the person with whom the proceedings took place or by the inspector, if the former refuses to propose them.

The minutes issued in duplicate shall be signed by the inspector and by the data controller, data processor, or the person with whom the inspection took place, who may take such steps as are considered appropriate.

If the party inspected refuses to sign the minutes, this circumstance shall be expressly noted therein. The refusal shall not affect the validity of the proceedings or the minutes themselves. The signature of the party inspected will not be considered as agreement with the minutes, only as the receipt thereof.

The party inspected will be given one of the originals of the inspection minutes and the other will be incorporated in the file.

Contents of Minutes of Inspections

Article 136. The inspection minutes shall state:

I. Name of the party inspected;

II. Time, day, month and year when the inspection began and ended;

III. Information clearly identifying the address, such as street, number, area [*colonia*], municipality or district [*delegación*], postal code, and state where the visit took place, as well as the telephone number or other form of communication available for the party inspected;

IV. Number and date of the order authorizing the inspection;

V. Name and title of the person with whom the inspection was conducted;

VI. Name and address of the people who acted as witnesses;

VII. Information concerning the proceedings;

VIII. Declaration of the party inspected, if he wishes to give it, and

IX. Name and signature of those taking part in the inspection, including those of the inspectors. If the party inspected or his legal representative refuses to sign, this will not affect the validity of the minutes, although the inspector shall make a note thereof.

The parties inspected for whom the minutes of the inspection were drawn up may make observations in the minutes and take such steps with respect to the contents of the minutes as they consider legally appropriate or may do so in writing within a period of five days after the date of the minutes.

Decision

Article 137. The inspection proceedings shall conclude with a decision issued by the Plenum of the Institute, establishing, if applicable, the measures to be adopted by the data controller within the period established therein.

The decision of the Plenum may begin the commencement of sanction proceedings or establish a period for them to begin, something which will be carried out pursuant to the provisions of the Law and these Regulations.

Notice of the decision of the Plenum shall be given to the party inspected and to the complainant, if any.

Challenging a Decision

Article 138. Against the decision issued in the inspection proceedings, a nullity action may be filed with the Federal Tax and Administrative Justice Tribunal.

Redirection of Proceedings

Article 139. If the complaint filed does not refer to the proceedings mentioned in this Chapter, but instead to one of the bases for admissibility of proceedings for the protection of rights contained in Article 115 of these Regulations, the matter will be redirected to the appropriate administrative office, within a period not to exceed ten days, calculated from the day on which the request was received.

Chapter X
Procedure for Imposing Sanctions

Beginning

Article 140. For the purposes of Article 61 of the Law, the Institute shall begin proceedings for imposing sanctions when, from proceedings for the protection of rights or from an inspection, presumed violations of the Law capable of being sanctioned under Article 64 of the Law have been seen. Once the proceedings for doing so have been completed, the appropriate decision will be issued.

The proceedings will begin by notification to the presumed violator at the address recorded with the Institute in the proceedings for the protection of rights or inspection.

The notification will be accompanied by a report describing the facts constituting the presumed violation, summoning the presumed violator to provide a response within a period of fifteen days, calculated from the day on which the notification takes effect, and offer the evidence it considers appropriate.

Offer and Submission of Evidence

Article 141. The presumed violator shall make concrete statements in its response concerning each of the facts expressly imputed to him, affirming them, denying them, indicating that he has no knowledge of them because they are not his own or explaining how they occurred, as the case may be; and will submit arguments to deny the violation of which he is charged and the evidence thereof.

If expert or witness testimony evidence is offered, the facts to be dealt with must be specified and the names and addresses of the expert or witnesses must be stated, attaching the list of questions or interrogatories, respectively, needed to prepare the same. Without these indications, the evidence shall be deemed as not offered.

Admission and Rejection of Evidence

Article 142. Concerning the offer of evidence by the presumed violator, a decision must be made admitting or rejecting the same, and evidence will then be submitted.

If necessary, the place, date and time will be established for the submission of evidence, which by its nature, requires this. A record of the hearing and submission of evidence shall be prepared.

Closing of the Proceedings and Decision

Article 143. After the submission of evidence, if applicable, the presumed violator shall be notified that he has five days to submit arguments, calculated from the day on which the notification takes effect. At the end of this period, the proceedings will be closed and the decision of the Institute shall be issued within a period not exceeding fifty days from the beginning of the proceedings.

In justified cases, the Plenum of the Institute may extend once, for up to a period equal to the period of fifty days referred to in the previous paragraph.

Challenging a Decision

Article 144. Against the decision in the proceedings for imposing sanctions, a nullity action may be filed with the Federal Tax and Administrative Justice Tribunal.

Transitional Provisions

First. These Regulations enter into force the day after their publication in the Federal Official Gazette.

Second. Any processing governed by the Law and these Regulations carried out after the date of the Law enters into force must be in compliance with the provisions of the same, regardless of the fact that the personal data may have been obtained or the database may have been made or created before the entry into force of the Law. It shall not be necessary to obtain the consent of the data subjects for personal data obtained prior to the entry into force of the Law, provided that it complies with the following paragraph.

Data controllers that have collected personal data before the entry of the Law into force and that continue processing the same shall make a privacy notice available to the data subjects or, as the case may be, use any of the compensatory measures, as required, in accordance with the provisions of Article 18 of the Law and Articles 32, 33, 34, and 35 of these Regulations.

A data subject may exercise his ARCO rights with respect to the processing of which he is informed in the privacy notice or the corresponding compensatory measure.

Third. The general guidelines for the use of compensatory measures to which Article 32 of these Regulations refer shall be published by the Institute no later than three months after the date these Regulations enter into force.

Fourth. Data controllers shall comply with the provisions of Chapter III of these Regulations no later than eighteen months after the same enters into force.

Fifth. The Ministry, in cooperation with the Institute, shall issue the parameters to which Articles 82, 83, 84, 85, and 86 of these Regulations refer within six months of their entry into force.

Given at the Office of the President, Mexico City, Federal District, on the 19th day of December, 2011. Filipe de Jesus Calderon Hinojasa. Initials. The Secretary of the Economy, Bruno Francisco Ferrari Garcia de Alba. Initials