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

I, FELIPE DE JESÚS CALDERÓN HINOJOSA, President of the United Mexican States, in exercise of the power vested in me by article 89, section I of the Political Constitution of the United Mexican States, pursuant to article 34 of the Organic Law of the Federal Public Administration and article 3, section XIII and Transitory Article Two of the Federal Law on the Protection of Personal Data in the Possession of Individuals, see fit to issue the following:

REGULATION OF THE FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA IN THE POSSESSION OF INDIVIDUALS

Chapter I
General Provisions

Article 1. The purpose of this law is to regulate the provisions of the Federal Law on the Protection of Personal Data in the Possession of Individuals.

The provisions of the Federal Law on the Protection of Personal Data in the Possession of Individuals and of this Regulation will apply without prejudice to the international treaties concluded and ratified by Mexico.

Scope
Article 2. This Regulation will apply to the processing of personal data found on physical and/or electronic media.

In accordance with the provisions of article 3, section II of the Federal Law on the Protection of Personal Data in the Possession of Individuals, databases will be understood as any ordered set of personal data that allow identifying individuals or making them identifiable, as well as the access to personal data according to specific criteria, regardless of the form or method of their creation, type of medium, processing, storage, organization and access.

Pursuant to article 3, section V of the Federal Law on the Protection of Personal Data in the Possession of Individuals, personal data may be any numerical, alphabetical, graphic, photographic, acoustic or other information, concerning an identified or identifiable individual.

Article 3. This Regulation will be binding for any personal data processing when:

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

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

III. The data controller is not established in Mexican territory but is subject to Mexican laws as a consequence of the execution of a contract or in the terms of international law, and

IV. The data controller is not established in Mexican territory and uses, in the processing of personal data, means located in said territory, except if such means are used only for transit purposes. In this case, the data controller must designate a representative established in Mexican territory.

When the data controller is not located in Mexican territory, but the data processor is, the latter will be subject to the provisions related to the security measures contained in Chapter III of this Regulation.

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

In case of legal persons, the establishment will mean the location of the main administration of the business; in case of legal persons residing abroad, the location of the main administration of the business in Mexican territory, or in the absence thereof, that designated by them or any stable installation that allows actual or real performance of an activity.

Article 4. Pursuant to article 2, section II of the Federal Law on the Protection of Personal Data in the Possession of Individuals, processing of personal data means that carried out by individuals exclusively for personal and household use, without purposes of commercial disclosure or use, i.e. that referring to activities within the realm of the private or family life of the individuals.

Definitions

Article 5. In addition to the definitions established in article 3 of the Federal Law on the Protection of Personal Data in the Possession of individuals, for the purposes of this Regulation, the following definitions will apply:

I. **Support:** Coordination at the administrative level for the joint issuance of secondary regulations and other acts between departments, the Secretariat and the Institute, according to their respective functions, in the terms set forth in Chapter VI of the Law;

II. **Departments:** Those indicated in article 26 of the Organic Law of the Federal Public Administration, as well as the regulatory authorities referred to in Chapter VI of the Law;

III. **ARCO rights**: Are the rights of access, correction, cancellation and objection;

IV. **Digital environment**: Is the environment made up of the assembly of hardware, software, networks, applications and services of the information society that allow for the exchange or computerized or digitalized processing of data;

V. **Exclusion list**: Database intended to record free of charge the refusal of the data subject concerning the processing of his personal data for commercial prospecting and/or offering and promoting goods, products and services;

VI. **Verbal medium**: Medium that allows proving the existence of a manifestation through speech;

VII. **Identifiable individual**: Any individual whose identity can be determined, directly or indirectly, by any information referring to his physical, physiological, psychological, economic, cultural or social features. An individual will not be deemed identifiable if these proportionate efforts are necessary to do so;

VIII. **Electronic medium:** Storage medium which can be accessed only through the use of a device with electronic circuits that processes its content in order to examine, modify or store the personal data, including microfilms;

IX. **Physical medium**: 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

X. **Transmission:** Processing of personal data implying the communication thereof in or out of the Mexican territory when the purpose is to carry out processing by the data processor on behalf of the data controller.

Public access source

Article 6. For the purposes of article 3, section X of the Law, only the following will have the character of public access source, regardless of the medium through which access is gained:

I. Telephone directories in the terms provided in specific regulations;

II. Official newspapers, gazettes and/or bulletins, and

III. Social communication media, such as television, press, radio, inter alia.

Remote or local media of electronic, optical and other technology communication will not have the character of public access source, unless the

communications or access carried out by said media are included in any of the cases provided in the previous sections.

For the cases listed in this article to be considered public access sources, it will be necessary to be able to be consulted by any person not prevented by a limitative rule, or without other requirements than, if applicable, the payment of a price, fee or rate.

Obtaining personal data from a public access source does not exempt their processing from complying with the provisions of the Law, the Regulation and other provisions in the matter.

Third party in processing

Article 7. For the purposes of article 3, section XVI of the Law, the third party will also be considered the national or foreign individual or legal person other than the data subject, data controller, data processor and the persons authorized to process personal data under the direct authority of the data controller or data processor.

Article 8. The persons making up a group acting without legal identity and processing personal data for their own specific purposes will also be deemed data controllers, data processors or third parties, as the case may be.

Alternate system

Article 9. In the procedures for the exercise of ARCO rights, the Federal Code of Civil Procedure will alternatively apply in the aspects not provided by the Law and this Regulation. Concerning the procedures carried out by the Institute, the Federal Law of Administrative Procedure will apply alternatively and, in the aspects not provided therein, the Federal Code of Civil Procedure.

Chapter II
Principles of Protection of Personal Data

Section I
Principles

Principles of Data Protection

Article 10. Pursuant to article 6 of the Law, the following constitute the governing principles of protection of personal data in the possession of individuals:

I. Legitimacy;
II. Consent;
III. Information;
IV. Quality;

V. Purpose;
VI. Loyalty;
VII. Proportionality and
VIII. Responsibility.

Principle of legitimacy
Article 11. The processing of personal data must follow and comply with the provisions of Mexican laws and international law.

Principle of consent
Article 12. For the processing of personal data, the data controller must obtain the prior consent of the data subject, unless it is not required under article 10 of the Law.

The consent gives the owner of the personal data, as a manifestation of will, the power to decide on the processing thereof, which may be express or tacit, pursuant to articles 8 and 9 of the Law and this Regulation.

In any case, the consent of the data subject must be:

I. Free: without error, bad faith, violence or fraud that may affect the manifestation of will of the data subject;
II. Specific: refers to one or several explicit, determined and legitimate purposes that justify the processing;
III. Informed: the data subject must previously know about the processing to be done on his personal data and the consequences of granting his consent, and
IV. Unequivocal: there must be elements that unquestionably demonstrate that it was granted.

Obtaining the consent
Article 13. The request for consent must refer to an explicit, determined and legitimate purpose or purposes.

The data controller must facilitate a simple, free-of-charge medium for the data subject to declare his consent or refusal of the processing of the data.

Tacit consent
Article 14. Unless the Law required the express consent of the data subject, the tacit consent will be valid as a general rule, pursuant to articles 12 and 13 of this Regulation.

For the purposes of article 8, paragraph three of the Law, the data controller has the tacit consent of the data subject, provided it made available to him the corresponding

privacy notice, and as long as the latter does not declare that he refuses the processing of his personal data.

When the data subject has refused his consent for the processing of his personal data for certain purposes, the tacit consent will not apply to such purposes unless the data subject so requests afterwards.

Express consent

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

I. It is required by a law;
II. In the case of financial or assets data;
III. In the case of sensitive data;
IV. It is requested by the data controller to prove it, or
V. It is so agreed by the data subject and the data controller.

Verbal consent

Article 16. It is considered that express consent was given verbally when it is given to the data controller directly, by telephone, be it fixed or mobile or by videoconference, among other technologies, provided that such circumstance may be proven by the data controller.

Written consent

Article 17. It will be considered that the express consent was given in writing when it appears in a document with the autographed signature of the data subject. In case of digital environment or the Internet, electronic signature may be used, as well as any mechanism or procedure that has the effect of identifying the data subject, as well as the devices or media that the data controller makes available to the data subject to declare his consent through data messages.

Withdrawal of consent

Article 18. At any time, the data subject may revoke his consent for the processing of his personal data by exercising the rights of cancellation or opposition, depending on whether he wants to revoke consent for the processing of his personal data in possession of a data controller or for certain purposes, provided he is not prevented by a legal provision.

Article 19. In case of refusal by the data controller to stop the processing of the personal data in case of withdrawal of consent, the data subject may file with the Institute the request for the protection of rights referred to in Chapter VIII of this Regulation.

Principle of information

Article 20. The data controller must communicate to the data subject the information related to the existence and main characteristics of the processing to which his personal data will be submitted, through the privacy notice, pursuant to the Law and this Regulation.

Characteristics of the privacy notice

Article 21. The privacy notice must be characterized by being simple, with the necessary information, written in a clear and understandable language, and with a structure and design to facilitate its understanding.

Distribution means

Article 22. For the distribution of the privacy notices, the data controller may use physical forms, electronic forms, verbal means or any other technology, provided it guarantees and complies with the duty of informing the data subject.

Elements of the privacy notice

Article 23. The privacy notice must contain the elements referred to in articles 8, 15, 16 and 36 of the Law, as well as those established in the guidelines referred to in article 43, section III of the Law.

Article 24. In the terms of article 17 of the Law, when the personal data are obtained directly from the data subject, he 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 for the data subject to be aware of the privacy notice.

The immediate distribution of the above information does not exempt the data controller from the obligation to provide mechanisms for the data subject to know the content of the privacy notice, pursuant to article 23 of this Regulation.

Article 25. The purposes of the personal data processing referred to in section II of article 16 of the Law must include those concerning processing for marketing, advertising and/or commercial prospecting purposes.

The above is without prejudice to the current provisions in the matter, when they contemplate higher protection for the data subject, concerning the personal data, than that provided in the Law and this Regulation.

Duty of the data controller to prove that it made the privacy notice available

Article 26. The data controller must keep the form of privacy notice used by it to comply with the duty to inform, as long as personal data are processed according to it and the obligations arising from it continue. For the storage of the form, the data controller may use computer, electronic media or any other technology.

Compensatory measures

Article 27. Pursuant to paragraph three of article 18 of the Law, when it is impossible to communicate the privacy notice to the data subject or it requires disproportionate efforts given the number of data subjects or the old age of the data, the data controller may implement compensatory measures of mass communication according to the categories authorized by the Institute under which it is possible to use the compensatory measures established in the following article.

The cases not included in the categories authorized by the Institute will require the authorization of the latter, prior to the implementation of the compensatory measure, which will have a term of ten days after the receipt of the compensatory measure request from the data controller, to issue the corresponding resolution.

If the Institute does not resolve within the established term, the request will be deemed authorized.

Article 28. Mass communication compensatory measures must contain the data provided in article 24 of this Regulation and may be the following, inter alia:

I. Publication of the privacy notice in a newspaper with national circulation;
II. Publication of the privacy notice in local newspaper or specialized journal when it is proven that the owners of the personal data reside in a certain federative entity or belong to a certain activity;
III. Publication of the privacy notice on a website of the data controller;
IV. Publication of the privacy notice in a hyperlink or hotlink on a website produced for this purpose by the Secretariat or the Institute, when the data controller does not have its own website;
V. Publication of the privacy notice using posters;
VI. Distribution of the privacy notice in information ads on the radio, or
VII. Other alternative mass communication media.

Quality principle

Article 29. The personal data processed by the data controller will meet the principle of quality when they are pertinent and correct, i.e. when they are exact and kept complete and updated, as required for the achievement of the purpose for which they are processed.

The personal data are presumed correct when they are directly provided by the data subject until he declares and proves otherwise, or the data controller has objective evidence contradicting them.

When the personal data were not obtained from the data subject, the data controller must take reasonable measures for them to meet the principle of quality, as long as the processing lasts.

The data controller must adopt the necessary mechanisms for the update of the personal data depending on their nature.

Preservation terms

Article 30. The preservation terms of the personal data may not exceed those necessary to achieve the purposes that justify the processing. 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.

Article 31. The data controllers must document the procedures for the preservation and, if necessary, blockage and suppression of the data, including the periods of preservation thereof, according to the provisions applicable to the matter in question, taking into account the administrative, accounting, tax, legal and historical aspects of the information.

Principle of purpose

Article 32. The personal data may be processed only in connection with certain explicit and legitimate purposes for which they were obtained. The data controller must indicate clearly and concretely in the privacy notice the purpose or purposes of processing.

It will be understood that the purpose of processing is determined when it concretely specifies the processing of personal data, and legitimate when it does not violate any legal provision.

Article 33. The data controller will identify the purposes that originated the processing from those that are not indispensible for it in the privacy notice.

Article 34. The data controller may not engage in processing for purposes that are not compatible or similar to those for which the personal data were originally collected and which were mentioned in the privacy notice.

For the processing of the data with different purposes, it will be necessary for a law to explicitly require it or for the data controller to have the consent of the data subject for the new processing, according to the Law and this Regulation.

Processing with historical, statistical or scientific purposes

Article 35. For the effects provided in the previous article, the processing with statistical, historical or scientific purposes will not be deemed incompatible if the data were previously dissociated.

For processing with historical or scientific purposes in which it is not possible to previously dissociate the personal data, the data controller must request the authorization of the Institute according to the provisions to be issued for this purpose. The Institute may request the opinion of the authority competent in the matter in question in order to establish the existence of historical or scientific values or, in the absence thereof, the opinion of its experts.

Principle of loyalty

Article 36. The principle of loyalty establishes the obligation to process the personal data privileging the protection of the interests of the data subject and the reasonable expectation of privacy, in the terms of article 7 of the Law.

Misleading or fraudulent means may not be used under any circumstances 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 on the processing of the personal data, or
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 37. Only the personal data that are necessary, appropriate, relevant and non-excessive in connection with the purposes for which they were obtained may be processed.

Article 38. The data controller must make reasonable efforts to limit the personal data processed to the minimum necessary.

Principle of responsibility

Article 39. Pursuant to articles 6 and 14 of the Law, the data controller has the obligation to watch over and answer for the processing of personal data found under its custody or in its possession or those it communicated to a data processor, whether or not the latter is located in Mexican territory.

To comply with this obligation, the data controller may use international standards and best practices, as well as self-regulation arrangements.

Article 40. Pursuant to article 14 of the Law, the data controller must adopt measures to guarantee due processing of personal data, privileging the interests of the data subject regarding such processing and the reasonable expectation of privacy.

The measures that may be adopted by the data controller include, indicatively but without limitation thereto, the following:

I. Prepare privacy policies and programs that are binding and enforceable within the organization of the data controller;
II. Implement a program to train and update the personnel about, and make them aware of, the obligations in matters of protection of personal data;
III. Establish an internal supervision and monitoring system, as well as external audits to verify compliance with privacy policies;
IV. Dedicate resources to the implementation of privacy programs and policies;
V. Implement a procedure to cover the risk for the protection of personal data due to 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 the modifications required;
VII. Establish procedures to receive and answer questions and complaints of the data subjects in connection with their personal data, or
VIII. Have mechanisms to comply with the privacy policies and programs, as well as sanctions for the breach thereof.

Relationship between data controller and data processor

Article 41. The relationship between the data controller and data processor must be regulated in a contract and must establish expressly as obligations of the data processor the following:

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

II. Not to process personal data for a purpose other than that appearing in the contract;
III. Implement the required safety measures according to the Law, the Regulation and other applicable provisions;
IV. Maintain confidentiality regarding the personal data subjected to processing;
V. Eliminate personal data processed from the data controller, pursuant to article 44 of this Regulation, after the contractual service is performed by the data processor and/or by the instructions of the data controller, and
VI. Not to transfer personal data except if the data controller so determined, the communication arises from subcontracting, or if so required by the 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.

Article 42. Pursuant to article 3, section IX of the Law, the data processor will be the individual or legal person, public or private, national or foreign, which, alone or together with others, processes personal data on behalf of the data controller, as a consequence of the existence of a legal relationship that connects it to the latter and delimits the scope of its acts for the performance of a service. Data processors may also be the persons who are members of a group acting without legal identity and who process personal data for their own specific purposes.

Article 43. National and international transmissions of personal data between a data controller and a data processor need not be reported to the data subject or obtain his consent.

If the data processor uses the personal data for a different purpose or transfers them to a third party, violating the instructions of the data controller, arising from the stipulations of the contract, it will be deemed data controller for the new processing, with the obligations and responsibilities typical of the latter.

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 a third party pursuant to this Regulation.

Article 44. Pursuant to section V of article 41 of this Regulation, the data processor will not eliminate the personal data when there is a legal provision that requires their preservation.

Article 45. The provider of hosting services for personal databases in the infrastructure of the digital infrastructure will not be deemed the data processor when the data controller uses its platforms or servers without express contract, pursuant to article 41 of this Regulation and it adheres to preexisting services rendered by said provider.

Consequently, the data controller will assume the obligations implied in the storage of the personal data in said platforms or services to avoid their access, reproduction, alteration or elimination without the consent of the data subject.

Subcontracting of services

Article 46. Any subcontracting of services by the data processor implying the processing of personal data must be authorized by the data controller, and will be done in the name and on behalf of the latter.

After obtaining the authorization, the data processor must formalize a contract with the subcontractor, establishing the provisions in sections I to VI of article 41 of this Regulation.

The subcontracted individual or legal person will assume the same obligations established for the data processor under the Law, this Regulation and other applicable provisions.

The obligation to prove that the subcontracting was done with authorization of the data controller will correspond to the data processor.

Article 47. When the contract between the data controller and the data processor provides the subcontracting of services, the authorization referred to in the previous article will be understood to be granted through the stipulations of the contract.

If the subcontracting was not provided in the contract executed between the data controller and the data processor, the latter must obtain the corresponding authorization from the data controller prior to subcontracting.

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

Section II
Sensitive Personal Data

Cases for creation of databases of sensitive personal data

Article 48. Pursuant to article 9, paragraph two of the Law, databases containing sensitive personal data may be created only when:

I. It obeys a legal mandate;
II. It is justified in the terms of article 4 of the Law, or
III. The data controller requires it for legitimate, concrete purposes in accordance with its explicit activities or purposes.

In all cases, the data controller must establish sufficient measures to avoid the discrimination of the data subjects whose sensitive personal data is in its possession and the disclosure of sensitive personal data to unauthorized third parties.

Chapter III
Security Measures in the Processing of Personal Data

Scope
Article 49. The data controller and data processor must establish and maintain administrative, physical, security and, if applicable, technical measures for the protection of the personal data pursuant to the Law and this Chapter, regardless of the processing system. For the purposes of this Chapter, security measures means the security control or group of controls to protect the personal data.

In the event referred to in article 45 of this Regulation, the data controller must make sure that the provider of the corresponding service has appropriate security measures to protect the personal data.

The above is without prejudice to the current provisions in matters of security issued by the competent authorities to the corresponding sector, when they provide greater protection for the personal data subjects than that provided in the Law and this Regulation.

Article 50. Pursuant to article 65, section III of the Law, whenever there is a violation of the security of the personal data, compliance with the recommendations issued by the Institute in matters of security measures will be taken into account to determine the attenuation of the corresponding sanction.

Security function
Article 51. To guarantee the effective establishment and maintenance of the security measures, the data controller will perform the security functions or hire an employee for this purpose.

Security measures
Article 52. The data controller will determine the security measures applicable to the personal data processed by it, taking into account the following factors:

I. The inherent risk by type of personal data;
II. The sensitivity of the personal data processed;
III. The number of data subjects;
IV. The technological development;
V. The possible consequences of a violation for the data subjects;
VI. The vulnerabilities previously occurring in the processing systems;
VII. The value the data may have for an unauthorized third party, and
VIII. Other factors that may impact the risk level or which result from other laws or regulations applicable to the data controller.

For these purposes, the Institute will issue recommendations to identify the security measures based on the previous sections.

Article 53. The Institute will develop and make available to the data controllers, by way of recommendation, a tool to identify the minimum security measures to be applied to the personal data processed.

When there is low risk for the personal data processed, according to the recommendations issued by the Institute, the tool will facilitate the preparation of the security document and the identification of the actions provided in the following article.

Security Document
Article 54. In order to guarantee the security of the personal data, the data controller must take into account the following actions:

I. Prepare an inventory of personal data and processing systems of personal data;
II. Determine the functions and obligations of the persons who process personal data;
III. Conduct a risk analysis of personal data consisting of identifying dangers and estimating the risks for 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 for each type of data and for each processing system;
VI. Prepare a work plan for the implementation of the missing security measures arising from the gap analysis;
VII. Carry out revisions and/or audits;
VIII. Train the personnel who process personal data;
IX. Keep a record of cancellations or destructions of personal data, and

X. Keep a record of the means of storage of the personal data.

The data controller must prepare a security document establishing the actions provided in the previous paragraphs and, if applicable, identifying the people in charge of the security functions.

Updates of the security document

Article 55. The security document must be reviewed and, if applicable, updated when the following events occur:

I. Modifications of the security measures and/or processes are made for their continuous improvement, arising from the revisions of the security policy of the data controller;
II. Substantial modifications are made in the processing of personal data arising from a change in the risk level;
III. The processing systems are violated, as provided in article 20 of the Law and 56 of this Regulation, or
IV. There is an impairment of the personal data other than the above.

In the case of sensitive personal data, the security document must be revised and updated once a year.

Security violations

Article 56. The violations of the security of personal data which occur in each processing phase are:

I. Loss or unauthorized destruction;
II. Theft, misplacement or unauthorized copy;
III. Unauthorized use, access or processing, or
IV. Unauthorized damage, alteration and/or modification.

Notification of security violations

Article 57. The data controller must inform the data subject of the violations that significantly affect the property or moral rights of the data subjects immediately, upon becoming aware of the violation and must have taken action in order to trigger a process of exhaustive review of the magnitude of the violation, so that the affected data subjects may take the corresponding measures.

Article 58. The data controller must inform the data subject of at least the following:

I. The nature of the violation;
II. The personal data compromised;
III. Corrective actions implemented immediately, and

IV. The means by which it may obtain more information in this regard.

Article 59. In case of a violation of the personal data, the data controller must analyze the causes of its occurrence and implement the corrective, preventive and improvement actions to adapt the corresponding security measures, in order to avoid the repetition of the violation.

Chapter IV
Transfers of Personal Data

Article 60. The transfer implies the communication of personal data to a person other than the data subject, data controller or data processor which acts on behalf of the latter, within or outside of the national territory.

Article 61. Any transfer of personal data, be it national or international, is subject to the consent of its data subject and must be communicated to him through the privacy notice, with the exceptions provided in the Law.

Article 62. The transfer of personal data will be legitimate, when it was approved by the data subject, barring the exceptions set forth in the Law, only if it is limited to the purpose that justifies it and is duly documented, pursuant to the following article.

Article 63. The transfer of personal data will be possible when the transferor of the personal data guarantees that the receiver will comply with the provisions of the Law, this Regulation and other applicable regulations, through contractual clauses or other mechanisms providing at least the same obligations which are binding for the data controller who transfers the data and containing the necessary provisions for the protection of personal data.

Chapter V
Coordination between Authorities

Article 64. When the competent department, responding to the needs noticed by it in its sector, determines the need to regulate the processing of personal data in the possession of individuals, it may issue or modify the specific regulations, in cooperation with the Institute.

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

Article 65. For the preparation, issuance and publication of the regulation referred to in article 40 of the Law, the department and the Institute will establish the corresponding coordination mechanisms.

Chapter VII
Binding Self-regulation

Object of self-regulation

Article 66. Pursuant to article 44 of the Law, individuals or legal persons may agree between them 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, this Regulation and the provisions issued by the departments in their development within the scope of their functions. 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 adhere thereto and facilitate the exercise of the rights of the data subjects.

Specific objectives of self-regulation

Article 67. Binding self-regulation will have the following main objectives:

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

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

III. Guarantee assurance and traceability;

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

VI. Promote the commitment of the data controllers to be accountable and adopt internal policies consistent with external criteria, and to support mechanisms to implement privacy policies, including tools, transparency, continuous internal supervision, risk assessment, external inspections and remediation systems; and

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

Article 68. Self-regulation arrangements may translate into ethics or good professional practice codes, trust marks or other mechanisms and will contain specific rules or standards.

When a data controller adopts and maintains a self-regulation arrangement, this circumstance will be taken into account to determine the reduction of the corresponding sanction, in case of breach of the provisions of the Law and this Regulation by the Institute.

These arrangements will be binding on those who adhere to them; however, membership will be voluntary.

Content of self-regulation arrangements

Article 69. Self-regulation arrangements must take into account the parameters issued by the Secretariat, in cooperation with the Institute, for the correct development of this type of self-regulation mechanisms and measures, considering at least the following:

I. The agreed upon arrangement, which may become ethics codes, good professional practice code, trust marks, or others that enables the data subjects to identify the data controllers committed to protecting their personal data;
II. The procedures or mechanisms to be used to measure the efficacy of personal data protection by the members;
III. Mechanisms to facilitate the rights of the data subjects;
IV. Identification of adhering individuals or legal persons, which enables recognizing the controllers that meet the requirements for a given self-regulation arrangement and are committed to the protection of the personal data they hold, and
V. Effective corrective measures in case of breach.

Article 70. The self-regulation parameters referred to in article 43, section V of the Law will contain mechanisms for the accreditation and dismissal of third-party certifiers, as well as their functions and procedure for the notification of binding self-regulation arrangements.

Chapter VII
Rights of the Personal Data subjects and their Exercise

Section I
General Provisions

Persons authorized to exercise the rights

Article 71. ARCO rights will 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 previously agreed upon between the data subject and the data controller. The use of the advanced electronic signature or the electronic instrument replacing it will exempt it from presenting the copy of the identification document, and

II. By the representative of the data subject, after proving the representation by public instrument or letter of power of attorney signed before two witnesses, or declaration on personal appearance of the data subject.

When the request is made by a person other than the data subject, and it is not proven that he acts in representation of the latter, the data controller to which the request was made must deem the request null and void.

Customer service

Article 72. When the data controller has any kind of customer service or in the resolution of claims related to the service rendered or the products offered, the data controller may be given the possibility to resolve requests for the exercise of ARCO rights through such services, provided that the terms do not contradict the provisions of 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 the performance of its services or contracting of its products, provided that such means guarantee the identity of the data subject.

Article 73. The exercise of any of the ARCO rights does not exclude the possibility to exercise any of the others, nor may it constitute a prior requirement for the exercise of any of such rights.

Costs

Article 74. The exercise of the ARCO rights will be simple and free of charge, whereby the data subject must pay only the expenses for shipping, reproduction and, if applicable, certification of documents, with the exception provided in paragraph two of article 35 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 the requests to exercise ARCO rights any means that imply a cost for the data subject.

Restrictions in the exercise of the rights

Article 75. The exercise of the ARCO rights may be restricted for reasons of national security, provisions of public policy, public safety and health or to protect the rights of third parties, in the cases and with the scope provided in the applicable laws in the matter, or by resolution of the competent authority duly grounded and motivated.

Means to exercise the rights

Article 76. For the exercise of ARCO rights, the data controller may use remote or local electronic communication means or others, as it deems pertinent.

The data controllers may prepare forms, systems and other simplified methods to help the data subjects exercise the ARCO rights, which must be reported in the privacy notice.

Article 77. When the laws applicable to certain databases establish a specific procedure to request the exercise of ARCO rights, the provisions that offer higher guarantees to the data subject and do not contradict the provisions of the Law will apply.

Article 78. For the exercise of the ARCO rights, the data subject or his representative may submit the request to the data controller, according to the means established in the privacy notice.

Address of the data subject

Article 79. For the purposes of article 29, section I of the Law, the data subject or his representative must indicate in their request the address or any other means designated to be notified of the answer to the request. If he does not comply with this requirement, the data controller will deem the request not presented, and will note it for the record.

Record of requests

Article 80. The data controller must process any request for the exercise of ARCO rights, provided that the data subject proves receipt thereof by the data controller. The term to resolve the request will start being calculated from the day it was received by the data controller, in which case it will record the request and return an acknowledgement of receipt, showing the date of recording.

Request for additional information

Article 81. If the information provided in the request is insufficient or inaccurate for its resolution, or the documents referred to in articles 29, section 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 produce the elements or documents necessary for its processing. The term to answer, as mentioned in the previous article, will start running as of the time the request is met by the data subject.

If ten days lapse without answer to the request by the data subject, the request will be deemed not presented.

Extension of the terms

Article 82. Pursuant to article 32 of the Law, if the data controller decides to extend the term to answer a request for the exercise of ARCO rights or the term for implementing the answer, it must notify the applicant of the causes that justify the extension, within the following terms:

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

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

Answer from the data controller

Article 83. The answer to the data subject must include all personal data submitted to processing, except if he referred in his request to a processing in particular, to specific personal data or to a category of personal data.

The answer must be presented in a legible and understandable format with easy access. In case of use of codes, initials or keys, the corresponding meanings must be provided.

Article 84. In all cases, the data controller must answer the request sent to it, regardless of whether or not the personal data of the data subject appear in its databases, pursuant to the terms established in article 32 of the Law.

When the 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 term lapses and the

data subject has not come to obtain access to his personal data, he will need to submit a new request.

Article 85. In any case, the data controller must justify its refusal to grant the exercise of ARCO rights by the data subject, and inform the latter of his right to request the beginning of the procedure for the protection of rights with the Institute.

Section II
Right to Access and Its Exercise

Article 86. Pursuant to article 23 of the Law, the data subject or his representative has the right to obtain from the data controller his personal data, as well as information regarding the conditions and general features of the processing, including the data used to make decisions without human assessment intervention.

Article 87. For the exercise of the right of access, the data subject or his representative may choose the reproduction of the information requested in uncertified copies, magnetic media, optical, sound, visual, holographic media, as well as other technologies or media.

The access modalities may be restricted, depending on the configuration or features of the database, provided that the situation is justified to the data subject and alternative ways are offered to facilitate access.

Section III
Right of Correction and Its Exercise

Article 88. Pursuant to article 24 of the Law, the data subject or his representative may request at any time from the data controller to correct his personal data that are inaccurate or incomplete.

Article 89. The request for correction must indicate to what personal data it refers, as well as the correction to be made, and must be accompanied by the documentation proving the admissibility of the request.

Section IV
Right of Cancellation and Its Exercise

Article 90. Pursuant to article 25 of the Law, cancellation implies the cessation of the processing of personal data by the data controller, starting from their blockage and their subsequent elimination.

Article 91. The data subject or his representative may request at any time that the data controller cancel the personal data. The request will be suitable when the processing thereof by the data controller does not meet the principles of proportionality, purpose and quality established by the Law and this Regulation, i.e. when the data processed are inadequate, unnecessary or irrelevant in connection with the purpose for which they were collected; they are used for purposes that are unauthorized or incompatible with the purpose that justified their processing; or the data controller has not eliminated them in spite of the completion of the purpose for which they were collected. Furthermore, the cancellation will apply when the data subject requests the revocation of consent to process all his personal data in possession of the data controller, provided that he is not prevented by a legal provision.

The cancellation will apply to all personal data of the data subject contained in a database, or only part thereof.

Blockage

Article 92. If the cancellation is suitable and without prejudice to the provisions of Article 32 of the Law, the data controller must:

I. Determine a blockage period according to the responsibilities that motivate the processing, as well as the legal or contractual prescription thereof, and communicate it to the data subject or his representative within a term of twenty days from the date it received the request for cancellation;
II. Take appropriate security measures for the blockage, and
III. After the blockage period, make the corresponding elimination under the security measures previously established by the data controller.

Article 93. Pursuant to article 3, section III of the Law, the blockage has as its purpose the prevention of the processing of the personal data or possible access by any person, except for the data subject, unless otherwise established in a legal provision.

The blockage period will be up to the corresponding legal or contractual prescription term.

Section V
Right of Objection and its Exercise

Right of objection

Article 94. Pursuant to article 27 of the Law, the data subject may object to the processing of his personal data or require it to stop when:

I. His specific situation so requires, in which case, he must prove that, even though the treatment is lawful, it must stop in order to avoid its continuation from causing damage to the data subject, or

II. Required to declare his objection or revocation of consent to the processing of his personal data, including before its start, to avoid the processing for specific purposes.

Exclusion lists

Article 95. In order to exercise the right to opposition, data controllers may prepare their own exclusion lists, including in them the data of the persons who refused the processing of their personal data, either for their products or those of third parties.

Furthermore, the data controllers may prepare common exclusion lists by industries or general [lists].

In both cases, the recording of the data subject in said lists must be free of charge, and the data subject must be given means to obtain certainty of said recording.

Article 96. 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 the User of Financial Services, as well as any similar one, constitute exclusion lists in the terms of this Regulation, and will be governed in accordance with the applicable provisions.

Section VI
Decisions without human assessment intervention

Article 97. In case of personal data for decision-making without the intervention of the assessment of an individual, the data controller must inform the data subject about said situation through the privacy notice, as well as of the mechanisms to request reconsideration of such decisions.

Chapter IX
Procedure for the protection of rights

Beginning

Article 98. The request to start the procedure for the protection of rights must be submitted by the data subject or his representative; either by free brief, in the forms determined for this purpose by the

Institute or through the system established by the latter, within the term provided in 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 determined by it.

When filing a request for the protection of rights, the data subject or his representative must prove his identity pursuant to article 71 of this Regulation.

Article 99. The 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 private person has the certification of the electronic identification means referred to in article 69-C of the Federal Law of Administrative Procedure. In any case, the applicant will be given an acknowledgment of receipt showing, reliably, 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 be made to him through said system, unless he indicates a different means for notifications.

The term for the substantiation of this procedure will be calculated pursuant to article 47 of the Law.

Causes for admissibility

Article 100. The procedure for the protection of rights will be admissible against disagreements arising from the exercise of ARCO rights, inter alia, when:

I. The data subject did not receive an answer from the data controller;
II. The data controller does not give access to the personal data requested or does so in an illegible or incomprehensible format;
III. The data controller refuses to make the corrections of the personal data;
IV. The data subject disagrees with the information delivered, because he considered that it is incomplete or does not correspond to that requested or with the cost or modality of reproduction;
V. The data controller refuses to cancel the personal data, either due to the exercise of the right of cancellation or the withdrawal of consent by the data subject, or

VI. The data controller persists in the processing, in spite of the fact that the request for objection was admissible, or refuses to grant the request for objection or the revocation of consent.

Article 101. The applicant must attach to his request, pursuant to article 46 of the Law:

I. Copy of the request for the exercise of rights in question and in case of withdrawal of consent the circumstantial elements thereof, as well as copy of the documents enclosed 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 answer of the data controller, if applicable;
IV. If he challenges the lack of answer of the data controller, he must enclose a copy showing the acknowledgement or proof of receipt of the request for the exercise of rights by the data controller;
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 104 of this Regulation, and
VII. Any other document he deems applicable to submit to the judgment of the Institute.

Article 102. After agreeing on the admission of the request for the protection of rights, the Institute will communicate it to the applicant and the same will be conveyed to the data controller, enclosing all documents produced by the data subject in order to show cause within the term of fifteen days from notification, with the obligation to offer the evidence it deems relevant.

Admission or rejection of evidence
Article 103. The Institute will issue a decision of admission or rejection of the evidence, and if necessary, the evidence will be examined in a hearing, the place or means, date and time of which will be communicated to the parties.

Production of evidence
Article 104. The following may be produced as evidence:

I. Public documentation;
II. Private documentation;
III. Inspection, provided it is conducted through the competent authority;
IV. Photographs, websites, briefs and other elements provided by science and technology, and
V. Presumption evidence, in its double aspect, legal and human.

In case of producing expert evidence, it will be necessary to specify the facts they concern and indicate the name and address of the expert. Without these indications, said evidence will be deemed not produced.

Conciliation

Article 105. After the application is admitted and without prejudice to the provisions of article 54 of the Law, in the first fifteen days, the Institute will issue a decision of conciliation between the parties according to the following procedure:

I. The Institute will require the parties to declare their will to reconcile, presenting to them a summary of the request for protection of personal data and the answer of the data controller, if any, indicating the common elements and the controversial points, and will urge them to reach a settlement protecting the rights of the owner of the personal data.

The conciliation may be held in person, remotely or by local electronic communication means or by any other means determined by the Institute. In any case, the conciliation will be recorded using means that allow proving its existence.

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 Rights of Children and Adolescents, related to the Law and this Regulation, were violated, unless the minor has duly accredited legal representation.

II. If the parties accept the possibility of reconciling, the Institute will indicate the place or means, day and time for a conciliation hearing within five days after the Institute receives the declaration of the will to reconcile of the parties, attempting to reconcile the interests between the data subject and the data controller.

The conciliator may, at any time, request that the parties produce the elements of conviction he deems necessary for conciliation. The parties may produce the evidence they deem necessary to prove the elements of the request of the data subject and the answer of the data controller.

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

Any conciliation hearing will be entered in the respective minutes, showing its result. If the data controller or the data subject or their respective representatives do not sign the minutes, it will not affect its validity, it being necessary to state said refusal.

III. If the data controller does not come to the conciliation hearing and does not justify his absence, he will be deemed in default and will be called to a second conciliation hearing. If he does not come to it, the procedure for the protection of rights will continue. If the data subject does not come, without justification, to the first conciliation hearing, the procedure will continue. In both cases, if there is justified cause, a second conciliation hearing will be scheduled;

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

V. If the conciliation is achieved in the hearing, the agreement must be put in writing and will be binding and, if applicable, will indicate the term for its enforcement, and

VI. The enforcement of the agreement will terminate the procedure for the protection of rights; otherwise, the Institute will resume the procedure.

The term referred to in article 47 of the Law will be suspended during the enforcement period of the conciliation agreement.

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

Hearing

Article 106. For the purposes of the penultimate paragraph of article 45 of the Law, the Institute will determine, if applicable, the place or means, date and time for the hearing, which may be postponed only for justified cause. At said hearing, the evidence which by its nature is so required, will be examined, and the corresponding minutes will be drawn up.

Presentation of arguments

Article 107. Before rendering a decision, the documents will be made available to the parties to formulate arguments, within a term of five days, from the notification of the corresponding decision. At the end of said term, the investigation will be closed and the Institute will issue its decision within the term established in article 47 of the Law.

Interested third party

Article 108. If no interested third party has been indicated, he must appear in the procedure by brief stating legal interest to intervene in the matter, before the closing of the investigation. He must attach to his brief the document proving his identity when he does not act in his own name and the documentary evidence offered by him.

Assumed denial

Article 109. If the procedure starts due to lack of answer from the data controller to a request for exercise of ARCO rights, the Institute will send a copy to the data controller in order to prove, if applicable, that it did answer the request or, in the absence thereof, issue the corresponding answer and communicate it to the data subject with copy to the Institute, within a term of ten days from notification.

If the data controller proves that it did answer the request for exercise of rights in due time and form, and the request for the procedure for the protection of rights was filed by the data subject within the term and with the requirements established by Law and this Regulation, the Institute will ask the data subject to clearly declare the content of his claim concerning the answer of the data controller, within a period of three days from notification. If the data subject declares his agreement with the answer issued by the data controller, the procedure for the protection of rights will be set aside; otherwise the procedure for the protection of rights will continue.

When the data controller proves that it did answer the request for exercise of rights in due time and form and the request for the protection of rights was not filed by the data subject within the term and with the requirements set forth in the Law and this Regulation, the procedure for the protection of rights will be set aside.

If the answer is issued by the data controller during the procedure for the protection of rights or was issued outside the term established in article 32 of the Law, the data controller will communicate said answer to the data subject and to the Institute, so that within a term of fifteen days from notification, it may show cause, in order to continue the course of the procedure. If the data subject declares his agreement with the answer, the procedure will be set aside.

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 will be deemed true, and the decision will be made with the elements found in the file.

Decisions

Article 110. The decisions of the Institute must be enforced within the time period and in the terms indicated in them, and they may set up the beginning of other procedures provided by Law.

Article 111. Against the decision in the procedure for the protection of rights, it is possible to file an appeal for review under the Federal Law of Administrative Procedure or an action for nullity with the Federal Court of Tax and Administrative Justice.

Article 112. If the request for the protection of rights does not contain any of the causes for admissibility provided in article 100 of this Regulation, but refers to the inspection proceedings contained in Chapter IX of this Regulation, the Institute must take the appropriate steps in order to refer, in a simple and expeditious manner, the request of the data subject to the corresponding inspection proceedings.

Chapter X
Inspection proceedings

Beginning

Article 113. The Institute, in order to prove compliance with the provisions of the Law or the regulation arising from it, may start the inspection proceedings, asking the data controller for the necessary documentation and/or making visits to the establishment where the respective databases are located, during business days and business hours.

Article 114. The inspection proceedings will be carried out ex officio or ex parte, by instruction of the Plenum of the Institute.

Any person may complain to the Institute about alleged violations of the principles or provisions of the Law and other applicable regulations, provided that they do not meet the cases of admissibility of the procedure for the protection of rights. In this case, the Plenum will determine, in a grounded and motivated manner, the admissibility of starting the corresponding inspection, as well as the manner in which, if applicable, the complainant will intervene, in light of the legal interest he may have.

Requirements of the complaint

Article 115. The complaint must indicate the following:

I. Name and address of the complainant or, if applicable, data for his location;
II. List of the facts on which he bases his complaint and, if applicable, the elements he has to prove his allegations, and
III. Name of the complainant and address or the means to receive notifications, if applicable.

The complaint may be filed by the same means established for the procedure 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 be made to him by the same system, unless he indicates a different means for notifications.

When the proceedings are carried out as a consequence of the existence of a complaint, the Institute will acknowledge receipt of the complaint and may request the documentation it deems appropriate for the course of the proceedings.

Course of the inspection

Article 116. The inspection proceedings will have a maximum duration of one hundred eighty days from the day the Plenum issued the decision to begin it. The Plenum of the Institute may extend this term once and up to an equal period. This term must be communicated to the data controller or data processor and, if applicable, to the complainant.

Article 117. The personnel of the Institute who carry out the inspection visits must have a grounded and motivated written order with autographed signature of the competent authority of the Institute, specifying the location of the establishment of the data controller, or the location of the databases subject to inspection, the purpose of the visit, the scope it must have and the underlying legal provisions.

Article 118. When starting the visit, the inspector must show his valid credential with photograph, issued by the Institute which accredits him to carry out such function, as well as the express order referred to in the previous article, a copy of which must be left with the person visited.

Article 119. The inspection visits will end with the drawing up of the corresponding minutes which will indicate the steps taken during the inspection visit or visits. 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 refused to propose them.

The minutes issued in duplicate will be signed by the acting inspector and by the data controller, data processor or the person with whom the proceedings took place, who may show cause.

If the party inspected refuses to sign the minutes, this circumstance will be expressly noted therein. The refusal will not affect the validity of the proceedings or of the minutes themselves. The signature of the party inspected will not imply his agreement, only 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.

Article 120. The inspection minutes will indicate:

I. Name, corporate name or style of the party inspected;
II. Time, day, month and year when the visit started and ended;
III. Street, number, town or colonia [colony], telephone number or other form of communication available, municipality or delegation, postal code and federative entity where the visit took place;
IV. Number and date of the commission letter motivating it;
V. Name and title of the person with whom the visit was conducted;
VI. Name and address of the persons who acted as witnesses;
VII. Data concerning the proceedings;
VIII. Declaration of the party inspected, if he wishes to give it, and
IX. Name and signature of the participants in the visit, including those of the inspectors. If the party inspected or his legal representative refuses to sign, it will not affect the validity of the minutes, and the inspector must enter the corresponding note.

The parties inspected for whom inspection minutes were drawn up may make observations in the act of the visit and show cause in connection with the facts contained therein or in writing within the term of five days after the date the minutes were drawn up.

Article 121. When, as a consequence of the inspection proceedings, the Institute makes observations, they will be put in writing and motivated, specifying the facts or omissions known and implying violation of the provisions of the Law or the regulation arising from it.

The data controller will have a term of twenty days from the date following the effective date of the notification of the observations letter to submit evidence in order to deny the facts or omissions entered therein and show cause.

The facts or omissions entered in the observations letter will be deemed approved, if, within the term referred to in the previous paragraph, the data controller does not present elements of proof denying them.

After the examination of the evidence, if applicable, the data controller will be notified that he has a term of five days from the corresponding notification to present arguments. At the end of said term, the investigation will be closed and the

Institute will issue its decision within the term established in article 116 of this Regulation.

Decision

Article 122. The inspection proceedings will end with the decision issued by the Plenum of the Institute, establishing, if applicable, the measures to be adopted by the data controller within the term established therein.

The decision of the Plenum may start the beginning of a sanctioning proceedings or establish a term for its beginning, which will be carried out pursuant to the provisions of the Law and this Regulation.

The determination of the Plenum will be communicated to the party inspected and to the complainant, if applicable.

Means of appeal

Article 123. Against the decision of the inspection proceedings, it is possible to file an appeal for review as established in the Federal Law of Administrative Procedure or an action for nullity with the Federal Court of Tax and Administrative Justice.

Article 124. If the complaint filed does not indicate the proceedings referred to in this chapter, but indicates any of the causes for admissibility of the procedure for the protection of rights contained in article 100 of this Regulation, the provisions of Chapter VIII of this Regulation will apply. The Institute must take the necessary steps to deliver, in a simple and expeditious manner, the complaint to the procedure for the protection of rights.

Chapter X
Measures for the stoppage of the use of personal data

Article 125. To guarantee the due protection of the personal data, exceptionally, the Institute may order the data controller to stop the use of the personal data during the substantiation of the procedure for the protection of rights and inspection, when the following conditions are met:

- **I.** There is a founded and motivated presumption of serious violations of the Law, of the Regulation and other applicable provisions, and
- **II.** When any delay may cause irreparable or difficult-to-repair damage for the data subject.

Article 126. These measures must be proportional and suitable for the risk foreseen.

The Institute must request, from the data subject or complainant, the information to prove the presumed violation of the Law, the Regulation or other applicable provisions.

Article 127. The data controller must comply with the measure ordered by the Institute within a term that may not exceed five days from notification.

If the data controller fails to comply with the measure ordered by the Institute within the term established in this article, the Institute will start the procedure for imposing sanctions, pursuant to article 63, section XVI of the Law.

Article 128. The data controller may show cause within a term of five days from notification, with the right to offer the evidence it deems pertinent within the same term.

Article 129. The measure will be lifted as soon as the causes that originated it stop, by decision of the Institute, which must be issued within a term not exceeding ten days from the presentation of evidence by the data controller. The decision must be communicated to the data controller.

Chapter XII
Procedure for Imposing Sanctions

Beginning

Article 130. For the purposes of article 61 of the Law, the Institute will start the procedure for imposing sanctions when the procedures for the protection of rights or inspection find violations of the Law likely to be sanctioned under article 64 of the Law. For these purposes, the Secretariat for the Protection of Personal Data will supervise, coordinate and substantiate procedure for imposing sanctions referred to in this Chapter and will issue the corresponding decision and communicate it to the parties.

The procedure will start with the notification made to the violator at the address recorded with the Institute, arising from the procedures for the protection of rights or inspection.

The notification will be accompanied by a report describing the facts constituting the violation, summoning the violator to show cause within a term of fifteen days and produce the evidence it deems convenient for the determination of the sanction.

Production and examination of evidence

Article 131. The violator will make concrete declarations in its answer concerning each of the facts imputed expressly, affirming them, denying them, indicating that it ignores them because they are not its own or explaining how they occurred as the case may be; and will submit arguments to deny the violation charged against it and the corresponding evidence.

If expert or testimonial evidence is produced, the facts concerned by it must be specified, and the names and addresses of the expert or witnesses must be indicated. Without these indications, said evidence will be deemed not produced.

Article 132. Concerning the production of evidence of the violator, a decision must be made admitting or rejecting the elements of conviction produced.

If necessary, the place, date and time will be established for the examination of evidence which, by its nature, requires it. Minutes of the hearing and examination of evidence will be drawn up.

Closing of the investigation and decision

Article 133. After examining the evidence, if applicable, the violator will be notified that it has five days to submit arguments. At the end of said term, the investigation will be closed and the decision of the Institute must be issued within a term not exceeding fifty days after the beginning of the procedure.

In case of justified cause, the Plenum of the Institute may extend once, for up to a period equal to the term referred to in the previous paragraph.

Article 134. Against the decision in the procedure for imposing sanctions, it is possible to file an appeal for review under the Federal Law of Administrative Procedure or an action for nullity with the Federal Court of Tax and Administrative Justice.

Transitory provisions

Article One. This Regulation enters into force the day after its publication in the Official Gazette of the Federation.

Any processing of personal data governed by the Law and this Regulation carried out after the effective date of the Law must be in compliance with the provisions of said regulations, regardless of the fact that the personal data were obtained or the corresponding database was made up or created after the entry into force of the Law.

Article Two. The cases of application of compensatory measures authorized by the Institute referred to in article 27 of this Regulation will be published by the Institute, at the latest three months after the entry into force of this Regulation.

Article Three. To comply with the obligation established in article 31 of this Regulation, the data controllers will have twelve months from the entry into force of this Regulation.

Article Four. The Institute will issue general recommendations concerning the security measures referred to in Chapter III of this Regulation, at the latest six months after the entry into force of the Regulation.

Article Five. The data controller must implement the applicable security measures, at the latest eighteen months after the entry into force of this Regulation.

Article Six. The Secretariat, in cooperation with the Institute, will issue the parameters referred to in articles 69 and 70 of this Regulation, within six months after its entry into force.