EXECUTIVE BRANCH

MINISTRY OF INTERNAL AFFAIRS

EXECUTIVE ORDER issuing the General Law on Protection of Personal Data Held by Obligated Parties

In the margin the National Seal with the legend: United Mexican States – Office of the President of the Republic

I, Enrique Peña Nieto, President of the United Mexican States, address the inhabitants of the nation to inform them that:

The Honorable Congress of the Union has sent me the following

DECREE

"THE GENERAL CONGRESS OF THE UNITED MEXICAN STATES DECREES THE ENACTMENT OF:

THE GENERAL LAW ON PROTECTION OF PERSONAL DATA HELD BY OBLIGATED PARTIES

Sole Article.- The General Law on Protection of Personal Data Held by Obligated Parties is issued.

General Law on Protection of Personal Data Held by Obligated Parties

TITLE FIRST
GENERAL PROVISIONS
Chapter I
Purpose of the Law

Article 1. This law is a matter of public order and of general observance throughout the Republic, and is the regulatory law of articles 6, Base A and 16, second paragraph of the Political Constitution of the United Mexican States, regarding the protection of personal data held by obligated parties.

All the provisions of this General Law are, as pertinent, of direct application and observance for federal obligated parties within their purviews.

The Institute will exercise the attributions and authority vested in it by this Law, independently from those granted to it in other applicable provisions.

Its purpose is that of establishing the bases, principles and procedures required to uphold the right of any person to the protection of his/her personal data held by obligated parties.

Obligated parties under this Law in the federal, state and local sphere are any authority, entity, agency or body of the Executive, Legislative and Judiciary Branches, autonomous entities, political parties, trusts and public funds.

Unions and any other individual or legal entity receiving and making use of public funds or acting as authority in the federal, state or local spheres will be responsible for the personal data in accordance with the laws applicable to the protection of personal data held by private parties.

In all other instances different from those mentioned in the preceding paragraph, individuals and legal entities will be subject to the provisions of the Federal Law on Protection of Personal Data Held by Private Parties.

Article 2. The purposes of this Law are the following:

I. Allocating jurisdictional authority among Federal and State Guarantor bodies in regard to the protection of personal data held by obligated parties;

II. Establishing the minimal bases and homogeneous conditions which will govern the processing of personal data and the exercise of the rights of access, rectification, cancellation and opposition, by means of simple and expedite procedures;

III. Regulating the organization and operation of the National System for Transparency, Access to Information and Personal Data Protection to which reference is made herein and in the General Law on Transparency and Access to Public Information, regarding its functions with respect to the protection of personal data held by obligated parties;

IV. Ensuring compliance with personal data protection principles contemplated in this Law and other applicable provisions on the matter;

V. Protecting the personal data held by any authority, entity, agency or body of the Executive, Legislative and Judiciary Branches; autonomous agencies, political parties, trusts and public funds of the Federation, the Federated States and the municipalities, in order to regulate their due processing;

VI. Enabling all persons to exercise the right of protection of their personal data;

VII. Promoting, fostering and disseminating a data protection culture;

VIII. Establishing the mechanisms to ensure compliance with and effective application of enforcement measures applicable to acts that contravene the provisions of this Law; and

IX. Regulating available means of judicial review and procedures for the filing of actions of unconstitutionality and constitutional controversies by local and federal Guarantor bodies, within the scope of their respective faculties.

Article 3. For the purposes of this Law the following definitions will apply:

I. **Administrative security measures:** Policies and procedures in the matter of personal data protection to manage, provide support and oversee security at the organizational level, to allow the identification, classification and safe deletion of the information, as well as personnel's awareness and training on the matter of personal data protection.

II. **ARCO rights:** The rights of access to, rectification and cancellation of, and opposition regarding the processing of personal data;

III. **Areas**: Administrative units of obligated parties that hold, may hold, process and be responsible for or in charge of personal data as contemplated in the relevant internal regulations, organic statutes or equivalent instruments;

IV. **Assessment of impact on the protection personal data:** Document by which obligated parties that intend to put into operation or modify public policies, computer software, systems and platforms, electronic applications or any other technology involving intensive or relevant processing of personal data will assess the actual impact in regard to a given processing of personal data, so as to identify and mitigate possible risks relating to the data owners' principles, duties and rights, as well as specify the data controller's and data processor's duties as are provided in applicable regulations.

V. **Blocking:** The labeling and retention of personal data once it has served the purpose for which they were collected, with the sole purpose of determining possible responsibilities in relation to its processing, until the end of the legal or contractual limitation period of said responsibilities. During this period, personal data may not be processed, and, once the period has ended, the data will be cancelled in the relevant database.

VI. **Cloud computing:** Mode of providing external computing services on demand, that includes the provision of infrastructure, platforms or software distributed in a flexible manner, by virtual procedures, where resources are dynamically shared;

VII. **Compensatory measures:** Alternate mechanisms used to make the privacy notice available to data owners through its dissemination by mass media outlets or others of widespread reach;

VIII. **Consent:** Free expression of the data owner's specific and informed will to allow the processing of his/her data.

IX. **Data Controller:** The obligated parties referred to in article 1 hereof, that decide on the processing of personal data;

X. **Data owner:** The individual to whom the personal data relates;

XI. **Data processor:** The public or private individual or legal entity, external to the data controller's organization which, alone or jointly with others, processes personal data on behalf of the data controller.

XII. **Databases:** Ordered set of personal data concerning identified or identifiable individuals, subject to specific criteria, howsoever created, regardless of where they are supported, or how they are processed, stored and organized.

XIII. **Days:** Working days;

XIV. **Dissociation:** The procedure through which personal data cannot be associated with the data owner nor allow, by reason of their structure, content or degree of disaggregation, his/her identification.

XV. **Guarantor bodies:** Those having constitutional autonomy specialized in access to information and protection of personal data, as provided in articles 6 and 116, section VIII of the Political Constitution of the United Mexican States;

XVI. **Institute:** The National Institute for Transparency, Access to Information and Personal Data Protection, which is a Federal Guarantor body in regard to the protection of personal data held by obligated parties;

XVII. **National Council:** The Transparency, Access to Information and Protection of Personal Data National Council referred to in article 32 of the General Law on Transparency and Access to Public Information;

XVIII. **National Platform:** The National Transparency Platform referred to in Article 49 of the General Law on Transparency and Access to Public Information;

XIX. **National Program for Personal Data Protection:** National Program for Personal Data Protection;

XX. **National System:** The National System for Transparency, Access to Information and Personal Data Protection;

XXI. **Personal data:** Any information concerning an identified or identifiable individual. An individual is deemed to be identifiable when his/her identity may be directly or indirectly deduced from any information;

XXII. **Physical security measures:** Set of actions and mechanisms to protect the physical environment of personal data and of the resources involved in their processing. The following activities, listed here as an enumeration and not by way of limitation, must be taken into consideration:

a) Preventing unauthorized access within the perimeter of the organization, its physical premises, critical areas, resources and information;

b) Preventing damage to or interference with the physical premises and critical areas of the organization, its resources and information;

c) Providing protection to mobile or portable resources, and any physical or electronic support medium which may be taken out of the organization; and

d) Providing effective maintenance to the equipment containing personal data, so as to ensure its availability and integrity;

XXIII. **Privacy Notice**: Document generated by the data controller and made available to the data owner in physical, electronic or any other format upon of collection of the latter's personal data, in order to inform him/her on the purposes of their processing;

XXIV. **Processing:** Any operation or set of operations undertaken by manual or automated means applied to personal data, relating to the retrieval, use, recording, organization, preservation, preparation, utilization, communication, dissemination, storage, holding, accessing, managing, exploitation, release, transfer or disposal of personal data;

XXV. **Public Access Sources:** Such databases, systems or archives which may, under the law, be consulted by the public where no impediment exists by reason of restrictive regulation, with no other requirement save for the payment of a fee, rate or duty. A source is not deemed to be of public access when the information it contains was unlawfully collected or is of an unlawful origin, this as provided in the provisions of this Law and other applicable regulations;

XXVI. **Safety Measures:** Set of actions, activities, controls or administrative, technical and physical mechanisms that enable personal data protection;

XXVII. **Security document:** Instrument describing and informing generally on the technical, physical and administrative measures adopted by the data controller to ensure the confidentiality, integrity and availability of the personal data held by it;

XXVIII. Sensitive personal data: Personal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. As an enumeration and not by way of limitation, sensitive data are considered to be those which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, political views and sexual preference;

XXIX. Suppression: The archival deletion of personal data in accordance with applicable archival regulations, resulting in the deletion, erasure o destruction of the personal data under the data controller's previously established security measures;

XXX. Technical security measures: Set of actions and mechanisms that make use of technology relating to hardware and software to protect the digital environment of personal data, and the resources involved in their processing. The following activities, listed here as an enumeration and not by way of limitation, must be taken into consideration:

a) Ensuring in advance that access to the data bases and information as well as to any resources be allowed solely to identified and authorized users;

b) Setting up a system of privileges to enable the user to carry out the activities required by his/her functions;

c) Checking security configuration of hardware and software at the time of acquisition, operation, development and maintenance; and

d) Administering communications, operations and storage media of computer resources used in the processing of personal data.

XXXI. Transfer: Any data communication made to a person other than the data owner, the data controller or the data processor;

XXXII. Transmittal: Any transfer of personal data occurring exclusively between the data controller and the data processor, within the Mexican territory or abroad;

XXXIII. Transparency Committee: Body to which reference is made in article 43 of the General Law on Transparency and Access to Public Information; and

XXXIV. Transparency Unit: The governmental entity referred to in article 45 of the General Law on Transparency and Access to Public Information.

Article 4. This Law will be applicable to any processing of personal data contained in physical or electronic support mediums, regardless of the mode or manner in which they were created, the type of support, processing, storage and organization.

Article 5. For the purposes of this Law, the following are considered to be public access sources:

I. Web pages, or remote or local electronic, optical, or other type of technological communication media, provided the site where the personal data are found has been conceived to easily provide information to the public and is open for general consultation.

II. Telephone directories under the specific regulations;

III. The official dailies, gazettes or bulletins, under the provisions applicable to them;

IV. Social communications media; and

V. Public registries under the provisions applicable to them.

In order for the foregoing listed items to be considered as public access sources, they must be available for consultation by any person that is not subject to restrictive regulation, or such being the case, available under no other condition except for the payment of a fee, charge or duty. A source will not be considered of public access when the information it contains is illegitimate or has been unlawfully obtained.

Article 6. The State guarantees the privacy of individuals and must ensure that third parties do not engage in conducts which may arbitrarily affect it.

The right to protection of personal data will only be curtailed by reason of national security, as set forth in the law on the matter, in provisions relating to public order, public safety and health care matters, or in order to protect the rights of third parties.

Article 7. As a general rule, sensitive personal data may not be processed, unless express consent has been obtained from the data owner, this condition not being applicable in the cases set forth in article 22 of this Law.

The processing of the personal data of minors requires that the best interest of the child be given priority.

Article 8. Application and construction of this Law shall proceed in the light of the provisions of the Political Constitution of the United Mexican States, the International Treaties to which Mexico is a party, as well as of court decisions and binding precedents issued by national and international specialized bodies, by furthering at all times the right to privacy, the protection of personal data and affording persons the broadest protection.

As regards its construction, the criteria, determinations and opinions issued by national and international bodies on the matter of the protection of personal data may be taken into consideration.

Article 9. In the absence of an express provision in this Law, the provisions of the Federal Code of Civil Procedure and of the Federal Law of Administrative Procedure will be applied to supply for any deficiencies.

The Federated States must, within their respective purviews, establish in their laws the provisions that may be applicable to Guarantor bodies in supplying for any deficiencies when applying and interpreting this Law.

Chapter II

The National System for Transparency, Access to Information and Personal Data Protection

Article 10. The National System will be set up as provided for in the General Law on Transparency and Access to Public Information. In regard to the protection of personal data, the function of this System is to coordinate and assess actions relating to horizontal public policy on personal data protection, as well as to establish and implement criteria and guidelines on the matter, as set forth in this Law, in the General Law on Transparency and Access to Public Information and other applicable regulations.

Article 11. The National System will contribute to maintain the right to personal data protection in full force nationwide, at the three levels of government.

This joint and comprehensive effort will contribute to the implementation of public policies in strict compliance with applicable regulations on the matter; to the full exercise of and respect for the right to personal data protection and to the dissemination of a culture on this right and on its accessibility.

Article 12. In addition to the objectives contemplated in the General Law on Transparency and Access to Public Information, the objective of the National System will be to design, put into execution and assess a Program for Personal Data Protection which will define the national policy and establish, as a minimum, objectives, strategies, actions and goals to:

I. Promote education in and a culture for the protection of personal data in Mexican society;

II. Foster the exercise of the rights of access, rectification, cancelation and opposition;

III. Provide training to obligated parties on the subject of the protection of personal data;

IV. Give impulse to the implementation and preservation of a security management system as referred to in article 34 of this Law, as well as to promote the adoption of national and international standards and good practices on the matter; and

V. Establish in advance the mechanisms to measure, report on and verify established goals.

The National Program for Personal Data Protection will become the guiding instrument for the integration and coordination of the National System, and must specify and prioritize the objectives and goals to be met by the latter, and must in addition define the general courses of action that may be required.

The National Program for Personal Data Protection must be assessed and updated at the close of each fiscal year and will define the set of activities and projects to be undertaken during the following year.

Article 13. The National System will have a National Council. The provisions of the General Law on Transparency and Access to Public Information and other applicable provisions must be observed in the integration, organization, operation and attributions of the National Council.

Article 14. The National System will, in addition to that which is provided in the General Law on Transparency and Access to Public Information and other applicable regulations, have the following functions in matters pertaining to the protection of personal data:

I. Promoting exercise of the right to protection of personal data throughout the Mexican Republic;

II. Fostering in society a culture on the protection of personal data;

III. Analyzing, expressing its opinion on, and proposing bill drafts to reform or amend the regulations on the matter to the proper governmental authorities;

IV. Agreeing on, and establishing coordination mechanisms to enable the formulation and execution of comprehensive, systematic, continuous and assessable public instruments and policies intended to foster compliance with the objectives and purposes of the National System, of this Law and all other applicable provisions on the matter;

V. Issuing general resolutions regarding the operation of the National System;

VI. Formulating, establishing and executing general policies regarding the protection of personal data;

VII. Fostering effective coordination of the governmental agencies part of the National System and monitoring the actions established to achieve this purpose;

VIII. Promoting harmonization and development of the procedures provided for in this Law and assessing their progress;

IX. Designing and implementing policies on the protection of personal data;

X. Establishing efficient mechanisms to allow society to participate in the assessment of policies and of the institutions that are part of the National System;

XI. Developing common projects of nationwide scope to measure compliance and progress by data controllers;

XII. Entering into collaboration agreements the purpose of which is to provide assistance in complying with the objectives of the National System and those provided for in this Law and other applicable provisions on the matter;

XIII. Promoting and implementing action to ensure conditions of accessibility to enable vulnerable groups to exercise, all other things being equal, their right to protection of personal data;

XIV. Proposing codes of good practices or models on the matter of the protection of personal data;

XV. Promoting communication and coordination with domestic federal, state and municipal authorities, and with international authorities and organizations, in order to further and foster the objectives of this Law;

XVI. Proposing actions to link the National System with other nationwide, regional or local systems and programs;

XVII. Promoting and advancing the exercise and protection of the right to protection of personal data, by implementing, organizing, and operating the National Platform referred to in the General Law on Transparency and Access to Public Information and other applicable regulations;

XVIII. Approving the National Program for Personal Data Protection referred to in article 12 of this Law;

XIX. Issuing additional criteria in order to determine the cases in which intensive or relevant processing of personal data is involved, this as provided for in articles 70 and 71 of this Law;

XX. Issuing the necessary administrative provisions to assess the content filed by obligated parties when conducting the Assessment of impact on the protection of personal data, so as to issue the relevant non-binding recommendations; and

XXI. Such others as are set forth in other provisions on the matter pertaining to the operation of the National System.

Article 15. The National Council will function as provided in the General Law on Transparency and Access to Public Information and other applicable laws and regulations.

TITLE SECOND

PRINCIPLES AND DUTIES

Chapter I

Principles

Article 16. The data controller must adhere to the principles of legality, purpose, fidelity, consent, quality, proportionality, notice and responsibility in the processing of personal data.

Article 17. The processing of personal data by the data controller must be carried out within the scope of the faculties and attributions conferred to the data controller under applicable regulations.

Article 18. All processing of personal data by the data controller must be justified as undertaken for specific, lawful, explicit and legitimate purposes relating to the attributions vested in the data controller under applicable regulations.

The data controller may process personal data for purposes other than those set forth in the privacy notice, provided the data controller has the required attributions to do so as conferred by law and has obtained the data owner's consent, unless a person reported as missing is concerned, this as provided in this Law and other applicable provisions on the matter.

Article 19. The data controller must not obtain and process personal data by deceitful or fraudulent means, prioritizing the protection of the data owner's interests and the reasonable expectation of privacy.

Article 20. When any one or more of the causes for exemption contemplated in Article 22 of this Law are not present, the data controller must obtain the data owner's prior consent to process his/her personal data, which must be granted:

I. Freely: without the involvement of error, bad faith, duress or dolus which may affect the data owner's expression of free will;

II. Specifically: it must refer to concrete, lawful, explicit and legitimate purposes that justify their processing; and

III. In an informed manner: the data owner being cognizant of the privacy notice prior to any processing of his/her personal data.

When obtaining the consent of minors or individuals whose status of interdiction or incapacity has been legally declared, the rules on representation provided for in the applicable civil laws will apply.

Article 21. Consent may be granted expressly or tacitly. Consent will be understood as expressly granted when the data owner's will has been expressed orally, in writing, by electronic or optical means, by unequivocal signs or by the use of any other technology.

Consent will be tacit when the privacy notice is made available to the data owner without him/her expressing anything to the contrary.

As a general rule tacit consent will be valid, except in the event that applicable provisions require that the data owner's will be expressly stated.

Regarding sensitive personal data, the data controller must obtain the express written consent from the data owner for its processing, by means of his/her autograph or electronic signature, or by any other means of authentication established for such a purpose, except in the cases contemplated in article 22 of this Law;

Article 22. The data controller will not be obligated to obtain the data owner's consent to process his/her personal data in the following cases:

I. Where so provided in a statute, such assumptions having to adhere to the bases, principles and provisions set forth in this Law, without contravening it under any circumstance;

II. Where transfers made between data controllers involve personal data used in exercising their own, compatible or analogous faculties for the purpose that gave rise to the processing of the personal data;

III. Where there is a court order, decision or mandate grounded in law and fact issued by a competent authority;

IV. For the recognition or defense of the data owner's rights before a competent authority;

V. Where the personal data are required to exercise a right or comply with obligations arising from a legal relationship between the data owner and the data controller;

VI. Where an emergency arises that has the potential of causing damage or injury to the person or property of an individual;

VII. Where the personal data are required to provide preventive treatment or diagnosis when providing healthcare;

VIII. Where the personal data are contained in public access sources;

IX. Where the personal data have been subject to a prior dissociation process; or

X. Where the data owner is a person reported as missing as provided in the law on the matter.

Article 23. The data controller must take the necessary measures to maintain the accuracy, completeness, and correctness of the personal data held by it and to keep them up to date, so as not to alter their veracity.

There is the presumption that quality of personal data has been complied with when the same have been directly provided by the data owner, unless and until otherwise expressed and evidenced by the data owner.

Where personal data are no longer needed to achieve the purposes specified in the privacy notice which gave rise to their processing in accordance with applicable provisions, they must be suppressed, having first been blocked if required, once the term provided for their preservation has elapsed.

The terms for preservation of personal data must not exceed those that are necessary to achieve the purposes that warranted their processing, must adhere to the applicable provisions on the relevant matter and take into consideration the administrative, accounting, tax, legal and historical aspects of the personal data.

Article 24. The data controller must establish and document the procedures to be followed for preservation and, such being the case, blocking and suppression of personal data, which must specify the terms for preservation of the same, in accordance with the provisions of the preceding article of this Law.

In the procedures mentioned in the preceding paragraph, the data controller must include mechanisms that allow for compliance with the terms established for the suppression of personal data, as well as for conducting periodic review on the need for preserving the personal data.

Article 25. The data controller must process only such personal data as are suitable, relevant and strictly necessary to achieve the ends that justify their processing.

Article 26. The data controller must inform the data owner, by means of the privacy notice, on the existence and main characteristics of the processing to be given to his/her personal data, to enable him/her to make informed decisions in such regard.

As a general rule, the privacy notice must be disseminated on the electronic and physical means available to the data controller.

For the privacy notice to properly comply with its informative function, it must be drafted and structured in clear and simple terms.

Where it is impossible to make the privacy notice directly available to the data owner or if this requires a disproportionate effort, the data controller may implement alternate means of mass communication in accordance with the criteria issued on the matter by the National System for Transparency, Access to Public Information and Personal Data Protection.

Article 27. The privacy notice referred to in article 3, section II, will be made available to the data owner in two versions: a simplified and a complete version. The simplified version must contain the following information:

I. Data owner's name;

II. The purpose of the treatment for which the personal data are being collected, specifying those that require the data owner's consent;

III. Where personal data transfers requiring consent are to be made, information on the following must be provided:

a) the governmental authorities, branches, entities, agencies and bodies of the three levels of government and the individuals and legal entities to whom personal data will be transferred, and

b) the purpose of such transfers.

IV. The mechanisms and means available to allow the data owner, if so required, to express his/her opposition to the processing of his/her personal data for purposes and transfers of personal data requiring the data owner's consent; and

V. The web page where the complete privacy notice may be consulted.

Availability of the privacy notice referred to in this article does not release the data controller from the obligation of providing the mechanisms allowing the data owner to become cognizant of the content of the privacy notice referred to in the following article.

The mechanisms and means referred to in section IV of this article must be made available to enable the data owner to express his/her opposition to the processing of his/her personal data for purposes or transfers requiring the data owner's consent, prior to any such processing.

Article 28. The complete privacy notice must contain, in addition to that which is specified in the sections of the preceding article, at least the following information:

I. The data controller's address;

II. The personal data that will be subject to processing, identifying those that are sensitive;

III. The legal grounds on which the data controller's authority to process rests;

IV. The purposes of the processing for which the personal data are collected; with the specification of those requiring the data owner's consent;

V. The available mechanisms, means and procedures to exercise ARCO rights;

VI. The address of the Transparency Unit; and

VII. The means to be used by the data controller to inform data owners on any changes in the privacy notice.

Article 29. The data controller must implement the mechanisms contemplated in article 30 of this Law in order to evidence compliance with the principles, duties, and obligations established in this Law and to become accountable to the data owner, the Institute or the Guarantor bodies, as applicable, for the processing of the personal data it holds; in order to do so, it must comply with the Constitution and the International Treaties to which Mexico is a Party. To achieve this end, it may resort to domestic or international standards and best practices insofar as these do not contravene Mexican regulations.

Article 30. Among the mechanisms the data controller must adopt to comply with the principle of responsibility established in this Law, the following are listed as an enumeration and not by way of limitation:

I. To allocate resources authorized for such purpose to be used in the implementation of programs and policies for the protection of personal data;

II. To develop policies and programs for the protection of personal data that are of mandatory compliance within the data controller's organization;

III. To put into practice a training and updating program for personnel regarding the obligations and other duties in regard to personal data protection;

IV. To review the security programs and policies regarding personal data from time to time to decide on any changes that may be required;

V. To establish an internal and/or external oversight and monitoring program, including audits, to verify compliance with personal data protection policies;

VI. To establish the procedures for the reception and response to queries and complaints made by data owners;

VII. To design, develop and implement its public policies, programs, services, computer systems or platforms, electronic applications or any other technology that entails the processing of personal data, in accordance with the provisions set forth in this Law and such others that may be applicable on the matter; and

VIII. To ensure that its public policies, programs, services, computer systems or platforms, electronic applications or any other technology that entails the processing of personal data comply automatically with the obligations contemplated in this Law and in other applicable provisions on the matter.

Chapter II

Duties

Article 31. Regardless of the type of system on which personal data are hosted or the type of processing applied, the data controller must establish administrative, physical and technical security measures to protect personal data that afford protection against damage, loss, alteration, destruction or unauthorized use, access to, or processing, and must ensure their confidentiality, integrity and availability.

Article 32. The security measures adopted by the data controller must take into consideration:

I. The inherent risk regarding processed personal data;

II. The sensitivity of the processed personal data;

III. Technological developments;

IV. The possible consequences of a breach affecting data owners;

V. The personal data transfers to be made;

VI. The number of data owners;

VII. The previous breaches that have occurred in the processing systems; and

VIII. The risk relating to the potential quantitative or qualitative value processed personal data may have for a third party lacking authorization to hold them.

Article 33. In establishing and maintaining the security measures required for personal data protection, the data controller must undertake, at the least, the following interrelated activities:

I. Establishing internal policies on personal data management and processing that take into account the context in which processing is to take place and the personal data lifecycle, that is to say, their collection, use and ulterior suppression;

II. Defining the functions and obligations of the personnel involved in the processing of the personal data;

III. Taking an inventory of the personal data and of the processing systems;

IV. Conducting risk analysis on the personal data, taking into account existing threats and vulnerabilities regarding the personal data and the resources involved in their processing; such as the hardware, software, the data controller's personnel, among others, these listed here as an enumeration and not by way of limitation;

V. Performing gap analysis by comparing existing security measures against those still lacking in the data controller's organization;

VI. Preparing a work plan for the implementation of the security measures found lacking, as well as for the implementation of measures for daily compliance with the personal data management and processing policies,

VII. Monitoring and reviewing implemented security measures, as well as the threats and vulnerabilities to the personal data from time to time; and

VIII. Designing and applying different training levels for personnel under its command, depending on their roles and responsibilities in regard to the processing of personal data.

Article 34. The actions relating to the personal data processing security measures must be documented and kept in a management system.

A management system will be understood to be the set of interrelated elements and activities set up to establish, implement, operate, monitor, review, maintain and improve the processing and security of personal data, in accordance with the provisions of this Law and other applicable provisions on the matter.

Article 35. In particular, the data controller must prepare a security document containing, at least, the following:

I. The inventory on the personal data and the processing systems;

II. The functions and duties of the persons involved in the processing of personal data;

III. Risk analysis;

IV. Gap analysis;

V. Work plan;

VI. The monitoring and review mechanisms regarding security measures; and

VII. The general training program.

Article 36. The data controller must update the security document whenever any of the following events occurs:

I. Substantial changes in the processing of the personal data are made that entail a change in risk level;

II. As a result of a continuing improvement process, arising from the monitoring and review of the management system;

III. As a result of an improvement process intended to mitigate the impact of a security breach that may have occurred; and

IV. After the implementation of corrective and preventive measures as a result of a security breach.

Article 37. Should a security breach occur, the data controller must analyze the causes that gave rise to it and include in its work plan the preventive and corrective actions required to adapt the security measures and the personal data processing, such being the case, so as to prevent the breach from occurring again.

Article 38. In addition to those specified in the relevant laws and in applicable regulations, any of the following events, listed here as a minimum, are considered to be security breaches at any phase in the processing of personal data:

I. Loss or unauthorized destruction;

II. Theft, misplacement or unauthorized copying;

III. Unauthorized use, access or processing; and

IV. Damage to and unauthorized alteration or modification.

Article 39. The data controller must keep a logbook to record security breaches, which must include a description of same, date of occurrence, their causes and the corrective measures that were implemented forthwith and definitively.

Article 40. The data controller must forthwith inform the data owner and, as applicable, the Institute and the Guarantor bodies of the Federated States, on any breaches that significantly affect economic or moral rights, upon confirmation that a breach has occurred, and once the data controller has begun to take the action required to trigger in-depth examination in regard to the extent of the breach, so as to enable affected data owners to take the required measures to defend their rights.

Article 41. The data controller must provide the data owner with at least the following information:

I. The nature of the incident;

II. The compromised personal data;

III. Recommendations to the data owner on the measures he/she may adopt to protect his/her own interests;

IV. The corrective actions that were implemented forthwith;

V. The media where more information on the matter may be obtained.

Article 42. The data controller must establish controls or mechanisms intended to ensure that any and all persons involved in any phase of the processing of personal data maintain the confidentiality of the same. This obligation must survive termination of their relationship with the data controller.

The foregoing without prejudice to the provisions regarding access to public information.

TITLE THIRD

DATA OWNERS' RIGHTS AND EXERCISE OF SAME

Chapter I

Rights to Access, Rectification, Cancellation and Opposition

Article 43. The data owner or his/her representative may at any time request the data controller access to, rectification or cancelation of his/her personal data, or express his/her opposition to their processing, as set forth in this Title. The exercise of any one of the ARCO rights does not constitute a prior requirement for, nor does it preclude the exercise of any other of these rights.

Article 44. The data owner will be entitled to access his/her personal data held by the data controller, as well as to know the information regarding the conditions and general characteristics of its processing.

Article 45. The data owner will be entitled to request the data controller to rectify or correct his/her personal data when these are inaccurate, incomplete or are not updated.

Article 46. The data owner will be entitled to request the cancellation of his/her personal data in the archives, records, files and systems of the data controller, for the same to be no longer held and processed by the latter.

Article 47. The data owner may oppose the processing of his/her personal data, or demand that it cease when:

I. Even though processing is lawful, it must cease to prevent damage or injury to be caused to the data owner should it continue; and

II. His/her personal data are subject to automated processing that produces undesired legal effects or that significantly affects his/her interests, rights or liberties, and is intended to assess certain personal characteristics of the data owner without human intervention, or to analyze or predict, in particular, his/her professional performance, financial situation, health condition, sexual preferences, reliability or behavior.

Chapter II

Exercise of the Rights of Access, Rectification, Cancelation and Opposition

Article 48. The reception and processing of requests to exercise ARCO rights submitted to data controllers will be subject to the procedure set forth in this Title and other applicable provisions on the matter.

Article 49. In order to exercise ARCO rights, the data owner must provide proof of identity, and in addition proof of identity and legal capacity of his/her representative, such being the case.

ARCO rights may be exercised exceptionally by a person other than the data owner or his/her representative, in the events contemplated in legal provisions, or else, under court order.

The exercise of ARCO rights of minors or individuals whose status of interdiction or incapacity has been legally declared under civil law, will be subject to the rules for representation set forth in such legislation.

In regard to personal data of the deceased, the person that provides proof of legal interest in accordance with applicable laws may exercise the rights granted by this Chapter, provided the data owner should have unquestionably stated his will on this matter or there is a court order to this effect.

Article 50. The exercise of ARCO rights must be free of charge. Fees may be charged solely to recover the cost of copying, certification or delivery services as provided in applicable regulations.

In regard to access to personal data, the laws establishing copying and certification fees must take into consideration that the amounts determined should allow or facilitate the exercise of this right.

When the data owner provides the magnetic or electronic medium or the mechanism required to make copies of his/her personal data, the same must be delivered to him/her free of charge.

The information must be delivered free of charge when the delivery of no more than twenty pages is involved. Transparency units may release the data owner from payment of copying and delivery fees taking into account the data owner's social and financial circumstances.

The data controller cannot condition the filing of requests to exercise ARCO rights to the use of any service o means that entails a cost for the data owner.

Article 51. The data controller must establish simple procedures to allow the exercise of ARCO rights, whose time of response should not exceed twenty days counted as of the day following reception of the request.

The term referred to in the preceding paragraph may be extended once up to ten days if so warranted by the circumstances, provided the data owner is so informed within the term provided for response.

Should the exercise of ARCO rights be found warranted, the data controller must enable such exercise within a term that cannot exceed fifteen days counted as of the day following that on which the response is notified to the data owner.

Article 52. Requests to exercise ARCO rights cannot be subject to requirements other than the following:

I. The specification of the data owner's name and address or other means to receive notification;

II. The documents providing proof of the data owner's identity and, such being the case, of the identity and legal capacity of his/her representative;

III. If possible, specification of the area in charge of processing the personal data, and the entity before whom the request is filed;

IV. A clear and accurate description of the personal data in regard to which the exercise of any of the ARCO rights is being sought, unless the right to access is involved;

V. The description of the ARCO right to be exercised; or else, of that which is being requested by the data owner; and

VI. Any other element or document that facilitates tracing of the personal data, such being the case.

Regarding a request for access to personal data, the data owner must specify the preferred form to be used in their reproduction. In processing the request, the data controller must honor the data owner's preference unless there is a physical or legal obstacle preventing it from reproducing the personal data in the form requested. In such event, it must offer other forms of delivery of the personal data and must specify the legal and factual grounds for doing so.

In the event a request for the protection of the data does not meet any one of the requirements referred to in this article, and the Institute or the Guarantor bodies do not have the means to supply for its deficiences, the data owner will be so notified once, within five days following the date the request for the exercise of ARCO rights was filed, to allow him/her to cure any deficiencies within a term of ten days counted as of the day following such notification.

Should this term elapse without the action as requested having been taken, the request to exercise ARCO rights will be deemed as not having been filed.

The notice will have the effect of staying the term the Institute, or such being the case the Guarantor bodies; have to resolve on the request for the exercise of ARCO rights.

In regard to a request for cancellation, the data owner must specify the reasons for requesting the suppression of his/her data from the data controller's files, records or databases.

With respect to a request expressing opposition, the data owner must specify the legitimate causes or the specific circumstances that give rise to his/her opposition to processing, and the damage or injury continued processing would cause, or if such were the case, the specific purposes for which he/she wishes to exercise the right to opposition.

Requests for the exercise of ARCO rights must be filed with the data controller´s Transparency Unit considered appropriate by the data owner, by submitting a brief, in the forms, electronic or any other media as are established by the Institute and the Guarantor bodies within the scope of their respective purviews.

The data controller must process all requests submitted for the exercise of ARCO rights and properly acknowledge receipt thereof.

The Institute and the Guarantor bodies may, as applicable, establish the forms, systems and other simplified methods required to facilitate the exercise of ARCO rights for data owners.

The means and procedures put in place by the data controller to handle the requests submitted for the exercise of ARCO rights must be easily accessible and provide the widest coverage, taking into account the data owners' profiles and the manner in which they maintain daily or regular contact with the data controller.

Article 53. In the event the data controller is not the appropriate entity to process the request for the exercise of ARCO rights, it must so inform the data owner within three days following submission of the request, and if capable of making the determination as to the appropriate data controller, it must refer the data owner to the latter.

In the event the data controller states that the personal data are not found in its archives, records, systems or on file, this statement must be set down in a resolution issued by the Transparency Committee confirming the non-existence of the personal data.

In the event the data controller becomes aware that the request for the exercise of ARCO rights is being filed in regard to rights not contemplated in this Law, it must so inform the data owner and refer him/her to the proper authorities.

Article 54. Where the provisions applicable to certain personal data processing contemplate a specific handling or procedure to request exercise of ARCO rights, the data controller must inform the data owner on the existence of such requirement, within a term not to exceed five days following the date the request is filed, so as to allow the data owner to decide whether he/she is to exercise his/her rights resorting to such specific procedure, or else, will resort to the institutional procedure set up by the data controller to handle requests for the exercise of ARCO rights in accordance with the provisions of this Chapter.

Article 55. The only instances in which the exercise of ARCO rights will be found not to be warranted are listed herein below:

I. Should the data owner or his/her representative not provide evidence of their legal capacity to do so;

II. Should the personal data not be held by the data controller;

III. Should there be a legal impediment;

IV. Should the infringement of rights of a third party be involved;

V. Should such exercise operate to obstruct judicial or administrative proceedings;

VI. Should there exist a resolution by a competent authority that restricts access to the personal data, or prevents rectification or cancellation of, or opposition to the same;

VII. Should cancellation or opposition rights have already been exercised;

VIII. Should the data controller not be the competent authority;

IX. Should it be necessary to protect the data owner's legally protected interests;

X. Should it be necessary in order to comply with legally acquired obligations binding upon the data owner;

XI. Should the Mexican State, acting on the basis of its legal attributions, find that it is required and proportional to make daily use, keep and handle [personal data] in order to preserve the integrity, stability and permanence of the Mexican State; or

XII. Should the personal data be part of information that the entities subject to financial regulation and oversight by the obligated party have provided the latter in order to comply with demands for information on their operations, organization and activities.

In all the foregoing instances, the data controller must inform the data owner on the reasons for its determination, within the term of twenty days referred to in the first paragraph of article 51 of this Law and other applicable provisions, and must do so through the same means through which the request was filed, attaching any pertinent evidence, if so required.

Article 56. The petition for review referred to in article 94 of this Law is available in the event the data controller refuses to process any request for the exercise of ARCO rights or fails to provide an answer to such request.

Chapter III

Data Portability

Article 57. Where personal data are processed via electronic means in a commonly used structured format, the data owner will be entitled to obtain from the data controller a copy of the processed data in a commonly used structured electronic format allowing him/her their continuous use.

Where the data owner has provided personal data and processing is based on consent or contract, he/she will be entitled to transmit such personal data and any other information he/she may have provided, which is kept in an automated processing system, to another system in a commonly used electronic format, no impediment being placed by the processing data controller that is being subjected to removal of the personal data.

The National System will establish guidelines providing for the parameters to be taken into consideration to determine the hypotheses under which the presence of a commonly used structured format is presumed to be present, as well as for the technical standards, modalities and procedures for the transfer of personal data.

TITLE FOURTH

RELATIONSHIP BETWEEN THE DATA CONTROLLER AND THE DATA PROCESSOR

Sole Chapter

Data controller and Data processor

Article 58. The data processor will be in charge of personal data processing activities without having any decision making authority regarding the scope and content of such processing, and its actions will be subject to the terms established by the data controller.

Article 59. The relationship between the data controller and the data processor must be formalized under contract or any other legal instrument as determined by the data controller, that adheres to applicable regulations, and which evidences its existence, content and scope.

The contract or legal instrument chosen by the data controller must contain, as a minimum, the following general clauses in regard to the services to be provided by the data processor setting forth that:

I. Personal data processing will take place as instructed by the data controller;

II. Personal data processing will not be used for purposes other than those as are specified by the data controller;

III. Security measures will be implemented in accordance with applicable legal instruments;

IV. The data controller will be informed when any breach in the processing of personal data as per the data controller's instructions occurs;

V. Confidentiality will be maintained in regard to the personal data being processed;

VI. The personal data subject to processing will be suppressed or returned once the legal relationship with the data controller is terminated, provided there is no legal provision requiring the preservation of the personal data; and

VII. The personal data will not be transferred unless so determined by the data controller, or if such communication is the result of subcontracting, or unless it takes place as a result of an express order of a competent authority.

The covenants between the data controller and the data processor regarding the processing of personal data must not contravene this Law and other applicable provisions, nor the provisions contained in the relevant privacy notice.

Article 60. Should the data processor fail to act as instructed by the data controller and decides on processing on its own, it will assume the role of data controller according to applicable laws on the matter.

Article 61. The data processor may, in its turn, subcontract the services entailing the processing of personal data on behalf of the data controller, provided the data controller's express consent has been obtained. The subcontractor shall assume the role of data processor under the terms provided in this Law and other applicable provisions on the matter.

Where the contract or legal instrument that formalizes the relationship between the data controller and the data processor provides that the latter may subcontract the services, the authorization referred to in the preceding paragraph shall be understood to have been granted as provided in such instrument.

Article 62. Once express authorization has been obtained from the data controller, the data processor must formalize its relationship with the subcontractor in a contract or other legal instrument that serves to document, in accordance with applicable regulations, the existence, content and scope of the services that are to be provided under the terms set forth in this Chapter.

Article 63. The data controller may contract for or adhere to cloud computing services, applications and infrastructure, and for services in other areas involving personal data processing, provided the external supplier guarantees personal data protection policies that are the equivalent of the principles and obligations set forth in this Law and other applicable provisions on the matter.

In such event, the data controller must establish the constraints placed on the processing of the personal data by the external supplier under contractual provisions or other legal instruments.

Article 64. In regard to the processing of personal data using cloud computing services, applications and infrastructure and for services in other areas to which the data controller adheres under general contractual terms and conditions, it may use only those services in which the provider:

I. Meets, at least, the following conditions:

a) Having in place and applying personal data protection policies that conform to the applicable principles and duties set forth in this Law and other applicable regulations;

b) Contemplates the transparency of the subcontracting arrangements that involve the information for which the service is provided;

c) Abstains from including conditions on the provision of the service that authorize or allow it to become the owner or acquire title over the information for which the service is being provided; and

d) Maintains the confidentiality of the personal data for which the service is being provided;

II. Has in place, at least, the mechanisms required to:

a) Inform on changes to its privacy policies or to the conditions of the services it provides;

b) Allow the data controller to establish limits on the type of processing of the personal data for which the services are provided;

c) Establish and maintain security measures for the protection of the personal data for which the services are provided;

d) Ensure suppression of personal data once the services provided to the data controller come to an end, and the data controller has been able to retrieve them; and

e) Prevent access to the personal data to persons who lack privileges of access, or else, in the event involving a request duly grounded in fact and law from a competent authority, to inform the data controller of this fact.

The data controller cannot, under any circumstance, adhere to services which do not guarantee due protection of the personal data, as established in this Law and other applicable provisions on the matter.

TITLE FIFTH

COMMUNICATIONS OF PERSONAL DATA

Sole Chapter

Personal Data Transfers and Transmittals

Article 65. All transfers of personal data, whether domestic or international, are subject to the data owner's consent, except for the exceptions contemplated in articles 22, 66 and 70 of this Law.

Article 66. All transfers must be formalized by the execution of contractual clauses, collaboration agreements or any other legal instrument, in adherence to the regulations applicable to the data controller, that provide evidence on the scope of the processing of the personal data, as well as on the obligations and responsibilities undertaken by the parties.

The provisions of the foregoing paragraph will not apply in the following cases:

I. When involving a domestic transfer taking place between data controllers to comply with a legal provision, or when the data controllers are exercising attributions expressly conferred upon them; or

II. When involving an international transfer which is contemplated in a law or treaty signed and ratified by Mexico; or else, when it takes place at the request of a foreign authority or competent international body acting as recipient, provided the faculties of the transferring data controller and the recipient are equivalent; or else, when the ends for which the transfer takes place are analogous to or compatible with those that gave rise to processing by the transferring data controller.

Article 67. When the transfer involved is domestic, the personal data recipient must process the personal data, undertake the commitment to ensure their confidentiality and use them solely for the purposes for which they were transferred, while adhering to the provisions of the privacy notice of which the transferring data controller must make it cognizant.

Article 68. The transfer or transmittal of personal data outside the Mexican territory by the data controller can only take place when the third party recipient or data processor undertakes to protect such data in adherence to the principles and duties established in this Law and the applicable provisions on the matter.

Article 69. The data controller must, when making any transfer of personal data, provide the personal data recipient with the privacy notice governing the processing of the data owner's personal data.

Article 70. The data controller may transfer personal data without the need of obtaining the data owner's consent in the following cases:

I. When such transfer is contemplated in this Law or other statutes, international agreements or Treaties signed and ratified by Mexico;

II. When transfer is between data controllers, provided the personal data are used in the exercise of their own faculties as are compatible with or analogous to the purposes that gave rise to the processing of the personal data;

III. When transfer is legally ordered in the investigation and prosecution of crimes as well as for purposes of law enforcement and the administration of justice;

IV. When transfer is required to uphold, exercise or defend a right before the competent authority, provided transfer has been requested by such authority;

V. When transfer is required for health prevention or medical diagnosis, to provide health care, medical treatment or for the management of health care services, provided evidence of this requirement is provided;

VI. When transfer is required to preserve or comply with the legal relationship between the data controller and the data owner;

VII. When transfer is required under a contract executed or to be executed by the data controller and a third party in the data owner's interest;

VIII. When involving the cases in which the data controller is not under the obligation of obtaining the data owner's consent for processing and transmission of his/her personal data, as provided in article 22 of this Law; or

IX. When the transfer is required for reasons of national security.

Action by the data controller falling within the exceptions contemplated in this article does not preclude its compliance with applicable obligations set forth in this Chapter.

Article 71. Domestic or international transmittals of personal data taking place between the data controller and the data processor will not require that they be informed to the data owner nor his/her consent.

TITLE SIXTH

PREVENTIVE ACTIONS IN THE MATTER OF PESONAL DATA PROTECTION

Chapter I

Best Practices

Article 72. In complying with the obligations contemplated in this Law, the data controller may develop or adopt on its own, or jointly with other data controllers, data processors or organizations, best practices schemes intended to:

I. Increase the level of protection of the personal data;

II. Harmonize personal data processing for a specific sector;

III. Facilitate the exercise of ARCO rights;

IV. Facilitate personal data transfer;

V. Supplement the provisions contemplated in applicable regulations in the matter of the protection of personal data; and

VI. Provide to the Institute or Guarantor bodies, as the case may be, proof of compliance with applicable regulations in the matter of of personal data protection.

Article 73. Any scheme of best practices for which validation by, or recognition from the Institute, or such being the case, the Guarantor bodies is sought, must:

I. Comply with the parameters issued for this purpose by the Institute or the Guarantor bodies, as applicable, in accordance with the criteria established by the former; and

II. Be notified to the Institute or, such being the case, the Guarantor bodies, in accordance with the procedure established under the parameters mentioned in the preceding section, for them to be assessed and, if found to be warranted, validated or recognized and recorded in the registry referred to in the last paragraph of this article.

The Institute and the Guarantor bodies, as applicable, must issue the operating rules for the registries where validated or recognized best practices schemes will be recorded. Guarantor bodies may record the best practices schemes which have been validated or recognized by them in the registry administered by the Institute, in accordance with rules set by the latter.

Article 74. Should the data controller intend to put into operation or modify public policies, or computational systems or platforms, electronic applications or any other technology which, in its opinion and in accordance with this Law entail an intensive or relevant processing of personal data, it must conduct an Assessment of impact on the protection of personal data and submit it to the Institute or the Guarantor bodies, as applicable, which can issue non-binding specialized recommendations on the subject of personal data protection.

The content of the Assessment of impact on the protection of personal data must be established by the National System for Transparency, Access to Public Information and Protection of Personal Data.

Article 75. For the purposes of this Law, there is intensive or relevant processing of personal data when:

I. There is inherent risk in regard to the personal data to be processed,

II. Sensitive personal data are involved;

III. Transfers of personal data take or are intended to take place.

Article 76. The National System may issue additional criteria on the basis of objective parameters which lead to the determination that intensive or relevant processing of personal data is involved, this in accordance with the provisions of the preceding article, in terms of:

I. The number of data owners;

II. The target public;

III. The development of the technology used; and

IV. The relevance of the personal data processing in view of its social or economic impact, or else of the public interest being pursued.

Article 77. Obligated Parties that conduct an Assessment of impact on the protection of personal data must submit it to the Institute or the Guarantor bodies, as applicable, thirty days in advance of the date on which public policies, computer platforms or systems, electronic applications or any other technologies are intended to be put into operation or modified, for them to issue the relevant non-binding recommendations.

Article 78. The Institute and the Guarantor bodies, as applicable, must issue, such being the case, non-binding recommendations regarding the Assessment of impact on the protection of personal data submitted by the data controller.

The recommendations referred to in the preceding paragraph must be issued within a term of thirty days counted as of the day following that on which the assessment is submitted.

Article 79. When, in the opinion of the obligated party, the intended effects to be achieved by putting into operation or modifying public policies, or computational systems or platforms, electronic applications or any other technology entailing an intensive or relevant processing of personal data may be compromised, or should an urgent or emergency situation arise, an Assessment of impact on the protection of personal data need not be conducted.

Chapter II

Databases held by Agencies in Charge of Security, Law Enforcement and the Administration of Justice

Article 80. Personal data collection and processing under the provisions of this Law by obligated parties that are competent within the purviews of security, law enforcement and the administration of justice are limited to the requirements and data categories that are necessary and proportional to allow them to exercise their functions regarding national security, public safety or for the prevention and prosecution of crimes. Such data must be stored in databases created for such purposes.

Authorities which have access to and store personal data obtained from private parties in compliance with applicable legal provisions, must comply with the provisions set forth in this Chapter.

Article 81. Personal data processing as well as the use of databases for their storage undertaken by obligated parties that are competent within the purviews of security, law enforcement and the administration of justice must comply with the principles established in Title Second of this Law.

Private communications are inviolable. The federal judiciary is the sole authority which, by acting on the request of a federal authority properly empowered by law or of the head of the Public Prosecutor's Office of the relevant federated state, may authorize surveillance of any private communication.

Article 82. Data controllers of the data bases referred to in this Chapter must establish high level security measures to ensure the integrity, availability and confidentiality of the information so as to protect the personal data from being damaged, lost, altered or destroyed and to prevent unauthorized use, access or processing.

TITLE SEVENTH

GOVERMENTAL ENTITIES RESPONSIBLE FOR THE PROTECTION OF PERSONAL DATA HELD BY OBLIGATED PARTIES

Chapter I

Transparency Committee

Article 83. Every data controller must have a Transparency Committee in place, which will be set up and operate as provided in the General Law on Transparency and Access to Public Information and other applicable regulations.

The Transparency Committee will be the highest authority on the matter of the protection of personal data.

Article 84. For the purposes of this Law and without prejudice to other attributions granted to it under applicable regulations, the Transparency Committee will have the following functions:

I. Coordinating, overseeing and taking all action necessary to uphold the right to personal data protection within the organization of the data controller, in accordance with the provisions contemplated in this Law and others that may be applicable on the matter;

II. Establishing, as required, internal procedures to ensure greater efficiency in the handling of requests to exercise ARCO rights;

III. Confirming, modifying o revoking determinations declaring the non-existence of personal data, or denying the exercise of any of the ARCO rights for whatever reason;

IV. Establishing and overseeing the application of specific criteria as are necessary for better compliance with this Law and other applicable provisions on the matter;

V. Overseeing compliance with the measures, controls and actions contemplated in the security document in coordination with the competent administrative areas or units;

VI. Following up on and complying with the resolutions issued by the Institute and the Guarantor bodies, as applicable;

VII. Establishing training and updating programs for public servants in the matter of the protection of personal data; and

VIII. Informing the internal control body or equivalent entity when it, in the exercise of its functions, becomes cognizant of any presumed irregularity in regard to a given processing of personal data, particularly when cases relating to the statement of non-existence by data controllers are involved.

Chapter II

The Transparency Unit

Article 85. Every data controller must have a Transparency Unit which will be set up and operate as provided in the General Law on Transparency and Access to Public Information, this Law and other applicable provisions, which will have the following functions:

I. Providing the data owner with support and guidance in relation to the exercise of the right to protection of personal data;

II. Handling requests to exercise ARCO rights;

III. Establishing mechanisms to ensure that personal data are delivered only to their properly identified legal data owner or representative.

IV. Informing the data owner or his/her representative on the amount of costs to reproduce and deliver personal data, on the basis of the provisions of applicable regulations;

V. Submitting proposals to the Transparency Committee on internal procedures that will ensure and strengthen the efficient handling of requests to exercise ARCO rights;

VI. Applying instruments to assess quality in the handling of requests to exercise ARCO rights; and

VII. Providing advice to the areas under the data controller regarding the protection of personal data.

Data controllers which engage in the processing or relevant or sensitive personal data in carrying out their substantive functions may appoint a personal data protection official that has specialized in the field, who will exercise the attributions mentioned in this article and will be part of the Transparency Unit.

Obligated parties will foster the execution of agreements with specialized public institutions that may provide assistance in the reception, processing and the delivery of responses to requests for information in indigenous languages, Braille or any appropriate accessible format, in a more efficient manner.

Article 86. The data controller will strive to facilitate the exercise of the right to protection of personal data, all other things being equal, for people with disabilities or vulnerable groups.

Article 87. The data controller will adhere to the provisions of the General Law on Transparency and Access to Public Information when appointing the head of the Transparency Unit.

TITLE EIGHTH

GUARANTOR BODIES

Chapter I

The National Institute for Access to Public Information and Data Protection

Article 88. In regard to the creation, appointment procedure and operation of the Institute and the Advisory Council, the provisions of the General Law on Transparency and Access to Public Information, the Federal Law on Transparency and Access to Public Information and other applicable regulations must be observed.

Article 89. In addition to the faculties conferred upon the Institute under the General Law on Transparency and Access to Public Information, the Federal Law on Transparency and Access to Public Information and other regulations as may be applicable; it will have the following attributions:

I. Guaranteeing exercise of the right to protection of personal data held by obligated parties;

II. Interpreting this Law in the administrative sphere;

III. Taking cognizance of and deciding on petitions for review filed by data owners in accordance with the provisions of this Law and other applicable provisions on the matter;

IV. Taking cognizance of and deciding, by acting *ex officio* or on a properly grounded request from Guarantor bodies, on such petitions for review as found to be warranted given their interest and transcendence, in accordance with the provisions of this Law and other applicable provisions on the matter;

V. Taking cognizance and deciding on appeals filed by data owners, against resolutions issued by Guarantor bodies, in accordance with the provisions of this Law and other applicable provisions on the matter;

VI. Taking cognizance, pursuing and deciding on verification procedures;

VII. Establishing and enforcing coercive actions as are contemplated in this Law and other applicable provisions on the matter;

VIII. Denouncing any presumed infringements of this Law before the competent authorities and submitting any evidence it may have, if any;

IX. Coordinating with the competent authorities in order to process requests to exercise ARCO rights and any petitions for review submitted in an indigenous language, in the same language;

X. Ensuring, within its purview, that data owners from vulnerable groups are provided, all other things being equal, accessibility conditions that allow them to exercise the right to personal data protection;

XI. Preparing and publishing studies and research intended to foster and increase awareness on the subject matter of this Law;

XII. Providing technical support to data controllers in complying with the obligations set forth in this Law;

XIII. Publicizing and issuing recommendations, standards and best practices on the matters subject to regulation under this Law;

XIV. Overseeing and verifying compliance with the provisions contained in this Law,

XV. Administering the registry of schemes of best practices referred to in this Law, and issuing its operating rules;

XVI. Issuing, such being the case, the non-binding recommendations regarding Assessments of impact on the protection of personal data submitted to it;

XVII. Issuing the general provisions applicable to development of verification procedures;

XVIII. Conducting the assessments regarding notified best practices schemes, in order to decide whether they are to be recognized or validated for them to be recorded in the registry of best practices schemes, and in addition promoting their adoption.

XIX. Issuing, within the scope of its purview, the general administrative provisions intended to ensure due compliance with the principles, duties and obligations established in this Law, and ensuring proper exercise of data owners' rights;

XX. Entering into agreements with data controllers to develop programs intended to harmonize the processing of personal data in specific sectors, enhancing the protection of personal data, and undertaking any improvements regarding practices in this matter;

XXI. Defining and developing a certification system on the matter of the protection of personal data, this in accordance with that which is provided in the parameters referred to in this Law;

XXII. Presiding over the National System referred to in article 10 of this Law;

XXIII. Entering into agreements with the Guarantor bodies that will contribute to the achievement of the objectives contemplated in this Law and other applicable provisions on the matter;

XXIV. Undertaking actions and activities that foster awareness on the right to personal data protection, as well as of its prerogatives;

XXV. Designing and applying indicators and criteria in the performance assessment of data controllers in regard to compliance with this Law and other applicable provisions on the matter;

XXVI. Fostering training and updating of data controllers on the matter of the protection of personal data;

XXVII. Issuing general guidelines on proper personal data processing;

XXVIII. Issuing guidelines to harmonize the exercise of ARCO rights;

XXIX. Issuing general interpretation criteria to guarantee the right to protection of personal data;

XXX. Cooperating with other oversight authorities and domestic and international organizations, in order to provide assistance in the matter of personal data protection, in accordance with the provisions of this Law and other applicable regulations;

XXXI. Promoting, upholding and giving impulse to the exercise of the right to protection of personal data by the implementation and administration of the National Platform referred to in the General Law on Transparency and Access to Public Information and other applicable regulations;

XXXII. Filing, when so decided by the majority of the Commissioners, actions challenging the constitutionality of federal or state laws, as well as International Treaties signed by the President of the Republic and approved by the Senate, which infringe upon the right to personal data protection;

XXXIII. Filing, when so approved by a majority of the Commissioners; actions involving constitutional controversies as contemplated in article 105, section I, clause l) of the Political Constitution of the United Mexican States;

XXXIV. Cooperating with other domestic or international authorities to combat conducts relating to the unlawful processing of personal data;

XXXV. Designing, overseeing and, such being the case, operating the best practices system for the protection of personal data, as well as the certification system on this matter, by means of the regulations issued by the Institute for such purposes;

XXXVI. Entering into agreements with the Guarantor bodies and the data controllers that will assist in the achievement of the objectives contemplated in this Law and other applicable provisions on the matter; and

XXXVII. All others conferred upon it by this Law and other applicable laws and regulations.

Chapter II

Guarantor Bodies

Article 90. As regards the establishment, appointment procedure and operation of Guarantor bodies, the provisions of the General Law on Transparency and Access to Public Information and other applicable regulations will apply.

Article 91. For the purposes of this Law, and without prejudice to other attributions that may be conferred upon them in applicable regulations, the Guarantor bodies will have the following attributions:

I. Taking cognizance of, processing and resolving, within their respective purviews, on petitions for review filed by data owners, as provided in this Law and other applicable provisions on the matter;

II. Submitting a duly grounded petition to the Institute for the latter to take cognizance of such petitions for review which given their interest and transcendence warrant such action, this as provided in this Law and other applicable provisions on the matter;

III. Imposing coercive measures to ensure compliance with their resolutions;

IV. Fostering the widespread exercise of the right to personal data protection;

V. Coordinating with the competent authorities in order to process requests to exercise ARCO rights and any petitions for review submitted in an indigenous language, in the same language;

VI. Ensuring, within their respective purviews, that conditions of accessibility exist that enable data owners from vulnerable groups to exercise, all other things being equal, their right to protection of personal data;

VII. Preparing and publishing studies and research to disseminate and increase awareness on the subject matter of this Law;

VIII. Reporting to competent authorities on probable responsibility arising from non-compliance with the obligations contemplated in this Law and in other applicable provisions;

IX. Providing the Institute with the elements it requires to resolve on appeals submitted to it, this as provided in Title Ninth, Chapter II of this Law and other applicable provisions on the matter;

X. Entering into collaboration agreements with the Institute in order to attain the objectives contemplated in this Law and other applicable provisions on the matter;

XI. Overseeing compliance, within their respective purviews, with this Law and other applicable provisions on the matter;

XII. Undertaking the actions and activities intended to foster awareness on the right to personal data protection, as well as on its prerogatives;

XIII. Applying indicators and criteria to assess data controllers' performance in regard to compliance with this Law and other applicable provisions;

XIV. Fostering training and updating in regard to personal data protection among data controllers;

XV. Requesting the collaboration of the Institute as provided in article 89, section XXX of this Law;

XVI. Administering, within their purviews, the National Transparency Platform;

XVII. As found to be warranted, filing unconstitutionality actions challenging laws enacted by legislatures of the Federated States which violate the right to personal data protection: and

XVIII. Issuing, if found to be warranted, non-binding recommendations on the Assessment of impact on the protection of personal data submitted to them.

Chapter III

Coordination and Promotion of the Right to Personal Data Protection

Article 92. Data controllers must collaborate with the Institute and the Guarantor bodies, as the case may be, in the ongoing training and updating of all their public servants on the matter of protection of personal data, by providing courses, organizing seminars, workshops and any other type of teaching and training activities deemed to be pertinent.

Article 93. The Institute and Guarantor bodies, within their purviews, must:

I. Foster the inclusion of content on the right to protection of personal data in all curricular plans and programs, books and materials used in public schools of all levels and types, and also promote a culture regarding the exercise of and respect for this right,

II. Foster, in conjunction with institutions of higher education, the creation of research, dissemination and teaching centers dealing with the right to personal data protection which will promote awareness on this topic and provide assistance to the Institute and the Guarantor bodies in their substantive activities; and

III. Foster the creation of spaces of social and citizens' participation that stimulate the exchange of ideas among society, civic representative bodies and data controllers.

TITLE NINTH

CHALLENGE PROCEDURES IN REGARD TO THE PROTECTION OF PERSONAL DATA HELD BY OBLIGATED PARTIES

Chapter I

Common Provisions in Regard to Petitions for Review and Appeals

Article 94. The data owner or his/her representative may file a petition for review or appeal with the Institute or the Guarantor bodies, as appropriate, or else with the Transparency Unit, through the following means:

I. By submitting a brief at the address of the Institute or Guarantor bodies, as appropriate, or at the offices set up for such purposes;

II. By certified mail, return receipt requested;

III. On the forms issued for such purpose by the Institute or Guarantor bodies, as applicable;

IV. Through electronic means as authorized for such purpose;

V. Any other means that may be established by the Institute or the Guarantor bodies, as applicable.

There will be the presumption that the data owner has accepted being served notice through the same means used to file his/her brief, except if he/she provides proof that he/she has indicated a different channel for notification purposes.

Article 95. The data owner can provide proof of identity in any one of the following manners:

I. Official ID;

II. Advanced electronic signature or the electronic instrument that replaces it; or

III. Authentication mechanisms authorized by the Institute or Guarantor bodies, as applicable, under a general resolution published in the Official Gazette of the Federation or in the official daily bulletins and gazettes of the Federated States.

The use of an advanced electronic signature or the electronic instrument that replaces it will serve as waiver of the requirement to submit a copy of the ID document.

Article 96. When the data owner is acting through a representative, the latter must provide proof of legal capacity to act as such in the following terms:

I. If an individual, by means of a proxy letter signed in the presence of two witnesses to be submitted together with photocopies of the signatories' ID documents, or by means of a public instrument, or by a statement made by the data owner and his/her representative by appearance in person before the Institute;

II. If a legal entity, by means of a public instrument.

Article 97. A petition for review or an appeal involving the personal data of deceased persons, may be filed by any person providing proof that he/she has legal standing or a legitimate interest.

Article 98. In processing petitions for review and appeals, the notifications issued by the Institute and Guarantor bodies, as the case may be, shall produce effect as of the day they are served.

Notification may be served:

I. Personally when:

a) Involving the first notification;

b) It involves requiring the party to comply with an act;

c) It involves a request for submission of reports or documents;

d) It involves the resolution that brings the relevant proceeding to a close; and

e) All other cases provided by law.

II. By certified mail, return receipt requested or by digital means or systems authorized by the Institute or the Guarantor bodies, as applicable, which have been made public by a general resolution published in the Official Gazette of the Federation or official daily bulletins or gazettes of the Federated States, when involving requests, service of process, requests for reports or documents and resolutions which may be challenged.

III. By regular mail or regular electronic mail when involving acts other than those specified in the preceding sections; or

IV. By posting on the courthouse bulletin board, when the person to be notified cannot be found at his/her address, or when such address or that of his/her representative is not known.

Article 99. The statutes of limitations set forth in this Title will be counted as of the day following that on which the relevant notification produces effect.

Once the time periods set for the parties have run, the right that was to have been exercised will be deemed to have been forfeited, without the Institute having to charge default of appearance.

Article 100. The data owner, the data controller, the Guarantor bodies or any authority must comply with any requirements for submission of information within the time periods and under the terms established by the Institute or the Guarantor bodies, as applicable.

Article 101. In the event the data owner, the data controller, the Guarantor bodies or any authority refuse to heed or comply with the requirements, requests for information and documentation, service of process, summons or proceedings as notified by the Institute or Guarantor bodies, as applicable, or refuse to facilitate the ordered proceedings, or hamper the actions of the Institute or the Guarantor bodies, as applicable, they will forfeit their right to enforce their rights at any other stage in the course of the proceedings, and the Institute or the Guarantor bodies, as applicable, will assume that the facts on which the proceedings are based are true and shall resolve on the basis of the available elements.

Article 102. During the course of the proceedings held on petitions for review or appeals, the parties may offer the following evidence:

I. public documentary evidence;

II. private documentary evidence;

III. inspection evidence;

IV. expert evidence;

V. testimonial evidence;

VI. admissions against interest, excluding those of authorities;

VII. Photographic images, electronic web pages, written documents and other elements made available by science and technology; and

VIII. factual and presumptive evidence.

The Institute and the Guarantor bodies, as applicable, may seek to obtain any additional evidence deemed as necessary, subject to no limitation save those provided by law.

Chapter II

Petitions for Review Submitted to the Institute and the Guarantor bodies

Article 103. The data owner may, acting on his/her own motion or through his/her representative file a petition for review with the Institute, or such being the case, the Guarantor bodies or the Transparency Unit of the data controller cognizant of the request for ARCO rights, within a time period that cannot exceed fifteen days following that on which the term to provide a response has elapsed.

Once the time period established to respond to a petition for the exercise of ARCO rights has elapsed without a response having been issued, the data owner, or such being the case, his/her representative may file a petition for review within fifteen days following that on which the term for response expired.

Article 104. A petition for review will be processed when it falls within the following assumptions:

I. Should the personal data be classified as confidential without the characteristics provided for in applicable laws having been met;

II. The personal data have been declared to be non-existent;

III. The data controller states it is not the competent authority;

IV. The personal data delivered are incomplete;

V. Personal data are delivered that are not those requested;

VI. Personal data access, rectification, cancellation or opposition are denied;

VII. No response is given to a request to exercise ARCO rights within the time periods established in this Law and other applicable provisions on the matter;

VIII. Personal data are delivered in a mode or format other than the one requested, or in an incomprehensible format;

IX. The data controller objects to reproduction or delivery costs, or delivery times of the personal data;

X. The exercise of ARCO rights is hampered, despite notice having been given that it was found to have been warranted;

XI. A request for the exercise of ARCO rights is not processed; and

XII. In all other cases provided by law.

Article 105. The brief filed on a petition for review must contain the following minimal information:

I. The responsible area before whom the request to exercise ARCO rights was submitted;

II. The petitioner data owner's name or that of his/her representative, and such being the case that of a third party intervenor, if any, as well as the address or means used for service and notification purposes;

III. The date on which the response was notified to the data owner; or else, in the event response should be lacking, the date on which the request to exercise ARCO rights was submitted;

IV. The action for which review is sought and claims being made, as well as the reasons or grounds for the action,

V. Such being the case, a copy of the response being challenged and of the notification thereof;

VI. The documents providing the data owner's proof of identity and, such being the case, proof of identity and legal capacity of his/her representative.

The brief filed on a petition for review may be accompanied by any evidence and other elements that the data owner deems should be submitted for consideration by the Institute, or such being the case, the Guarantor bodies.

Under no circumstance will it be required that the data owner ratify the brief for review filed.

Article 106. Once the petition for review has been admitted, the Institute, or such being the case, the Guarantor bodies may seek conciliation between the data owner and the data controller.

Should they reach an agreement, this agreement will be set down in writing and will have binding effect. The petition for review will become moot and the Institute, or such being the case, the Guarantor bodies, must verify compliance with the relevant agreement.

Article 107. Once the petition for review has been admitted, and without prejudice to the provisions of article 65 of this Law, the Institute will strive to bring the parties to conciliation by following the procedure set forth herein below:

I. The Institute and the Guarantor bodies, as applicable, will request that the parties express through any means their will to conciliate, within a term not to exceed seven days, counted as of the date such resolution is notified, notice which will contain a summary of the petition for review and of the response of the data controller, if any, specifying the points on which there is agreement and the points of controversy.

Conciliation may take place by appearance in person, or by remote or local means of electronic communication or by any other means as determined by the Institute or the Guarantor bodies, as applicable. In any event, conciliation must be evidenced by any means that provide proof of its existence.

A minor data owner any one of whose rights, under the Law for the Protection of the Rights of Children and Adolescents linked to the Law and its Regulations, has been violated is exempted from the conciliation stage, unless his/her legal representation is fully evidenced;

II. Once both parties have agreed to the possibility of conciliation, the Institute and the Guarantor bodies, as applicable, will specify the place or means, date and time to conduct a conciliatory hearing, which must take place within ten days following that on which the Institute or the Guarantor bodies, as applicable, received from both parties the statement on their will to conciliate. At this hearing, the data owner and the data controller will strive to reconcile their interests.

The conciliator may at any time during the conciliation stage require that the parties submit, within a term of five days, any elements of proof he/she deems are necessary for conciliation.

The conciliator may adjourn the hearing once, at any time it deems such course of action pertinent, or at the request of both parties. Should the hearing be adjourned, the conciliator will set the date and time for it to continue within the following five days.

Minutes of the conciliation hearing will be drafted, wherein the results of the same will be set forth. The refusal by the data controller or the data owner or their respective representatives to sign the minutes will not affect their validity, and this will be expressly stated therein;

III. If either of the parties fails to appear at the conciliation hearing and justifies its absence within a term of three days, he/she/it will be summoned to appear at a second conciliation hearing which will take place within the following five days, should it fail to appear, the review proceedings will continue. When either one of the parties fails to appear at the conciliation hearing without providing justification, the proceeding will be carried on.

IV. Should no agreement be reached at the conciliation hearing, the review proceeding will continue;

V. Should an agreement be reached, such agreement will be set down in writing and will have binding effects. The review proceeding will become moot and the Institute, or such being the case, the Guarantor bodies must verify compliance with the relevant agreement; and

VI. Compliance with the agreement will bring the review proceeding to a close, otherwise, the Institute will reinstate the proceeding.

The statute of limitations referred to in the following article of this Law will be stayed during the time period allowed to comply with the agreement.

Article 108. The Institute and the Guarantor bodies will resolve on the review petition within a term not to exceed forty days, which may be extended only once for an additional twenty days.

Article 109. In the course of the proceedings referred to in this Chapter, the Institute and the Guarantor bodies must, as applicable, amend any deficient pleadings in the interest of the data owner, provided they do not alter the original content of the petition for review, nor modify the statements of fact or claims therein set forth, and must ensure that the parties are able to present their arguments and enter the evidence that serve as grounds for their claims.

Article 110. Should the brief for review filed by the data owner fail to comply with any one of the requirements set forth in article 105 of this Law, and the Institute or the Guarantor bodies, as applicable, do not have the means to supply for the deficiencies, they must request the data owner once, and within a term that cannot exceed five days counted as of the day following that on which the brief was filed, to provide the information to cure any such deficiencies.

The data owner will have a term that cannot exceed five days, counted as of the day following that on which he/she is served with notice of such request, to cure any such deficiencies, being forewarned that in the event he/she fails to comply with such request, the petition for review will be dismissed.

Such giving of notice will stay the period of time allowed to the Institute and Guarantor bodies to decide on the case, and the statutory term will continue to run as of the day following that on which such request is satisfied.

Article 111. The Institute, or such being the case, the Guarantor bodies may, by their resolutions:

I. Dismiss without consideration on the merits or dismiss the petition for review outright;

II. Uphold the data controller's response;

III. Revoke or modify the data controller's response; or

IV. Order delivery of the personal data, should the data controller have failed to do so.

Resolutions must specify, such being the case, the time periods and terms for compliance thereof and the procedures to ensure their enforcement. Data controllers must inform the Institute or, such being the case, the Guarantor bodies once compliance thereof has taken place.

Should the Institute, or such being the case, the Guarantor bodies fail to issue a resolution; the data controller's response will be understood as having been upheld.

When the Institute, or such being the case, the Guarantor bodies find in the course of the review proceedings that probable responsibility could have been incurred as a result of non-compliance with the obligations contemplated in this Law and other applicable provisions on the matter, they must inform the internal control body or the competent authority of this circumstance, for such entity to initiate, if found to be warranted, the relevant responsibility proceeding.

Article 112. A petition for review may be dismissed outright for lack of grounds when:

I. Filed late, after the time period established in article 103 of this Law has elapsed;

II. The data owner or his/her representative fail to provide proper proof of identity, and of legal capacity in the latter's case;

III. The Institute, or such being the case, the Guarantor bodies have issued a prior final and non-appealable ruling on the matter involved;

IV. It does not fall within the assumptions contemplated for a petition for review to be warranted listed in article 104 of this Law;

V. Remedial action is being pursued by the petitioner before the courts having jurisdiction, or such being the case, by a third party intervenor, against the action being challenged before the Institute or the Guarantor bodies, as applicable.

VI. The petitioner modifies or makes additional claims in the brief filed for review, solely as regards the new content; or

VII. The petitioner fails to evidence his/her legal standing.

Dismissal does not preclude the data owner's right to file a new petition for review with the Institute or the Guarantor bodies, as applicable.

Article 113. A petition for review may only be dismissed without consideration on the merits when:

I. The petitioner voluntarily asks for dismissal of action;

II. The petitioner dies;

III. Once the petition of review has been admitted, a cause for its inadmissibility as provided in this Law is found to have arisen;

IV. The data controller modifies or revokes its answer so as to render the petition for review moot; or

V. The petition for review becomes moot.

Article 114. The Institute and the Guarantor bodies must notify the parties and publicize the resolutions, in a public version, not later than the third day following their approval.

Article 115. The resolutions of the Institute and the Guarantor bodies will be binding, final and conclusive for data controllers.

Data owners may challenge such resolutions before the Federal Judiciary Branch by filing an *amparo* action for constitutional relief.

Article 116. In the cases involving resolutions issued on petitions for review by Guarantor bodies of the Federated States, private persons may opt to appear before the Institute to file an appeal as contemplated in this Law, or resort to filing an *amparo* action for constitutional relief before the Federal Judiciary Branch.

Chapter III

Appeals Brought before the Institute

Article 117. The data owner may, by acting on his/her own behalf or through his/her representative, challenge the resolution issued on a petition for review by the Guarantor body before the Institute, by filing an appeal.

The appeal may be filed with the Guarantor body that issued the resolution or with the Institute, within a term of fifteen days counted as of the day following the date on which notification of the challenged resolution took place.

The Guarantor bodies must remit the appeal brief to the Institute on the day following that of its reception, together with the case file that served as a basis for the resolution being challenged. The Institute will resolve on the basis of any evidentiary elements it deems as appropriate.

Article 118. An appeal will be found to be warranted when challenging resolutions issued by Guarantor bodies of the Federated States which:

I. Classify personal data without complying with the characteristics specified in applicable laws;

II. Declare the non-existence of personal data; or

III. Involve a refusal in regard to personal data, that is to say:

a) Personal data delivery is incomplete;

b) Personal data are delivered other than those requested;

c) Access to, rectification and cancellation of, or opposition to personal data processing is denied;

d) Personal data are delivered or made available in an incomprehensible format;

e) The data owner expresses his/her objection to the costs for reproduction, delivery, or delivery times of the personal data; or

f) A specific processing is indicated that contravenes the provisions of article 54 of this Law.

Article 119. The brief of appeal must include the following essential and required information:

I. The responsible area to which the request for the exercise of ARCO rights was submitted;

II. The Guarantor body that issued the resolution being challenged;

III. The name of the appellant data owner or that of his/her representative and, that of the third party intervenor, if any, as well as the address or means designated for notification purposes;

IV. The date on which the data owner was notified of the resolution;

V. The act being challenged and the claims made, as well as the legal grounds and reasons for the appeal;

VI. Such being the case, a copy of the resolution being challenged and the relevant notification; and

VII. Proof of identity of the data owner, and such being the case, proof of identity and legal capacity of his/her representative.

Appellant may submit his/her brief together with any evidentiary and other elements it deems are appropriate for consideration by the Institute.

Article 120. The Institute must resolve on the appeal within a term not to exceed thirty days counted as of the day following that on which the appeal is filed, period which may be extended only once for a like term.

Article 121. In the proceedings referred to in this Chapter, the Institute must amend any deficient pleadings in the interest of the data owner, provided it does not alter the original content of the appeal brief, nor modify the statements of fact or claims therein set forth, and must ensure that the parties are able to present their arguments and enter the evidence that serve as grounds for their claims.

Article 122. Should the appeal brief filed by the data owner fail to comply with any one of the requirements set forth in article 119 of this Law, and the Institute does not have the means to supply for the deficiencies, it must request the data owner once and within a term that cannot exceed five days, counted as of the day following that on which the brief was filed, to provide the information to cure any such deficiency.

The data owner will have a term that cannot exceed fifteen days, counted as of the day following that on which he/she is served with notice of the request, to cure any such deficiencies, being forewarned that in the event he/she fails to comply with such request, the appeal will be dismissed.

Such giving of notice will stay the period of time allowed to the Institute to decide on the case, and the statutory term will continue to run as of the day following that on which such request is satisfied.

Article 123. Once the evidence phase in the proceeding has concluded, the Institute will make the records of the proceedings available to the parties, and will allow them a term of five days, counted as of the day notification is given on this ruling as mentioned in this article, to enter their arguments.

Article 124. The resolutions of the Institute may:

I. Dismiss without consideration or dismiss the appeal outright,

II. Uphold the resolution of the Guarantor body;

III. Revoke or modify the resolution of the Guarantor Body; or

IV. Order delivery of the personal data, should the data controller have failed to do so.

Resolutions must specify, such being the case, the time periods and terms for compliance thereof and the procedures to ensure their enforcement. Guarantor bodies must inform the Institute once compliance thereof has taken place.

Should the Institute fail to issue a resolution within the term established in this Chapter, the challenged resolution will be understood as having been upheld.

When the Institute finds in the course of the appeal proceedings that probable responsibility could have been incurred as a result of non-compliance with the obligations contemplated in this Law and other applicable provisions on the matter, it must inform the internal control body or the competent authority of this circumstance, for such entity to initiate, if found to be warranted, the relevant responsibility proceeding.

The coercive action contemplated in this Law will be applicable to ensure compliance with the resolutions issued on the appeals. Such enforcement measures must be specified in the resolution.

Article 125. An appeal may be dismissed outright for lack of grounds when:

I. Filed late, after the time period established in article 117 of this Law has elapsed;

II. The Institute has issued a prior final and conclusive resolution on the matter involved;

III. It does not fall within the assumptions contemplated for an appeal to be warranted that are listed in article 118 of this Law;

IV. Remedial action is being pursued by the data owner before the courts having jurisdiction, or such being the case, by a third party intervenor, against the action being challenged, or

V. The appellant modifies or makes additional claims in the appeal brief filed, solely as regards the new content.

Article 126. An appeal may be dismissed without consideration on the merits only when:

I. Appellant voluntarily asks for dismissal of action;

II. Appellant dies;

III. The Guarantor body modifies or revokes its answer so as to render the appeal moot; or

IV. Once the appeal has been admitted, a cause for its inadmissibility is found to have arisen as provided for in this Law.

Article 127. In the cases in which as a result of an appeal the resolution of the Guarantor body is modified or revoked, the Guarantor body must issue a new ruling that takes into consideration the guidelines set in the decision rendered on the appeal, and must do so within a term of fifteen days, counted as of the day following that on which it is notified or becomes cognizant of the decision on the appeal.

Article 128. Guarantor bodies will be responsible, within their purviews, for monitoring and overseeing due compliance by the data controller with the new resolution issued on the appeal as provided for in this Law.

Article 129. The resolutions of the Institute will be binding, final and conclusive for data controllers and Guarantor bodies.

Data owners may challenge such resolutions before the Federal Judiciary Branch by filing an amparo action for constitutional relief.

Chapter IV

Assertion of Jurisdiction over Petitions for Review

Article 130. For the purposes of this Law, the Plenum of the Institute may, when so authorized by a majority of the Commissioners, by acting *ex officio* or on a duly grounded request of Guarantor bodies, exercise the authority to assert its jurisdiction to take cognizance of any petitions for review regarding personal data protection over which Guarantor bodies have original jurisdiction that are pending resolution, which given their interest and transcendence warrant this action, this as provided in this Law and other applicable provisions.

Petitioners may inform the Institute on the existence of petitions for review regarding which it may take cognizance by acting *ex officio*.

As regards the general guidelines and criteria of compulsory compliance which the Institute must issue to determine the petitions for review of interest and transcendence of which it must take cognizance, in accordance with the General Law on Transparency and Access to Public Information; and when asserting its jurisdiction over petitions for review regarding the protection of personal data, the following factors must be taken into account:

I. The purpose for which the personal data are processed;

II. The number and type of data owners involved in the processing of the personal data by the data controller;

III. The sensitivity of the personal data processed;

IV. The possible consequences that may result from improper or indiscriminate processing of the personal data; and

V. The relevance of the personal data processing, taking into account the social and economic impact of the same, and the public interest involved in taking cognizance of the petition for review over which jurisdiction is asserted.

Article 131. In exercising its authority to assert its jurisdiction as contemplated in this Chapter, the Institute must state the facts and provide grounds for deciding that the case is of such relevance, novelty or complexity, that the decision rendered on it will have a substantial impact on the resolution of future cases so as to ensure that the right to personal data protection held by obligated parties is effectively safeguarded.

In the event the Guarantor body of the Federated state is the obligated party against whom the petition for review is filed, it must inform the Institute of this circumstance within a term not to exceed three days as of the date the petition is filed. The Institute will assert its jurisdiction and resolve on such petitions for review as provided for in this Chapter.

Article 132. The reasons given by the Institute to exercise its authority to assert its jurisdiction over a case, will constitute just a preliminary study to determine whether the matter meets the legal and constitutional

requirements of interest and transcendence as are provided in the preceding article, and therefore, it will not be necessary for them to be included when giving consideration to the merits of the case.

Article 133. The Institute will issue general guidelines and criteria of compulsory compliance in order to determine the petitions for review of interest and transcendence of which it must take cognizance, as well as internal procedures for their processing, taking into account maximum time periods established to process petitions for review.

Article 134. The authority to assert jurisdiction vested in the Institute must be exercised in adherence to the following rules:

I. When acting *ex officio*, the Plenum of the Institute may, when so approved by the majority of its Commissioners, assert its jurisdiction at any time, as long as the competent Guarantor body has not yet resolved on the petition for review. To do so, it will give notice to the parties and request the Guarantor body to turn over the case file, or

II. Should a Guarantor body of a Federated State make the petition [for the Institute] to assert jurisdiction, this body will have a maximum term of five days, except for that which is provided in the last paragraph of article 105 of this Law, to request the Institute to examine, and if found to be warranted, assert its jurisdiction over the case submitted to its consideration.

Once the above mentioned term has elapsed, the right of the Guarantor body to petition the Institute to assert its jurisdiction will be considered as having been forfeited.

The Institute will have a term not to exceed ten days to decide whether it will exercise its authority to assert jurisdiction, and should it decide to do so, it will notify the parties and request that the petition for review case file be turned over.

Article 135. Assertion of jurisdiction over the petition of review will stay the term Guarantor bodies have to resolve on it. Such term will continue to run as of the day following that on which the Institute notifies its determination not to assert jurisdiction over the petition for review.

Article 136. Prior to any determination by the Institute on assertion of jurisdiction as mentioned above, the Guarantor body of the Federated State that had original jurisdiction over the case must complete its review on all aspects that need to be considered prior to examination of the merits, except in the event that the important and transcendent issues involve the question of its admissibility.

If the Plenum of the Institute, when approved by a majority of the Commissioners, decides to assert jurisdiction, it will take cognizance or undertake the review and address the merits of the case over which jurisdiction has been asserted.

The Commissioner or Commissioners who vote against assertion of jurisdiction will not be precluded from expressing their opinion on the merits of the case.

Article 137. The resolution of the Institute will be final and conclusive for the Guarantor body and the obligated party involved.

Private persons may at all times challenge the resolutions of the Institute before the federal courts.

Article 138. The Legal Advisory Office of the President is the sole agency having the authority to petition the Supreme Court of Justice of the Nation for review on matters regarding national security, in the event the resolutions issued by the Institute on the actions described in this title may place national security in jeopardy.

This review on matters involving national security will be processed as provided in Chapter V below, entitled "Petition for Review on Matters Involving National Security".

Chapter V

Petition for Review on Matters Involving National Security

Article 139. The Legal Advisor to the President may file a petition for review on matters involving national security directly with the Supreme Court of Justice of the Nation, when it deems that the resolutions issued by the Institute jeopardize national security.

The petition must be filed within the seven days following that on which the Guarantor body gives notice of the resolution to the obligated party. The Supreme Court of Justice of the Nation will determine, forthwith, if stay of enforcement of the resolution is warranted, and will decide on admissibility or dismissal of the petition within the following five days.

Article 140. The Legal Advisor to the President must specify, in the brief filed, the resolution being challenged, include the statements of fact and considerations of law that serve as grounds to consider that national security is being jeopardized, and provide the needed evidence.

Article 141. Any information that is reserved or confidential that is requested, such being the case, by the Supreme Court of Justice of the Nation which is considered as essential to decide on the matter, must be maintained as such, and will not be made available in the case file, except in the events contemplated in article 120 of the General Law on Transparency and Access to Public Information.

The Justices must have access to the classified information at all times in order to decide on its nature, as required. Access will take place in accordance with previously established regulations regarding the preservation or safekeeping of the information by obligated parties.

Article 142. The Supreme Court of Justice of the Nation will exercise full jurisdiction to decide and under no circumstance can the case be remanded.

Article 143. Should the Supreme Court of Justice of the Nation uphold the resolution challenged, the obligated party must comply with it as set forth in the relevant provision of this Law.

In the event the resolution is revoked, the Institute must act as ordered by the Supreme Court of Justice of the Nation.

Chapter VI

Interpretation Criteria

Article 144. Once the resolutions issued on the actions submitted to its jurisdiction have become, final, conclusive and immediately available for execution, the Institute may issue the interpretation criteria deemed by it to be pertinent in the light of such resolutions, this as provided in the General Law on Transparency and Access to Public Information and other applicable regulations.

The Institute may issue criteria that derive from resolutions that have become final and conclusive, to serve as guidelines for Guarantor bodies, criteria which will become binding by reiteration when the Institute rules the same way on three analogous and consecutive cases, by decision of at least two thirds of the Plenum of the Institute.

Article 145. Criteria must be drafted with a heading, a text and the precedent or precedents that, such being the case, have given rise to their issuance.

Any criterion issued by the Institute must contain a control code for proper identification.

TITLE TENTH

VERIFICATION AUTHORITY OF THE INSTITUTE AND GUARANTOR BODIES

Sole Chapter

Verification Procedure

Article 146. The Institute and the Guarantor bodies, each within their respective purviews, will have the authority to oversee and verify compliance with the provisions contained in this Law and other regulations deriving herefrom.

When exercising their oversight and verification functions, the personnel of the Institute or, such being the case, of the Guarantor bodies will be under the obligation of maintaining the confidentiality of the information to which they have access as a result of the relevant verification.

The data controller cannot deny access to the documentation requested in the course of verification, or to its databases containing personal data, nor can it invoke reservation or confidentiality of the information.

Article 147. Verification will commence:

I. *Ex officio*, when the Institute or the Guarantor bodies have indications allowing for the presumption, duly grounded in fact and law, of existing violations to applicable laws; or

II. Upon denouncement made by a data owner, when he/she considers that he/she has been affected by the actions of the data controller that may contravene the provisions of this Law and other applicable regulations; or such being the case, made by any person when such person becomes aware of possible non-compliance with the obligations contemplated in this Law and other applicable regulations on the matter.

The right to denounce expires after a year has elapsed counted as of the day following that on which the acts or omissions that serve as grounds for the same occurred. When the acts or omissions are of continued duration, the term shall run as of the working day following that on which the last action took place.

Verification will be dismissed outright under the same hypotheses provided in this Law that are applicable to petitions for review or appeals.

Verification will not be admitted under the same hypotheses provided in this Law that are applicable to petitions for review or appeals.

The Institute or Guarantor bodies may conduct, prior to verification, preliminary investigations, in order to obtain the elements required to ground in law and fact the relevant initial resolution.

Article 148. Denouncement is subject to no other requirements save those specified herein below:

I. Name of denouncer or, such being the case, of his/her representative;

II. The address of, or means for notification to the denouncer;

III. The statements of fact which provide grounds for the denouncement and any evidence on hand that serves as proof of the claims being made;

IV. Specification of the data controller being denounced and its address or, such being the case, data leading to its identification and/or location;

V. The denouncer's signature or, such being the case, that of his/her representative. Should denouncer not know how to sign, his/her fingerprint will suffice.

A denouncement may be filed by submission of a brief or by using the forms, electronic or any other means established for this purpose by the Institute or the Guarantor bodies, as applicable.

Upon reception of a denouncement the Institute or the Guarantor bodies, as applicable, must acknowledge receipt thereof. Notice of the relevant resolution must be given to the denouncer.

Article 149. Verification will commence with a written order that includes the statements of fact and law that provide the grounds for the action being taken by the Institute or the Guarantor bodies, the purpose of which is to request the data controller to provide the documentation and information required relating to the alleged violation and/or to appear at the data owner's offices or facilities, or such being the case, at the location where the relevant personal data databases are found.

To conduct verification at national security and police offices, the relevant resolution must be approved by a qualified majority of the Commissioners of the Plenum of the Institute, or of the members of the Guarantor bodies of the Federated States, as applicable, and in addition it must include in precise detail the statements of fact and considerations of law that provide cause for the proceeding, and the information obtained must be reserved solely for the exclusive use of the authority and for the purposes set forth in article 150.

Verification must have a maximum duration of 50 days.

The Institute or the Guarantor bodies may order precautionary measures to be taken, should they find in the course of the verification that damage in regard to the protection of personal data is imminent or might be irreparable, provided they do not prevent compliance with functions nor seizure of the databases of obligated parties.

Such measures will be ordered solely for corrective purposes, be temporary and will remain in place until the obligated parties act upon the recommendations issued by the Institute or the Guarantor bodies, as applicable.

Article 150. The verification procedure will come to a close with the resolution issued by the Institute or the Guarantor bodies, wherein the measures to be adopted by the data controller and the term to do so will be set forth.

Article 151. –Data controllers may voluntarily submit to audits conducted by the Institute or the Guarantor bodies, as applicable, the purpose of which is to verify adaptation, suitability and efficacy of the controls, measures and mechanisms implemented in order to comply with the provisions set forth in this Law and other applicable regulations.

The audit report must include an opinion on the suitability of the measures and controls implemented by the data controller, identify any deficiencies, and in addition propose supplementary corrective action, or else any recommendations found to be advisable.

TITLE ELEVENTH

COERCIVE ACTION AND RESPONSIBILITIES

Chapter I

Coercive Action

Article 152. In complying with the resolutions issued by the Institute or the Guarantor bodies, as applicable, the latter and the data controller, such being the case, must adhere to the provisions of Chapter VI of Title Eighth of the General Law on Transparency and Access to Public Information.

Article 153. The Institute and the Guarantor bodies may take the following coercive action to enforce compliance with their decisions:

I. Public warning, or

II. Monetary sanction, in the range of one hundred and fifty to one thousand five hundred times the daily value of the Unit of Measure and Updating.

Non-compliance by obligated parties will be publicized on the web portals on transparency obligations of the Institute and the Guarantor bodies and will be taken into consideration when they are subject to assessment.

In the event that non-compliance with the determinations of the Institute and Guarantor bodies involves a presumed crime or one of the conducts specified in article 163 of this Law, they must report the facts to the appropriate authorities. Monetary enforcement measures cannot be satisfied with public funds.

Article 154. Should compliance with the resolution not take place despite enforcement of the coercive action contemplated in the preceding article, compliance will be required from the senior official, allowing him/her five days to order immediate compulsory compliance.

Should non-compliance persist, they will be applied on the coercive action specified in the preceding article (T. note: *sic* in the original). Once the term has expired without compliance having taken place, this circumstance will be reported to the competent authority in the matter of responsibility.

Article 155. The coercive action referred to in this Chapter must be taken by the Institute or the Guarantor bodies, acting on their own or with the assistance of the competent authority, in accordance with the procedures set forth in the relevant statutes.

Article 156. The monetary sanctions established by the Institute and the Guarantor bodies will be collected by the Tax Administration Service of the Departments of Finance of the Federated States, as applicable, through statutory procedures.

Article 157. To qualify the coercive action contemplated in this Chapter, the Institute and the Guarantor bodies must take into consideration:

I. The gravity of the data controller's fault, determined on the basis of the damage caused, indications of intent, the time the determinations issued by the Institute or the Guarantor bodies were disregarded, and its negative effect on the exercise of their attributions;

II. The infringer's financial condition; and

III. Recidivism.

The Institute and the Guarantor bodies will establish, through general guidelines, the attributions of the areas in charge of qualifying the gravity of instances of non-compliance with their determinations, and of giving notice and enforcing the coercive action to be applied and implemented, as contemplated in this article.

Article 158. In the event of recidivism, the Institute or the Guarantor bodies may impose a monetary sanction equal to twice that which may have been set by the Institute or the Guarantor bodies.

A recidivist will be the person or entity who incurs in an infringement of the same type or nature as that of a previously sanctioned infringement.

Article 159. Coercive action must be applied and implemented within a maximum term of fifteen days, counted as of the date it is notified to the infringing party.

Article 160. A public warning will be imposed by the Institute or the Guarantor bodies and will be carried out by the senior official of the infringing party involved.

Article 161. The Institute and the Guarantor bodies may require that the infringing party provide the information required to determine his/her financial situation, being forewarned that should he/she fail to do so, monetary sanctions shall be quantified on the basis of the information available, this being understood as that which can be found in public registries, that contained in information media or on their own web pages, and

generally, any information providing evidence of his/her financial situation; the Institute or the Guarantor bodies having the authority to require from the competent authorities submission of such information deemed as essential for such purposes.

Article 162. Applicable remedial action filed before the federal courts or before the appropriate state courts is available against the imposition of coercive action.

Chapter II

Sanctions

Article 163. The following are causes giving rise to sanction as a result of non-compliance with the obligations as set forth in this Law:

I. Acting with negligence, dolus or bad faith in the handling of requests for exercise of ARCO rights;

II. Failing to comply with the time periods contemplated in this Law to respond to requests to exercise ARCO rights or to uphold the relevant right;

III. Using, deleting, disclosing, concealing, altering, distorting, destroying or rendering personal data useless, in whole or in part, and improperly, that are held under the party's custody or to which he/she has access or has knowledge of by reason of his/her job, office or commission;

IV. Willfully processing personal data in contravention of the principles and duties established in this Law;

V. Not having a privacy notice, or else, omitting in the same any one of the elements referred to in article 27 of this Law, as the case may be, and other applicable provisions on the matter;

VI. Classifying, with dolus or negligence, personal data as confidential without these meeting the characteristics set forth in applicable laws. The sanction will only be warranted as a result of a prior final determination that is not subject to appeal regarding the classification criterion of the personal data;

VII. Failing to comply with the duty of confidentiality established in article 42 of this Law;

VIII. Failing to establish the security measures as are set forth in articles 31, 32 and 33 of this Law;

IX. When the personal data are violated are a result of the failure to implement the security measures as are set forth in articles 31, 32, and 33 of this Law;

X. Transferring personal data in contravention of the provisions of this Law;

XI. Obstructing verification action conducted by the authority;

XII. Creating personal data bases in contravention of the provisions of article 5 of this Law;

XIII. Failing to comply with the resolutions issued by the Institute and the Guarantor bodies; and

XIV. Failing to submit the annual report and other reports referred to in article 44, section VII of the General Law on Transparency and Access to Public Information, or else to do so extemporaneously.

Causes giving rise to responsibility contemplated in sections I, II, IV, VI, X, XII and XIV, as well as recidivism in the actions contemplated in the remaining sections of this article, will be considered to be grave for administrative sanctioning purposes.

In the event the presumed infringement is committed by a member of a political party, the investigation, and such being the case, sanction will be conducted and applied by the competent electoral authority.

Monetary sanctions cannot be settled with public funds.

Article 164. The conducts referred to in the preceding article will be reported to the competent authority for it to impose or enforce the sanction.

Article 165. Any responsibility that is established under the relevant administrative proceedings, arising from the infringement of the provisions of article 163 of this Law, is independent from any civil, criminal or other liabilities which may arise from the same actions.

Said responsibilities and liabilities will be determined independently, through the proceedings contemplated in applicable laws; and the sanctions which are imposed by the competent authorities, such being the case, will also be enforced independently.

To these ends, the Institute or the Guarantor bodies may denounce before the competent authorities any action or omission that is in violation of this Law, and submit the evidence considered to be pertinent, as provided in applicable laws.

Article 166. When non-compliance by political parties is involved, the Institute or competent Guarantor body will inform the National Electoral Institute, or the competent electoral local public bodies of the Federated States, as applicable, for them to resolve as pertinent, without prejudice to the sanctions established for political parties in applicable laws.

When possible infringements are involved that relate to public trusts or funds, the Institute or competent Guarantor body must inform the internal control body of the obligated party related to such trusts or funds, when they are public servants, for them to implement the administrative procedures found to be warranted.

Article 167. Where the presumed infringer is a public servant, the Institute or the Guarantor body must remit to the competent authority a file containing all the items of evidence that provide grounds for the presumed administrative responsibility together with the relevant denouncement.

The authority taking cognizance of the matter must inform the Institute or the Guarantor body, as applicable, when the proceeding is brought to an end and on the enforcement of the sanction, such being the case.

In order to carry out the proceeding mentioned in this article, the Institute or the relevant Guarantor body must draft a denouncement addressed to the office of the comptrollership, internal control body or equivalent

area, containing an accurate description of the actions or omissions which, in its opinion, have an impact on the proper application of this Law and which may entail probable responsibility.

Moreover, it must prepare a case file containing any such evidentiary elements deemed to be pertinent that may provide grounds to prove the existence of probable responsibility. To this end evidence must be provided of the causal nexus existing between the facts in issue and the evidence submitted.

The denouncement and the file must be sent to the comptrollership office, internal control body or equivalent area within the fifteen days following that on which the Institute or the relevant Guarantor body becomes cognizant of the facts.

Article 168. In the event that non-compliance with the determinations of the Guarantor bodies entails presumed commission of a crime, the relevant Guarantor body must file charges before the competent authority.

TRANSITIONAL PROVISIONS

First. This Law will enter into force on the day following its publication in the Official Gazette of the Federation.

Second. The Federal Law on Transparency and Access to Public Information, the other federal laws and the laws in force of the Federated States on the matter of the protection of personal data must be made consistent with the provisions contemplated in this statute within the term of six months following the entry into force of this Law.

In the event the Congress of the Union or the Legislatures of the Federated States fail, in whole or in part, to make the required legislative changes within the term provided for in the preceding paragraph, this Law will become directly applicable, the continued application of preexisting laws being possible to supply for any deficiencies in all things that do not contravene this Law, until the condition imposed by this article is satisfied.

Third. The Chamber of Deputies and the Legislatures of the Federated States must, within their respective purviews, set aside the budget appropriations required for operation of this Law and provide for the specific budget items in the Federal Expenditure Budget and the State Expenditure Budgets, as applicable, for the fiscal year following that of its entry into force.

Fourth. All federal, state and municipal provisions on the matter of protection of personal data that contravene those provided in this Law are repealed.

Fifth. The Institute and the Guarantor bodies must issue the guidelines referred to in this Law and publish them in the Official Gazette of the Federation, or in their local official daily bulletins or gazettes, respectively, not later than one year after the entry into force of this Executive Order.

Sixth.- The National System for Transparency, Access to Information and Personal Data Protection must issue the National Program for Personal Data Protection referred to in this Law and publish it in the Official Gazette of the Federation within one year following the entry into force of this Executive Order, notwithstanding the exercise of other attributions arising from the General Law on Transparency and Access to Public Information.

Seventh. Relevant obligated parties must process, issue or modify their internal regulations within eighteen months following the entry into force of this Law.

Eighth. The procedures and time periods in effect and applicable in this matter cannot be reduced or extended by regulations issued by the Federated States to the detriment of data owners.

Mexico City, on December 13, 2016.- Senator **Pablo Escudero Morales,** Chairman.- Deputy **Edmundo Javier Bolaños Aguilar,** Chairman.- Senator **Lorena Cuéllar Cisneros,** Secretary.- Deputy **María Eugenia Ocampo Bedolla,** Secretary.- Sígnatures."

Complying with the provisions set forth in section I of Article 89 of the Political Constitution of the United Mexican States and for its due publication and observance I issue this Executive Order at the Residence of the President of the Republic, in Mexico City, on January twenty fourth, two thousand and seventeenth.- **Enrique Peña Nieto.-** Signature.- The Secretary of Internal Affairs, **Miguel Ángel Osorio Chong.-** Signature.