EXECUTIVE POWER

SECRETARY OF THE INTERIOR

DECREE by which the General Law of Protection of Personal Data in Possession of Obliged Subjects is issued.

In the margin a seal with the National Shield, which says: United Mexican States.- Presidency of the Republic.

ENRIQUE PEÑA NIETO, President of the United Mexican States, to its inhabitants know:

That the Honorable Congress of the Union has served to address me the following

DECREE

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

THE GENERAL LAW ON THE PROTECTION OF PERSONAL DATA IN POSSESSION OF SUBJECTS IS ISSUED OBLIGATED

Sole Article.- The General Law on the Protection of Personal Data in Possession of Obliged Subjects is issued.

General Law on Protection of Personal Data in Possession of Obliged Subjects

FIRST TITLE

GENERAL DISPOSITION

Chapter I

Of the Object of the Law

Article 1. This Law is of public order and general observance throughout the Republic, regulating articles 6, Base A and 16, second paragraph, of the Political Constitution of the United Mexican States, in matters of data protection. personal in possession of obligated subjects.

All the provisions of this General Law, as appropriate, and within the scope of its competence, are of application and direct observance for obligated subjects belonging to the federal order.

The Institute will exercise the powers and authorities granted by this Law, regardless of the granted in the other applicable provisions.

Its purpose is to establish the bases, principles and procedures to guarantee the right that every person to the protection of their personal data, in possession of obligated subjects.

Subjects bound by this Law, at the federal, state and municipal levels, are any authority, entity, body and agency of the Executive, Legislative and Judicial Powers, autonomous bodies, political parties, trusts and public funds.

Unions and any other natural or legal person that receives and exercises public resources or performs acts of authority at the federal, state and municipal level will be responsible for personal data, in accordance with the applicable regulations for the protection of personal data in possession of individuals.

In all other cases other than those mentioned in the preceding paragraph, natural and legal persons will be subject to the provisions of the Federal Law on Protection of Personal Data Held by Private Parties.

Article 2. The objectives of this Law are:

I Distribute powers between the Guarantor Agencies of the Federation and the Federal Entities, in terms of protection of personal data held by regulated entities;

II. Establish the minimum bases and homogeneous conditions that will govern the processing of personal data and the exercise of the rights of access, rectification, cancellation and opposition, through simple and expeditious procedures;

III. Regulate the organization and operation of the National System of Transparency, Access to Information and Protection of Personal Data referred to in this Law and the General Law of Transparency and Access to Public Information, in relation to its functions for data protection personal in possession of obligated subjects;

IV. Guarantee the observance of the principles of protection of personal data provided in this Law and other provisions that are applicable in the matter;

v. Protect personal data in possession of any authority, entity, body and agency of the Executive, Legislative and Judicial Powers, autonomous bodies, political parties, trusts and public funds, of the Federation, the Federal Entities and the municipalities, with the purpose of regulate its due treatment;

SAW. Guarantee that every person can exercise the right to the protection of personal data;

VII. Promote, encourage and spread a culture of protection of personal data;

VII. Establish the mechanisms to guarantee compliance and the effective application of the enforcement measures that correspond to those conducts that contravene the provisions set forth in this Law, and

IX. Regulate the means of challenge and procedures for the filing of actions of unconstitutionality and constitutional controversies by the local Guarantor Agencies and the Federation; in accordance with their respective powers.

Article 3. For the purposes of this Law, it shall be understood as:

I **Areas:** Instances of the obligated subjects provided for in the respective internal regulations, organic statutes or equivalent instruments, which have or may have, treat, and be responsible or in charge of personal data;

II. **Privacy notice:** Document available to the holder in physical, electronic or in any format generated by the person in charge, from the moment in which their personal data is collected, in order to inform them of the purposes of their treatment;

III. **Databases:** Ordered set of personal data referring to an identified or identifiable natural person, conditioned to certain criteria, regardless of the form or modality of its creation, type of support, processing, storage and organization;

IV. **Blocking:** The identification and conservation of personal data once the purpose for which they were collected has been fulfilled, with the sole purpose of determining possible responsibilities in relation to their treatment, until their legal or contractual prescription period. During this period, the personal data may not be processed and after this, it will be canceled in the corresponding database;

v. **Transparency Committee:** Body referred to in article 43 of the General Law of Transparency and Access to Public Information;

SAW. **Cloud computing:** Model of external provision of computing services on demand, which implies the provision of infrastructure, platform or computer program, distributed in a flexible way, through virtual procedures, in dynamically shared resources;

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

VII. **Consent:** Manifestation of the free, specific and informed will of the owner of the data through which the treatment of the same is carried out;

IX. **Personal data:** Any information concerning an identified or identifiable natural person. A person is considered to be identifiable when their identity can be determined directly or indirectly through any information;

X. **Sensitive personal data:** Those that refer to the most intimate sphere of its owner, or whose improper use may give rise to discrimination or entail a serious risk for it.
In an enunciative but not limited way, personal data that may reveal aspects such as racial or ethnic origin, present or future health status, genetic information, religious, philosophical and moral beliefs, political opinions and sexual preference are considered sensitive;

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

XII. **Days:** business days;

XIII. **Dissociation:** The procedure by which the personal data cannot be associated with the owner or allow, due to its structure, content or degree of disaggregation, the identification of the same;

XIV. Security document: Instrument that describes and gives a general account of the technical, physical and administrative security measures adopted by the person in charge to guarantee the confidentiality, integrity and availability of the personal data held;

XV. **Manager:** The natural or legal person, public or private, outside the organization of the person in charge, who alone or jointly with others processes personal data in the name and on behalf of the person in charge;

XVI. **Impact assessment on the protection of personal data:** Document through which the regulated entities that intend to put into operation or modify public policies, programs, systems or computer platforms, electronic applications or any other technology that implies the intensive or relevant treatment of personal data , assess the real impacts regarding certain processing of personal data, in order to identify and mitigate possible risks related to the principles, duties and rights of the owners, as well as the duties of those responsible and in charge, provided for in the applicable regulations;

XVII. Public access sources: Those databases, systems or files that by law can be consulted publicly when there is no impediment by a limiting rule and without further requirement than, where appropriate, the payment of a consideration, fee or contribution. It will not be considered a source of public access when the information contained therein is obtained or has an illegal origin, in accordance with the provisions established by this Law and other applicable regulations;

XVIII. Institute: National Institute of Transparency, Access to Information and Protection of Personal Data, which is the guarantor body of the Federation in matters of protection of personal data held by regulated entities;

XIX. Compensatory measures: Alternative mechanisms to make the privacy notice known to the owners, through its dissemination by mass media or other wide-ranging media;

XX. **Security measures:** Set of administrative, technical and physical actions, activities, controls or mechanisms that allow personal data to be protected;

XXI. Administrative security measures: Policies and procedures for the management, support and review of information security at the organizational level, the identification, classification and secure deletion of information, as well as the awareness and training of personnel, in terms of data protection. personal information;

XXII. Physical security measures: Set of actions and mechanisms to protect the physical environment of personal data and the resources involved in its treatment. By way of example but not limitation, the following activities should be considered:

a) Prevent unauthorized access to the perimeter of the organization, its physical facilities, areas reviews, resources and information;

b) Prevent damage or interference to physical facilities, critical areas of the organization, resources and information;

c) Protect mobile resources, laptops and any physical or electronic support that may leave the organization, and

d) Provide the equipment that contains or stores personal data with effective maintenance, which ensures its availability and integrity;

XXIII. Technical security measures: Set of actions and mechanisms that use technology related to hardware and software to protect the digital environment of personal data and the resources involved in its treatment. By way of example but not limitation, the following activities should be considered:

a) Prevent access to databases or information, as well as resources, from being identified and authorized users;

b) Generate a scheme of privileges for the user to carry out the activities required by reason of their functions;

c) Review the security configuration in the acquisition, operation, development and maintenance of software and hardware, and

d) Manage communications, operations and means of storage of resources IT in the processing of personal data;

XXIV. Guarantor Organizations: Those with constitutional autonomy specialized in matters of access to information and protection of personal data, in terms of articles 6o. and 116, section VIII of the Political Constitution of the United Mexican States;

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

XXVI. National Program for the Protection of Personal Data: National Program for the Protection of Personal Data;

XXVII. Referral: Any communication of personal data made exclusively between the responsible and in charge, inside or outside the Mexican territory;

XXVIII. Responsible: The obligated subjects referred to in article 1 of this Law who decide about the processing of personal data;

XXIX. National System: The National System of Transparency, Access to Information and Protection of Personal Data;

XXX. Suppression: The archival deletion of personal data in accordance with the applicable archival regulations, which results in the elimination, deletion or destruction of personal data under the security measures previously established by the person in charge;

XXXI. Owner: The natural person to whom the personal data corresponds;

XXXII. Transfer: Any communication of personal data inside or outside of Mexican territory, made to a person other than the owner, the person in charge or the person in charge;

XXXIII. Treatment: Any operation or set of operations carried out through manual or automated procedures applied to personal data, related to obtaining, using, registering, organizing, preserving, preparing, using, communicating, disseminating, storing, possessing, accessing, managing, exploiting , disclosure, transfer or disposal of personal data, and

XXXIV. Transparency Unit: Body referred to in article 45 of the General Law of Transparency and Access to Public Information.

Article 4. This Law shall be applicable to any processing of personal data held in physical or electronic media, regardless of the form or modality of its creation, type of media, processing, storage and organization.

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

I Internet pages or remote or local means of electronic, optical and other communication technology, provided that the site where the personal data is found is designed to provide information to the public and is open to general consultation;

II. Telephone directories in terms of specific regulations;

III. Official newspapers, gazettes or bulletins, in accordance with their regulations;

IV. social media, and

v. Public records in accordance with the provisions that are applicable to them.

In order for the assumptions listed in this article to be considered public access sources, it will be necessary that their consultation can be carried out by any person not prevented by a limiting rule, or without further requirement than, where appropriate, the payment of a consideration, duty or fee. A source of public access will not be considered when the information contained therein is or has an illicit origin.

Article 6. The State shall guarantee the privacy of individuals and shall ensure that third parties do not engage in conduct that may arbitrarily affect it.

The right to the protection of personal data will only be limited for reasons of national security, in terms of the law on the matter, provisions of public order, public safety and health or to protect the rights of third parties.

Article 7. As a general rule, sensitive personal data may not be processed, except with the express consent of its owner or, failing that, in the cases established in article 22 of this Law.

In the treatment of personal data of minors, the best interest of the person must be privileged. girl, boy and adolescent, in terms of the applicable legal provisions.

Article 8. The application and interpretation of this Law will be carried out in accordance with the provisions of the Political Constitution of the United Mexican States, the International Treaties to which the Mexican State is a party, as well as the resolutions and binding sentences issued by the bodies specialized national and international, favoring at all times the right to privacy, the protection of personal data and people the broadest protection.

In the case of interpretation, the criteria, determinations and opinions of national and international organizations, in matters of personal data protection.

Article 9. In the absence of an express provision in this Law, the provisions of the Federal Code of Civil Procedures and the Federal Law of Administrative Procedure shall be applied in a supplementary manner.

The laws of the Federal Entities, within the scope of their respective powers, must determine the provisions that are applicable in supplementary matters to the Guarantor Agencies in the application and interpretation of this Law.

Chapter II

From the National System of Transparency, Access to Information and Protection of Personal Data

Article 10. The National System will be formed in accordance with the provisions of the General Law of Transparency and Access to Public Information. Regarding the protection of personal data, said System has the function of coordinating and evaluating the actions related to the transversal public policy of protection of personal data, as well as establishing and implementing criteria and guidelines in the matter, in accordance with what is indicated in this document. Law, the General Law of Transparency and Access to Public Information and other applicable regulations.

Article 11. The National System will contribute to maintaining the full validity of the right to protection of personal data at the national level, in the three orders of government.

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

Article 12. In addition to the objectives set forth in the General Law of Transparency and Access to Public Information, the National System will have the objective of designing, executing and evaluating a National Program for the Protection of Personal Data that defines the public policy and establishes, at least , objectives, strategies, actions and goals for:

I Promote education and a culture of protection of personal data among Mexican society;

II. Promote the exercise of the rights of access, rectification, cancellation and opposition;

III. Train obligated subjects in matters of personal data protection;

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

v. Provide mechanisms that allow measuring, reporting and verifying the established goals.

The National Program for the Protection of Personal Data will be constituted as a guiding instrument for the integration and coordination of the National System, and must determine and prioritize the objectives and goals that it must meet, as well as define the general lines of action that are necessary.

The National Program for the Protection of Personal Data must be evaluated and updated at the end of each year and will define the set of activities and projects that must be executed during the following year.

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

Article 14. The National System, in addition to the provisions of the General Law of Transparency and Access to Public Information and other applicable regulations, will have the following functions in terms of personal data protection:

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

II. Promote a culture of protection of personal data in society;

III. Analyse, give an opinion and propose to the authorities empowered to do so projects to reform or modify the regulations on the matter;

IV. Agree and establish the coordination mechanisms that allow the formulation and execution of comprehensive, systematic, continuous and evaluable public instruments and policies, tending to comply with the objectives and purposes of the National System, of this Law and other provisions that are applicable in the matter;

v. Issue general agreements and resolutions for the operation of the National System;

SAW. Formulate, establish and execute general policies regarding the protection of personal data;

VII. Promote the effective coordination of the instances that make up the National System and follow up on the actions established for this purpose;

VII. Promote the standardization and development of the procedures provided for in this Law and evaluate their progress;

IX. Design and implement policies regarding the protection of personal data;

X. Establish effective mechanisms for society to participate in the evaluation processes of the policies and institutions that make up the National System;

XI. Develop common projects of national scope to measure compliance and progress of those responsible;

XII. Sign collaboration agreements that are intended to contribute to the fulfillment of the objectives of the National System and those provided for in this Law and other provisions that are applicable in the matter;

XIII. Promote and implement actions to guarantee accessibility conditions so that vulnerable groups can exercise, in equal circumstances, their right to personal data protection;

XIV. Propose codes of good practice or models regarding the protection of personal data;

XV. Promote communication and coordination with national, federal, state, municipal authorities, international authorities and organizations, in order to promote and promote the objectives of this Law;

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

XVII. Promote and encourage the exercise and protection of the right to personal data protection, through the implementation, organization and operation of the National Platform, referred to in the General Law of Transparency and Access to Public Information and other applicable regulations;

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

XIX. Issue additional criteria to determine the cases in which there is an intensive or relevant treatment of personal data, in accordance with the provisions of articles 70 and 71 of this Law;

XX. Issue the necessary administrative provisions for the assessment of the content presented by the obligated subjects in the Impact Assessment on the protection of personal data, in order to issue the corresponding non-binding recommendations, and

XXI. The others that are established in other provisions on the matter for the operation of the National System.

Article 15. The National Council will function in accordance with the provisions of the General Transparency Law and Access to Public Information and other applicable regulations.

SECOND TITLE

PRINCIPLES AND DUTIES

Chapter I

Of the Principles

Article 16. The person in charge must observe the principles of legality, purpose, loyalty, consent, quality, proportionality, information and responsibility in the processing of personal data.

Article 17. The processing of personal data by the controller must be subject to the faculties or attributions that the applicable regulations confer on it.

Article 18. Any treatment of personal data carried out by the person in charge must be justified by specific, lawful, explicit and legitimate purposes, related to the powers that the applicable regulations confer on them.

The person in charge may process personal data for purposes other than those established in the privacy notice, as long as it has attributions conferred by law and the consent of the owner, unless it is a person reported as missing, in the terms provided in the this Law and other provisions that are applicable in the matter.

Article 19. The person in charge must not obtain and process personal data, through deceptive means or fraudulent, prioritizing the protection of the owner's interests and the reasonable expectation of privacy.

Article 20. When some of the grounds for exception provided for in article 22 of this Law are not updated, the person in charge must have the prior consent of the owner for the processing of personal data, which must be granted in the following manner:

I Free: Without error, bad faith, violence or fraud that may affect the expression of will of the holder;

II. Specific: Referring to specific, lawful, explicit and legitimate purposes that justify the treatment, and

III. Informed: That the owner is aware of the privacy notice prior to the treatment to which their personal data will be subjected.

In obtaining the consent of minors or persons who are in a state of interdiction or incapacity declared in accordance with the law, the provisions of the rules of representation provided for in the applicable civil legislation will be followed.

Article 21. Consent may be expressed expressly or tacitly. It should be understood that the consent is express when the will of the owner is expressed verbally, in writing, by electronic or optical means, unequivocal signs or by any other technology.

The consent will be tacit when the privacy notice has been made available to the owner, he does not express his will to the contrary.

As a general rule, tacit consent will be valid, unless the law or applicable provisions require that the will of the owner is expressly stated.

In the case of sensitive personal data, the person in charge must obtain the express and written consent of the owner for its treatment, through his autograph signature, electronic signature or any authentication mechanism established for this purpose, except in the cases provided for in article 22 of this Law.

Article 22. The person in charge will not be obliged to obtain the consent of the owner for the treatment of your personal data in the following cases:

I When a law so provides, and said assumptions must be in accordance with the bases, principles and provisions established in this Law, in no case may they contravene it;

II. When the transfers made between controllers are about personal data that are used for the exercise of their own powers, compatible or analogous with the purpose that motivated the processing of personal data;

III. When there is a court order, resolution or well-founded and motivated mandate from a competent authority;

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

v. When the personal data is required to exercise a right or fulfill obligations derived from a legal relationship between the owner and the person in charge;

SAW. When there is an emergency situation that could potentially harm an individual in his person or in his property;

VII. When the personal data is necessary to carry out a treatment for prevention, diagnosis, the provision of health care;

VII. When the personal data appears in publicly accessible sources;

IX. When the personal data is subjected to a prior dissociation procedure, or

X. When the owner of the personal data is a person reported as missing in the terms of the law on the matter.

Article 23. The person in charge must adopt the necessary measures to keep accurate, complete, correct and updated the personal data in their possession, so that their veracity is not altered.

It is presumed that the quality of personal data is met when they are provided. directly by the owner and until the latter states and proves otherwise.

When the personal data is no longer necessary for the fulfillment of the purposes set forth in the privacy notice and that motivated its treatment in accordance with the applicable provisions, it must be deleted, after blocking it, and once the processing is over. term of conservation of the same.

The periods of conservation of personal data must not exceed those that are necessary for the fulfillment of the purposes that justified their treatment, and must comply with the applicable provisions in the matter in question and consider the administrative, accounting, fiscal, legal and historical personal data.

Article 24. The person in charge must establish and document the procedures for the conservation and, where appropriate, blocking and deletion of the personal data that he carries out, in which the periods of conservation of the same are included, in accordance with the provisions in the previous article of this Law.

In the procedures referred to in the previous paragraph, the person in charge must include mechanisms that allow them to comply with the deadlines set for the deletion of personal data, as well as to carry out a periodic review of the need to retain personal data.

Article 25. The controller must only process the personal data that is adequate, relevant and strictly necessary for the purpose that justifies its treatment.

Article 26. The person in charge must inform the owner, through the privacy notice, of the existence and main characteristics of the treatment to which their personal data will be subjected, so that they can make informed decisions in this regard.

As a general rule, the privacy notice must be disseminated by the electronic and physical means with which tell the person in charge.

In order for the privacy notice to efficiently fulfill its informative function, it must be written and structured in a clear and simple way.

When it is impossible to make the privacy notice known to the owner, directly or this requires disproportionate efforts, the person in charge may implement compensatory mass communication measures in accordance with the criteria issued for this purpose by the National System of Transparency, Access to Public Information and Protection of Personal Data.

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

I The name of the person in charge;

II. The purposes of the treatment for which the personal data is obtained, distinguishing those that require the consent of the owner;

III. When transfers of personal data that require consent are made, the following must be reported:

a) The authorities, powers, entities, organs and government agencies of the three orders of government and the natural or legal persons to whom the personal data is transferred, and

b) The purposes of these transfers;

IV. The mechanisms and means available so that the holder, where appropriate, can express his refusal to process his personal data for purposes and transfers of personal data that require the consent of the holder, and

v. The site where you can consult the comprehensive privacy notice.

The provision of the privacy notice referred to in this article does not exempt the person responsible from its obligation to provide the mechanisms so that the owner can know 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 available so that the owner can express their refusal to process their personal data for the purposes or transfers that require the consent of the owner, prior to such occurrence. treatment.

Article 28. The comprehensive privacy notice, in addition to the provisions of the fractions of the previous article, referred to in section V of the previous article must contain, at least, the following information:

I The domicile of the person in charge;

II. The personal data that will be subjected to treatment, identifying those that are sensitive;

III. The legal basis that empowers the person in charge to carry out the treatment;

IV. The purposes of the treatment for which the personal data is obtained, distinguishing those that require the consent of the owner;

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

SAW. The address of the Transparency Unit, and

VII. The means by which the person in charge will notify the owners of the changes to the privacy notice.

Article 29. The person in charge must implement the mechanisms provided for in article 30 of this Law to prove compliance with the principles, duties and obligations established in this Law and render accounts on the processing of personal data in their possession to the owner and Institute or to the Guarantor Agencies, as appropriate, in which case the Constitution and International Treaties to which the Mexican State is a party must be observed; in what does not conflict with Mexican regulations, it may use national or international standards or best practices for such purposes.

Article 30. Among the mechanisms that the controller must adopt to comply with the principle of responsibility established in this Law are, at least, the following:

I Allocate authorized resources for this purpose for the implementation of programs and policies for the protection of personal data;

II. Develop policies and programs for the protection of personal data, mandatory and enforceable within the organization of the person in charge;

III. Implement a training and updating program for personnel on the obligations and other duties regarding the protection of personal data;

IV. Periodically review the personal data security policies and programs to determine the modifications that are required;

v. Establish an internal and/or external supervision and surveillance system, including audits, to verify compliance with personal data protection policies;

SAW. Establish procedures to receive and respond to doubts and complaints from the holders;

VII. Design, develop and implement its public policies, programs, services, computer systems or platforms, electronic applications or any other technology that involves the processing of personal data, in accordance with the provisions set forth herein
Law and the others that are applicable in the matter, and

VII. Guarantee that its public policies, programs, services, computer systems or platforms, electronic applications or any other technology that involves the processing of personal data, comply by default with the obligations set forth in this Law and the others that are applicable in the matter.

Chapter II

of homework

Article 31. Regardless of the type of system in which the personal data is found or the type of treatment that is carried out, the person in charge must establish and maintain the security measures of an administrative, physical and technical nature for the protection of personal data. , that allow them to be protected against damage, loss, alteration, destruction or their unauthorized use, access or treatment, as well as guarantee their confidentiality, integrity and availability.

Article 32. The security measures adopted by the person in charge must consider:

I The risk inherent in the personal data processed;

II. The sensitivity of the personal data processed;

III. Technological development;

IV. The possible consequences of a violation for the holders;

v. The transfers of personal data that are made;

SAW. The number of holders;

VII. The previous violations that occurred in the treatment systems, and

VII. The risk due to the potential quantitative or qualitative value that the personal data processed could have for a third party not authorized to possess it.

Article 33. To establish and maintain security measures for data protection personal, the person in charge must carry out, at least, the following interrelated activities:

I Create internal policies for the management and processing of personal data, which take into account the context in which the processing occurs and the life cycle of personal data, that is, its collection, use and subsequent deletion;

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

III. Prepare an inventory of personal data and treatment systems;

IV. Carry out a risk analysis of personal data, considering the existing threats and vulnerabilities for personal data and the resources involved in its treatment, such as, but not limited to, hardware, software, personnel of the person in charge, among others;

v. Carry out a gap analysis, comparing the existing security measures against those missing in the organization of the person in charge;

SAW. Prepare a work plan for the implementation of the missing security measures, as well as the measures for daily compliance with the personal data management and processing policies;

VII. Periodically monitor and review the security measures implemented, as well as the threats and violations to which personal data is subject, and

VII. Design and apply different levels of training for the personnel under your command, depending on their roles and responsibilities regarding the processing of personal data.

Article 34. Actions related to security measures for data processing personal data must be documented and contained in a management system.

Management system shall be understood as the set of interrelated elements and activities to establish, implement, operate, monitor, review, maintain and improve the treatment and security of personal data, in accordance with the provisions of this Law and the other provisions that are applicable to the matter.

Article 35. In particular, the person in charge must prepare a security document that contain at least the following:

I The inventory of personal data and treatment systems;

II. The functions and obligations of the people who process personal data;

III. Risk analysis;

IV. The gap analysis;

v. The work plan;

SAW. The mechanisms for monitoring and reviewing security measures, and

VII. The general training program.

Article 36. The person in charge must update the security document when the following events occur:

I Substantial modifications occur to the processing of personal data that result in a change in the level of risk;

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

III. As a result of an improvement process to mitigate the impact of a security breach that occurred, and

IV. Implementation of corrective and preventive actions in the event of a security breach.

Article 37. In the event of a security breach, the person in charge must analyze the causes for which it occurred and implement preventive and corrective actions in its work plan to adapt the security measures and the processing of personal data. if it were the case in order to prevent the violation from being repeated.

Article 38. In addition to those indicated by the respective laws and the applicable regulations, they will be considered as security breaches, at any stage of data processing, at least the following:

I Loss or unauthorized destruction;

II. Theft, loss or unauthorized copying;

III. The unauthorized use, access or treatment, or

IV. Damage, alteration or unauthorized modification.

Article 39. The person in charge must keep a log of the security violations in which it is described, the date on which it occurred, the reason for it and the corrective actions implemented immediately and definitively.

Article 40. The person responsible must inform the owner, and as appropriate, the Institute and the Guarantor Agencies of the Federal Entities, without delay, of the violations that significantly affect the patrimonial or moral rights, as soon as it is confirmed that the violation occurred and that the person in charge has begun to take the actions aimed at triggering a process of exhaustive review of the magnitude of the affectation, so that the affected owners can take the corresponding measures to defend their rights.

Article 41. The person in charge must inform the owner of at least the following:

I The nature of the incident;

II. Compromised personal data;

III. The recommendations to the holder about the measures that he can adopt to protect his interests;

IV. Corrective actions taken immediately, and

v. The means where you can get more information about it.

Article 42. The person in charge must establish controls or mechanisms whose purpose is that all those persons who intervene in any phase of the processing of personal data, keep confidentiality with respect to them, an obligation that will subsist even after the end of their relations with it.

The foregoing, without prejudice to the provisions of the provisions of access to public information.

THIRD TITLE

RIGHTS OF THE HOLDERS AND THEIR EXERCISE

Chapter I

Of the Rights of Access, Rectification,

Cancellation and Opposition

Article 43. At all times, the owner or his representative may request access, rectification, cancellation or opposition to the processing of personal data that concerns him, in accordance with the provisions of this Title. The exercise of any of the ARCO rights is not a prerequisite, nor does it prevent the exercise of another.

Article 44. The owner shall have the right to access their personal data that is in the possession of the person in charge, as well as to know the information related to the conditions and generalities of their treatment.

Article 45. The owner shall have the right to request the person in charge to rectify or correct their data when they turn out to be inaccurate, incomplete or out of date.

Article 46. The owner shall have the right to request the cancellation of their personal data from the files, records, records and systems of the person in charge, so that they are no longer in their possession and stop being processed by the latter.

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

I Even if the treatment is lawful, it must cease to prevent its persistence from causing damage or harm to the owner, and

II. Your personal data is subject to automated processing, which produces unwanted legal effects or significantly affects your interests, rights or freedoms, and is intended to evaluate, without human intervention, certain personal aspects thereof or analyze or predict, in particular, your professional performance, economic situation, state of health, sexual preferences, reliability or behavior.

Chapter II

Of the Exercise of the Rights of Access, Rectification,

Cancellation and Opposition

Article 48. The reception and processing of requests for the exercise of ARCO rights that are formulated to those responsible, will be subject to the procedure established in this Title and other provisions that are applicable in the matter.

Article 49. In order to exercise the ARCO rights, it will be necessary to prove the identity of the holder and, in your case, the identity and personality with which the representative acts.

The exercise of ARCO rights by a person other than its owner or its representative, will be possible, exceptionally, in those cases provided for by legal provision, or where appropriate, by court order.

In the exercise of the ARCO rights of minors or persons who are in a state of interdiction or disability, in accordance with civil laws, the rules of representation provided in the same legislation will be followed.

In the case of personal data concerning deceased persons, the person who proves to have a legal interest, in accordance with the applicable laws, may exercise the rights conferred by this Chapter, provided that the owner of the rights has reliably expressed his will in such meaning or that there is a court order to that effect.

Article 50. The exercise of ARCO rights must be free. Charges can only be made for recover the costs of reproduction, certification or shipping, in accordance with the applicable regulations.

For purposes of access to personal data, the laws that establish the costs of reproduction and certification must consider in their determination that the amounts allow or facilitate the exercise of this right.

When the holder provides the magnetic or electronic means or the necessary mechanism to reproduce personal data, they must be delivered at no cost to it.

The information must be delivered free of charge, when it involves the delivery of no more than twenty simple sheets. Transparency units may exempt payment for reproduction and shipping based on the socioeconomic circumstances of the owner.

The person in charge may not establish for the presentation of requests for the exercise of ARCO rights any service or means that implies a cost to the owner.

Article 51. The person in charge must establish simple procedures that allow the exercise of ARCO rights, whose response period must not exceed twenty days from the day following receipt of the request.

The term referred to in the preceding paragraph may be extended once for up to ten days when the circumstances justify it, and as long as the owner is notified within the response period.

If the exercise of the ARCO rights is appropriate, the person in charge must make it effective within a period that may not exceed fifteen days from the day after the response was notified to the owner.

Article 52. In the application for the exercise of the ARCO rights, greater requirements than the following:

I The name of the holder and his address or any other means to receive notifications;

II. The documents that prove the identity of the holder and, where appropriate, the personality and identity of his representative;

III. If possible, the responsible area that processes the personal data and to which the request is submitted;

IV. The clear and precise description of the personal data with respect to which one seeks to exercise any of the ARCO rights, except in the case of the right of access;

v. The description of the ARCO right that is intended to be exercised, or what the owner requests, and

saw. Any other element or document that facilitates the location of personal data, in its case.

In the case of a request for access to personal data, the owner must indicate the modality in which he prefers that they be reproduced. The person in charge must attend to the request in the modality required by the owner, unless there is a physical or legal impossibility that limits it to reproduce the personal data in said modality, in this case it must offer other modalities of delivery of the personal data founding and motivating said performance.

In the event that the data protection request does not meet any of the requirements referred to in this article, and the Institute or the guarantor agencies do not have elements to correct it, the owner of the data will be notified within the following five days to the presentation of the request to exercise the ARCO rights, for a single occasion, to correct the omissions within a period of ten days from the day following the notification.

Once the term has elapsed without discharging the prevention, the request to exercise the right will be deemed not submitted. ARCO rights.

The prevention will have the effect of interrupting the term that the Institute has, or in its case, the organisms guarantors, to resolve the request to exercise the ARCO rights.

In relation to a request for cancellation, the holder must indicate the causes that motivate him to request the deletion of your personal data in the files, records or databases of the person in charge.

In the case of the opposition request, the owner must state the legitimate causes or the specific situation that lead him to request the cessation of the treatment, as well as the damage or harm that the persistence of the treatment would cause, or in his case, the specific purposes for which it is required to exercise the right of opposition.

Requests for the exercise of ARCO rights must be submitted to the Transparency Unit of the person in charge, which the holder considers competent, through free writing, formats, electronic means or any other means established for this purpose by the Institute and the Guarantor Agencies, within the scope of their respective powers.

The person in charge must process any request for the exercise of ARCO rights and deliver the corresponding acknowledgment of receipt.

The Institute and the Guarantor Agencies, as appropriate, may establish forms, systems and other simplified methods to make it easier for holders to exercise ARCO rights.

The means and procedures enabled by the person in charge to attend to requests for the exercise of ARCO rights must be easily accessible and with the greatest possible coverage considering the profile of the owners and the way in which they maintain daily or common contact with the person in charge.

Article 53. When the person in charge is not competent to attend to the request for the exercise of ARCO rights, he must inform the owner of said situation within the three days following the presentation of the request, and in case of being able to determine it, guide him to the responsible person.

In the event that the person in charge declares the non-existence of the personal data in their files, records, systems or file, said declaration must be included in a resolution of the Transparency Committee that confirms the non-existence of the personal data.

In the event that the person in charge notices that the application for the exercise of the ARCO rights corresponds to a different right from those provided for in this Law, he must redirect the route by doing so.
of knowledge to the holder.

Article 54. When the provisions applicable to certain processing of personal data establish a specific process or procedure to request the exercise of ARCO rights, the person in charge must inform the owner of the existence thereof, within a period not exceeding five days following the presentation of the application for the exercise of the ARCO rights, so that the latter decides whether to exercise their rights through the specific procedure, or through the procedure that the person in charge has institutionalized for the attention of requests for the exercise of the ARCO rights in accordance with the provisions established in this Chapter.

Article 55. The only causes in which the exercise of ARCO rights will not be appropriate are:

I When the holder or his representative are not duly accredited for it;

II. When the personal data is not in the possession of the person in charge;

III. When there is a legal impediment;

IV. When the rights of a third party are injured;

v. When judicial or administrative actions are hindered;

SAW. When there is a resolution of the competent authority that restricts access to personal data or does not allow their rectification, cancellation or opposition;

VII. When the cancellation or opposition has been previously made;

VII. When the person in charge is not competent;

IX. When they are necessary to protect legally protected interests of the owner;

X. When they are necessary to comply with obligations legally acquired by the owner;

XI. When, based on its legal powers, the daily use, protection and management are necessary and proportional to maintain the integrity, stability and permanence of the Mexican State, or

XII. When the personal data is part of the information that the entities subject to the financial regulation and supervision of the regulated entity have provided to it, in compliance with the requirements of said information on its operations, organization and activities.

In all the above cases, the person in charge must inform the owner of the reason for its determination, within a period of up to twenty days referred to in the first paragraph of article 51 of this Law and other applicable provisions, and by the same means. in which the request was made, attaching, where appropriate, the pertinent evidence.

Article 56. Against the refusal to process any application for the exercise of ARCO rights or due to lack of response from the person in charge, the appeal for review referred to in article 94 of this Law will proceed.

Chapter III

Data Portability

Article 57. When personal data is processed electronically in a structured and commonly used format, the owner shall have the right to obtain from the controller a copy of the data being processed in a structured and commonly used electronic format that allows them to continue using them.

When the holder has provided the personal data and the treatment is based on consent or a contract, he will have the right to transmit said personal data and any other information that he has provided and that is kept in an automated treatment system to another system in a commonly used electronic format, without hindrance by the data controller from whom the personal data is withdrawn.

The National System will establish through guidelines the parameters to be considered to determine the assumptions in which it is in the presence of a structured and commonly used format, as well as the technical standards, modalities and procedures for the transfer of personal data.

FOURTH TITLE

RELATIONSHIP OF THE RESPONSIBLE AND MANAGER

Single Chapter

Responsible and in charge

Article 58. The person in charge must carry out the personal data processing activities without holding any power of decision over the scope and content of the same, as well as limit their actions to the terms set by the person in charge.

Article 59. The relationship between the person in charge and the person in charge must be formalized by means of a contract or any other legal instrument decided by the person in charge, in accordance with the regulations that are applicable, and that allows proving its existence, scope and content.

In the contract or legal instrument decided by the person in charge, at least the following general clauses related to the services provided by the person in charge:

I Carry out the processing of personal data in accordance with the instructions of the person in charge;

II. Refrain from processing personal data for purposes other than those instructed by the person in charge;

III. Implement the security measures in accordance with the applicable legal instruments;

IV. Inform the person in charge when there is a violation of the personal data that it processes by its instructions;

v. Maintain confidentiality regarding the personal data processed;

SAW. Delete or return the personal data subject to treatment once the legal relationship with the person in charge has been fulfilled, as long as there is no legal provision that requires the conservation of personal data, and

VII. Refrain from transferring personal data except in the event that the person in charge so determines, or the communication derives from a subcontracting, or by express mandate of the competent authority.

The agreements between the person in charge and the person in charge related to the processing of personal data must not contravene this Law and other applicable provisions, as well as what is established in the corresponding privacy notice.

Article 60. When the person in charge fails to comply with the instructions of the person in charge and decides for himself on the processing of personal data, he will assume the character of person in charge in accordance with the legislation on the matter that is applicable to him.

Article 61. The person in charge may, in turn, subcontract services that involve the processing of personal data on behalf of the person in charge, as long as there is the express authorization of the latter. The subcontracted party will assume the character of manager in the terms of this Law and other provisions that are applicable in the matter.

When the contract or the legal instrument through which the relationship between the person in charge and the person in charge has been formalized, foresees that the latter can in turn carry out the subcontracting of services, the authorization referred to in the previous paragraph will be understood as granted through the provisions of these.

Article 62. Once the express authorization of the person in charge has been obtained, the person in charge must formalize the relationship acquired with the subcontractor through a contract or any other legal instrument that he decides, in accordance with the regulations that are applicable to him, and allow to prove the existence , scope and content of the provision of the service in terms of the provisions of this Chapter.

Article 63. The person in charge may contract or adhere to services, applications and infrastructure in cloud computing, and other matters that imply the processing of personal data, as long as the external provider guarantees personal data protection policies equivalent to the principles and duties established in this Law and other provisions that are applicable in the matter.

Where appropriate, the controller must limit the processing of personal data by the provider external through contractual clauses or other legal instruments.

Article 64. For the processing of personal data in services, applications and computing infrastructure in the cloud and other matters, in which the person in charge adheres to them by means of general contract conditions or clauses, you can only use those services in which the supplier:

I Comply with at least the following:

a) Have and apply personal data protection policies related to the principles and duties provisions established by this Law and other applicable regulations;

b) Make transparent the subcontracting that involves the information on which the service is provided. service;

c) Refrain from including conditions in the provision of the service that authorize or allow it to assume the ownership or ownership of the information on which the service is provided, and

d) Maintain confidentiality regarding the personal data on which the service is provided;

II. Have mechanisms, at least, to:

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

b) Allow the person in charge to limit the type of treatment of the personal data on which it is provides the service;

c) Establish and maintain security measures for the protection of personal data on which the service is provided;

d) Guarantee the deletion of personal data once the service provided to the person in charge has concluded and that the latter has been able to recover them, and

e) Prevent access to personal data to people who do not have access privileges, or, if it is at the well-founded and motivated request of the competent authority, inform the person in charge of that fact.

In any case, the person in charge may not adhere to services that do not guarantee the due protection of personal data, in accordance with this Law and other provisions that are applicable in the matter.

FIFTH TITLE

PERSONAL DATA COMMUNICATIONS

Single Chapter

Of the Transfers and Remissions of Personal information

Article 65. Any transfer of personal data, whether national or international, is subject to the consent of its owner, except for the exceptions provided for in articles 22, 66 and 70 of this Law.

Article 66. Any transfer must be formalized through the signing of contractual clauses, collaboration agreements or any other legal instrument, in accordance with the regulations that are applicable to the person in charge, which allows demonstrating the scope of the processing of personal data, as well as the obligations and responsibilities assumed by the parties.

The provisions of the preceding paragraph shall not apply in the following cases:

I When the transfer is national and is made between controllers by virtue of compliance with a legal provision or in the exercise of powers expressly conferred on them, or

II. When the transfer is international and is provided for in a law or treaty signed and ratified by Mexico, or is carried out at the request of a foreign authority or competent international organization in its capacity as recipient, as long as the powers between the person transferring and receiver are homologous, or else, the purposes that motivate the transfer are analogous or compatible with respect to those that gave rise to the treatment of the transferor.

Article 67. When the transfer is national, the recipient of the personal data must treat the personal data, committing to guarantee its confidentiality and will only use them for the purposes that were transferred in accordance with what is agreed in the privacy notice that will be communicated to you by transferring manager.

Article 68. The person in charge may only transfer or forward personal data outside the national territory when the receiving third party or the person in charge undertakes to protect the personal data in accordance with the principles and duties established by this Law and the provisions that are applicable in The matter.

Article 69. In any transfer of personal data, the controller must notify the recipient of personal data the privacy notice according to which personal data is processed against the owner.

Article 70. The person in charge may carry out transfers of personal data without the need to require the consent of the owner, in the following cases:

I When the transfer is provided for in this Law or other laws, agreements or Treaties International signed and ratified by Mexico;

II. When the transfer is made between controllers, as long as the personal data is used for the exercise of own powers, compatible or analogous with the purpose that motivated the processing of personal data;

III. When the transfer is legally required for the investigation and prosecution of crimes, as well as the procurement or administration of justice;

IV. When the transfer is necessary for the recognition, exercise or defense of a right before a competent authority, as long as there is a request from the latter;

v. When the transfer is necessary for the prevention or medical diagnosis, the provision of health care, medical treatment or the management of health services, as long as said purposes are accredited;

SAW. When the transfer is necessary for the maintenance or fulfillment of a legal relationship between the person in charge and the owner;

VII. When the transfer is necessary by virtue of a contract concluded or to be concluded in the interest of the owner, by the person in charge and a third party;

VII. In the case of cases in which the person in charge is not obliged to obtain the consent of the owner for the treatment and transmission of their personal data, in accordance with the provisions of article 22 of this Law, or

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

The updating of some of the exceptions provided for in this article does not exempt the person responsible for comply with the obligations set forth in this Chapter that are applicable.

Article 71. The national and international transfers of personal data that are made between responsible and in charge will not require to be informed to the owner, nor to have their consent.

SIXTH TITLE

PREVENTIVE ACTIONS REGARDING

PERSONAL DATA PROTECTION

Chapter I

Best Practices

Article 72. In order to comply with the obligations set forth in this Law, the person in charge may develop or adopt, individually or in agreement with other managers, managers or organizations, schemes of best practices whose purpose is:

I Raise the level of protection of personal data;

II. Harmonize the processing of personal data in a specific sector;

III. Facilitate the exercise of ARCO rights by the owners;

IV. Facilitate transfers of personal data;

v. Complement the provisions set forth in the applicable regulations regarding the protection of personal data, and

SAW. Demonstrate to the Institute or, as the case may be, the Guarantor Bodies, compliance with the applicable regulations regarding the protection of personal data.

Article 73. Any scheme of best practices that seeks validation or recognition by the Institute or, as the case may be, by the Guarantor Agencies must:

I Comply with the parameters issued for this purpose, as appropriate, by the Institute and the Guarantor agencies according to the criteria established by the first, and

II. Be notified before the Institute or, where appropriate, the Guarantor Agencies in accordance with the procedure established in the parameters indicated in the previous section, so that they are evaluated and, where appropriate, validated or recognized and registered in the registry at referred to in the last paragraph of this article.

The Institute and the Guarantor Agencies, as appropriate, must issue the rules of operation of the registries in which the validated or recognized best practice schemes will be registered. The Guarantor Agencies may register the schemes of best practices that they have recognized or validated in the registry administered by the Institute, in accordance with the rules established by the latter.

Article 74. When the person in charge intends to put into operation or modify public policies, computer systems or platforms, electronic applications or any other technology that in his opinion and in accordance with this Law imply the intensive or relevant treatment of personal data, he must carry out an Evaluation of impact on the protection of personal data, and submit it to the Institute or Guarantor Agencies, as appropriate, which may issue non-binding recommendations specialized in the matter of personal data protection.

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

Article 75. For the purposes of this Law, it will be considered that there is an intensive or relevant treatment of personal data when:

I There are risks inherent to the personal data to be processed;

II. Sensitive personal data is processed, and

III. Transfers of personal data are made or intended to be made.

Article 76. The National System may issue additional criteria based on objective parameters that determine that there is an intensive or relevant treatment of personal data, in accordance with the provisions of the previous article, based on:

I The number of holders;

II. The target audience;

III. The development of the technology used, and

IV. The relevance of the processing of personal data in attention to the social or economic impact thereof, or the public interest pursued.

Article 77. The regulated entities that carry out an Impact Assessment on the protection of personal data must submit it to the Institute or Guarantor Agencies, as appropriate, thirty days prior to the date on which it is intended to put into operation or modify public policies, computer systems or platforms, electronic applications or any other technology, before the Institute or the guarantor agencies, as appropriate, in order for them to issue the corresponding non-binding recommendations.

Article 78. The Institute and the Guarantor Agencies, as appropriate, must issue, if applicable, non-binding recommendations on the Personal Data Protection Impact Assessment submitted by the person responsible.

The deadline for issuing the recommendations referred to in the preceding paragraph will be within the thirty days following the day following the presentation of the evaluation.

Article 79. When, in the opinion of the regulated entity, the effects that are intended to be achieved with the possible implementation or modification of public policies, computer systems or platforms, electronic applications or any other technology that implies intensive or relevant data processing may be compromised. or in the case of emergency or urgent situations, it will not be necessary to carry out the Impact Assessment on the protection of personal data.

Chapter II

Of the Databases in Possession of Security Instances, Procurement and Administration of Justice

Article 80. The collection and processing of personal data, in terms of the provisions of this Law, by the competent reporting entities in instances of security, procurement and administration of justice, is limited to those assumptions and categories of data that are necessary. and proportional for the exercise of functions in matters of national security, public security, or for the prevention or prosecution of crimes. They must be stored in the databases established for this purpose.

The authorities that access and store the personal data collected by individuals in compliance with the corresponding legal provisions, must comply with the provisions indicated in this Chapter.

Article 81. In the processing of personal data, as well as in the use of databases for their storage, carried out by the competent obligated subjects of the security, procurement and administration of justice instances, they must comply with the principles established in the Second Title. of this Law.

Private communications are inviolable. Exclusively the federal judicial authority, at the request of the federal authority empowered by law or the head of the Public Ministry of the corresponding federal entity, may authorize the interception of any private communication.

Article 82. Those responsible for the databases referred to in this Chapter must establish high-level security measures to guarantee the integrity, availability and confidentiality of the information, which allow personal data to be protected against damage, loss, alteration , destruction or unauthorized use, access or treatment.

SEVENTH TITLE

RESPONSIBLE FOR THE PROTECTION OF PERSONAL DATA IN POSSESSION OF THE OBLIGATED SUBJECTS

Chapter I

Transparency Committee

Article 83. Each person in charge will have a Transparency Committee, which will be integrated and will function in accordance with the provisions of the General Law of Transparency and Access to Public Information and other applicable regulations.

The Transparency Committee will be the highest authority in matters of personal data protection.

Article 84. For the purposes of this Law and without prejudice to other powers conferred on it in the applicable regulations, the Transparency Committee will have the following functions:

I Coordinate, supervise and carry out the necessary actions to guarantee the right to the protection of personal data in the organization of the person in charge, in accordance with the provisions set forth in this Law and in those provisions that are applicable in the matter;

II. Institute, where appropriate, internal procedures to ensure greater efficiency in the management of requests for the exercise of ARCO rights;

III. Confirm, modify or revoke the determinations in which the non-existence of personal data is declared, or the exercise of any of the ARCO rights is denied for any reason;

IV. Establish and supervise the application of specific criteria that are necessary for a better observance of this Law and in those provisions that are applicable in the matter;

v. Supervise, in coordination with the competent administrative areas or units, compliance with the measures, controls and actions provided for in the security document;

SAW. Monitor and comply with the resolutions issued by the Institute and the guarantor agencies, as appropriate;

VII. Establish training and updating programs for public servants on the protection of personal data, and

VII. Inform the internal control body or equivalent instance in those cases in which it becomes aware, in the exercise of its powers, of a presumed irregularity regarding certain processing of personal data; particularly in cases related to the declaration of non-existence made by those responsible.

Chapter II

From the Transparency Unit

Article 85. Each person in charge will have a Transparency Unit, which will be integrated and will function in accordance with the provisions of the General Law of Transparency and Access to Public Information, this Law and other applicable regulations, which will have the following functions:

I Assist and guide the owner who requires it in relation to the exercise of the right to personal data protection;

II. Manage requests for the exercise of ARCO rights;

III. Establish mechanisms to ensure that personal data is only delivered to its owner or duly accredited representative;

IV. Inform the owner or his representative of the amount of the costs to be covered for the reproduction and sending of personal data, based on the provisions of the applicable regulatory provisions;

v. Propose to the Transparency Committee the internal procedures that ensure and strengthen greater efficiency in the management of requests for the exercise of ARCO rights;

SAW. Apply quality evaluation instruments on the management of requests for the exercise of ARCO rights, and

VII. Advise the areas assigned to the person in charge in matters of personal data protection.

Those responsible who, in the exercise of their substantive functions, carry out relevant or intensive personal data processing, may appoint a personal data protection officer, specialized in the matter, who will carry out the powers mentioned in this article and will be part of the Transparency Unit.

The regulated entities will promote agreements with specialized public institutions that could help them receive, process and deliver responses to requests for information, in the indigenous language, braille or any corresponding accessible format, in a more efficient manner.

Article 86. The person in charge will ensure that people with some type of disability or groups vulnerable, can exercise, in equal circumstances, their right to the protection of personal data.

Article 87. In the appointment of the head of the Transparency Unit, the person in charge will be in accordance with the provisions of the General Law of Transparency and Access to Public Information and other applicable regulations.

EIGHTH TITLE

GUARANTEE AGENCIES

Chapter I

From the National Institute of Transparency, Access to Information and Protection of Personal Data

Article 88. In the integration, appointment procedure and operation of the Institute and the Consultative Council, the provisions of the General Law of Transparency and Access to Public Information, the Federal Law of Transparency and Access to Public Information and other regulations will be followed. applicable.

Article 89. In addition to the powers conferred on it by the General Law on Transparency and Access to Public Information, the Federal Law on Transparency and Access to Public Information and other applicable regulations, the Institute will have the following powers:

I Guarantee the exercise of the right to the protection of personal data held by obligated subjects;

II. Interpret this Law in the administrative field;

III. Know and resolve the review resources filed by the holders, in terms of the provisions of this Law and other provisions that are applicable in the matter;

IV. Hear and resolve, ex officio or upon request founded by the guarantor agencies, the review resources that, due to their interest and importance, so warrant, in terms of the provisions of this Law and other provisions that are applicable in the matter;

v. Know and resolve the appeals of disagreement filed by the holders, against the resolutions issued by the guarantor agencies, in accordance with the provisions of this Law and other provisions that are applicable in the matter;

SAW. Know, substantiate and resolve the verification procedures;

VII. Establish and execute the enforcement measures provided for in terms of the provisions of this Law and other provisions that are applicable in the matter;

VII. Report to the competent authorities the alleged violations of this Law and, where appropriate, provide the evidence available;

IX. Coordinate with the competent authorities so that the requests for the exercise of ARCO rights and the appeals for review that are presented in the indigenous language, are attended to in the same language;

X. Guarantee, within the scope of their respective competence, accessibility conditions so that holders belonging to vulnerable groups can exercise, in equal circumstances, their right to personal data protection;

XI. Prepare and publish studies and research to disseminate and expand knowledge on the subject of this Law;

XII. Provide technical support to those responsible for compliance with the obligations established in this Law;

XIII. Disseminate and issue recommendations, standards and best practices in the matters regulated by this Law;

XIV. Monitor and verify compliance with the provisions contained in this Law;

XV. Manage the registry of best practices schemes referred to in this Law and issue its operating rules;

XVI. Issue, where appropriate, the non-binding recommendations corresponding to the Impact Assessment on the protection of personal data that are presented to it;

XVII. Issue general provisions for the development of the verification procedure;

XVIII. Carry out the evaluations corresponding to the schemes of best practices that are notified to them, in order to decide on the origin of their recognition or validation and registration in the registry of schemes of best practices, as well as promote their adoption;

XIX. Issue, within the scope of its competence, the general administrative provisions for due compliance with the principles, duties and obligations established by this Law, as well as for the exercise of the rights of the owners;

XX. Enter into agreements with those responsible to develop programs that aim to standardize personal data processing in specific sectors, increase the protection of personal data and make any improvements to practices in the matter;

XXI. Define and develop the certification system in terms of personal data protection, in accordance with what is established in the parameters referred to in this Law;

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

XXIII. Enter into agreements with the guarantor agencies that contribute to the fulfillment of the objectives set forth in this Law and other provisions that are applicable in the matter;

XXIV. Carry out actions and activities that promote awareness of the right to protection personal data, as well as their prerogatives;

XXV. Design and apply indicators and criteria to evaluate the performance of those responsible with respect to compliance with this Law and other provisions that are applicable in the matter;

XXVI. Promote training and updating on the protection of personal data among the responsible;

XXVII. Issue general guidelines for the proper treatment of personal data;

XXVIII. Issue guidelines to standardize the exercise of ARCO rights;

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

XXX. Cooperate with other supervisory authorities and national and international organizations, in order to assist in matters of personal data protection, in accordance with the provisions set forth in this Law and other applicable regulations;

XXXI. Promote and promote the exercise and protection of the right to personal data protection through the implementation and administration of the National Platform, referred to in the General Law of Transparency and Access to Public Information and other applicable regulations;

XXXII. File, when approved by the majority of its Commissioners, actions of unconstitutionality against federal or state laws, as well as International Treaties signed by the Federal Executive and approved by the Senate of the Republic, that violate the right to the protection of personal data;

XXXIII. Promote, when approved by the majority of its Commissioners, constitutional controversies in terms of article 105, section I, subsection l), of the Political Constitution of the United Mexican States;

XXXIV. Cooperate with other national or international authorities to combat behaviors related to the improper processing of personal data;

XXXV. Design, monitor and, where appropriate, operate the system of good practices regarding the protection of personal data, as well as the certification system on the matter, through regulations issued by the Institute for such purposes;

XXXVI. Enter into agreements with the guarantor and responsible agencies that contribute to the fulfillment of the objectives set forth in this Law and other provisions that are applicable in the matter, and

XXXVII. The others conferred by this Law and other applicable regulations.

Chapter II

Guarantor Agencies

Article 90. In the integration, appointment procedure and operation of the guarantor agencies, the provisions of the General Law of Transparency and Access to Public Information and other applicable regulations will be followed.

Article 91. For the purposes of this Law and without prejudice to other powers conferred on them in the applicable regulations, the guarantor agencies shall have the following powers:

I Hear, substantiate and resolve, within the scope of their respective powers, the review resources filed by the owners, in terms of the provisions of this Law and other provisions that are applicable in the matter;

II. Submit a well-founded petition to the Institute, so that it may hear the appeals for review that, due to their interest and importance, warrant it, in terms of the provisions of this Law and other provisions that are applicable to the matter;

III. Impose enforcement measures to ensure compliance with its resolutions;

IV. Promote and disseminate the exercise of the right to personal data protection;

v. Coordinate with the competent authorities so that the requests for the exercise of ARCO rights and the appeals for review that are presented in indigenous languages, are attended to in the same language;

SAW. Guarantee, within the scope of their respective powers, accessibility conditions so that holders who belong to vulnerable groups can exercise, in equal circumstances, their right to personal data protection;

VII. Prepare and publish studies and research to disseminate and expand knowledge on the subject of this Law;

VII. Make the knowledge of the competent authorities, the probable responsibility derived from the breach of the obligations foreseen in this Law and in the other provisions that are applicable;

IX. Provide the Institute with the elements it requires to resolve the appeals of disagreement that are presented to it, in terms of the provisions of Title Ninth, Chapter II of this Law and other provisions that are applicable in the matter;

X. Sign collaboration agreements with the Institute for the fulfillment of the objectives set forth in this Law and other applicable provisions;

XI. Monitor, within the scope of their respective powers, compliance with this Law and other provisions that are applicable in the matter;

XII. Carry out actions and activities that promote knowledge of the right to personal data protection, as well as its prerogatives;

XIII. Apply indicators and criteria to evaluate the performance of those responsible regarding compliance with this Law and other applicable provisions;

XIV. Promote training and updating on the protection of personal data among those responsible;

XV. Request the cooperation of the Institute in the terms of article 89, section XXX of this Law;

XVI. Manage, within the scope of its powers, the National Transparency Platform;

XVII. As appropriate, file actions of unconstitutionality against laws issued by the legislatures of the Federal Entities, which violate the right to protection of personal data, and

XVIII. Issue, where appropriate, the non-binding recommendations corresponding to the Impact Assessment on personal data protection that are presented to it.

Chapter III

Of the Coordination and Promotion of the Right to the Protection of Personal Data

Article 92. Those responsible must collaborate with the Institute and the guarantor agencies, as appropriate, to permanently train and update all its public servants in matters of personal data protection, through the provision of courses, seminars, workshops and any other form of teaching and training that is considered pertinent.

Article 93. The Institute and the Guarantor Agencies, within the scope of their respective powers, must:

I Promote that in the programs and curricula, books and materials used in educational institutions of all levels and modalities of the State, contents on the right to protection of personal data are included, as well as a culture on the exercise and respect of it;

II. Promote, together with higher education institutions, the integration of research, dissemination and teaching centers on the right to protection of personal data that promote knowledge on this subject and assist the Institute and the Guarantor Bodies in their substantive tasks, and

III. Promote the creation of spaces for social and citizen participation that stimulate the exchange of ideas between society, citizen representation bodies and those responsible.

NINTH TITLE

OF THE CHALLENGE PROCEDURES REGARDING DATA PROTECTION PERSONAL IN POSSESSION OF OBLIGATED SUBJECTS

Chapter I

Provisions Common to Revision Resources and Nonconformity Resources

Article 94. The owner or his representative may file an appeal for review or an appeal for disagreement with the Institute or Guarantor Agencies, as appropriate, or with the Transparency Unit, through the following means:

I In free writing at the domicile of the Institute or the Guarantor Agencies, as appropriate, or at the authorized offices established for this purpose;

II. By certified mail with acknowledgment of receipt;

III. By formats issued for this purpose by the Institute or the Guarantor Agencies, as appropriate;

IV. By electronic means authorized for this purpose, or

v. Any other means established for this purpose by the Institute or the Guarantor Agencies, as appropriate.

It will be presumed that the holder accepts that the notifications are made through the same channel as submitted his brief, unless he proves that he has indicated a different one to receive notifications.

Article 95. The holder may prove his identity through any of the following means:

I Official identification;

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

III. Authentication mechanisms authorized by the Institute and the Guarantor Agencies, as appropriate, published by general agreement in the Official Gazette of the Federation or in the official newspapers and gazettes of the Federal Entities.

The use of the advanced electronic signature or the electronic instrument that replaces it will exempt the presentation of the copy of the identification document.

Article 96. When the holder acts through a representative, he must prove his personality in the following terms:

I If it is a natural person, through a simple power of attorney signed before two witnesses, attaching a copy of the identification of the subscribers, or public instrument, or declaration in personal appearance of the holder and the representative before the Institute.

II. If it is a moral person, through a public instrument.

Article 97. The filing of an appeal for review or nonconformity of personal data concerning deceased persons, may be carried out by the person who proves to have a legal or legitimate interest.

Article 98. In the substantiation of the appeals for review and appeals for disagreement, the notifications issued by the Institute and the Guarantor Agencies, as appropriate, will take effect on the same day they are made.

Notifications may be made:

I Personally in the following cases:

a) It is the first notification;

b) It is the requirement of an act to the party that must comply with it;

c) In the case of the request for reports or documents;

d) In the case of the resolution that puts an end to the procedure in question, and

e) In other cases provided by law;

II. By certified mail with acknowledgment of receipt or digital means or systems authorized by the Institute or Guarantor Agencies, as appropriate, and published by general agreement

in the Official Gazette of the Federation or official newspapers or gazettes of the Federal Entities, in the case of requirements, summons, requests for reports or documents and resolutions that may be challenged;

III. By ordinary postal mail or by ordinary electronic mail in the case of acts other than those indicated in the previous sections, or

IV. By courtrooms, when the person who must be notified is not reachable at his address, he or his representative is ignored.

Article 99. The computation of the terms indicated in this Title will begin to run from the day following that on which the corresponding notification has taken effect.

Once the deadlines set for the parties have concluded, the right that should have been lost within them will be considered lost. exercise, without the need for an acknowledgment of rebellion by the Institute.

Article 100. The owner, the person in charge and the Guarantor Agencies or any authority must meet the information requirements within the terms and conditions established by the Institute and the Guarantor Agencies, as appropriate.

Article 101. When the owner, the person in charge, the Guarantor Agencies or any authority refuse to meet or comply with the requirements, requests for information and documentation, summons, summons or proceedings notified by the Institute or the Guarantor Agencies, as appropriate, or facilitate the performance of the proceedings that have been ordered, or hinders the actions of the Institute or the Guarantor Agencies, as appropriate, will have lost their right to enforce it at some other point in the procedure and the Institute and the Guarantor Agencies, as appropriate, will have by certain the facts matter of the procedure and will resolve with the elements that it has.

Article 102. In the substantiation of the appeals for review or appeals for disagreement, the parties may offer the following tests:

I The public documentary;

II. The private documentary;

III. The inspection;

IV. The expert;

v. The testimonial;

SAW. The confessional, except in the case of authorities;

VII. The photographic images, electronic pages, writings and other elements contributed by science and technology, and

VII. The legal and human presumption.

The Institute and the Guarantor Agencies, as appropriate, may obtain the means of proof that they deem necessary, without further limitation than those established by law.

Chapter II

Of the Appeal for Review before the Institute and the Guarantor Agencies

Article 103. The holder, by himself or through his representative, may file an appeal for review before the Institute or, as the case may be, before the Guarantor Organizations or the Transparency Unit of the person in charge who has heard of the request for the exercise of the ARCO rights, within a period that may not exceed fifteen days from the day following the date of notification of the response.

Once the period provided for responding to a request for the exercise of ARCO rights has elapsed without it having been issued, the owner or, where appropriate, his representative may file the appeal for review within fifteen days following the expiration date. the deadline to respond.

Article 104. The appeal for review will proceed in the following cases:

I The personal data is classified as confidential without complying with the characteristics indicated in the applicable laws;

II. The non-existence of personal data is declared;

III. Incompetence is declared by the person in charge;

IV. Incomplete personal data is delivered;

v. Personal data is delivered that does not correspond to what was requested;

SAW. Access, rectification, cancellation or opposition of personal data is denied;

VII. No response is given to a request for the exercise of ARCO rights within the terms established in this Law and other provisions that are applicable in the matter;

VII. Personal data is delivered or made available in a modality or format other than the one requested, or in an incomprehensible format;

IX. The owner is dissatisfied with the costs of reproduction, shipping or delivery times of personal data;

X. The exercise of ARCO rights is hindered, despite the fact that their origin was notified;

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

XII. In other cases provided by law.

Article 105. The only requirements required in the writ of filing of the appeal for review will be the following:

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

II. The name of the holder who appeals or his representative and, where appropriate, of the interested third party, as well as the address or means indicated to receive notifications;

III. The date on which the response was notified to the owner, or, in the event of a lack of response, the date of the filing of the application for the exercise of ARCO rights;

IV. The act that is appealed and the petitions, as well as the reasons or motives for disagreement;

v. If applicable, a copy of the contested answer and the corresponding notification, and

SAW. The documents that prove the identity of the holder and, where appropriate, the personality and identity of his representative.

The review appeal may be accompanied by the evidence and other elements that the owner considers appropriate to submit to the judgment of the Institute or, where appropriate, of the Guarantor Agencies.

In no case will it be necessary for the holder to ratify the appeal for review filed.

Article 106. Once the appeal for review has been admitted, the Institute or, as the case may be, the Guarantor Agencies may seek a conciliation between the owner and the person in charge.

If an agreement is reached, it will be recorded in writing and will be binding. The appeal for review will remain without matter and the Institute, or as the case may be, the Guarantor Agencies, must verify compliance with the respective agreement.

Article 107. Once the appeal for review has been admitted and without prejudice to the provisions of article 65 of this Law, the Institute will promote conciliation between the parties, in accordance with the following procedure:

I The Institute and the Guarantor Agencies, as appropriate, will require the parties to express, by any means, their willingness to conciliate, within a period not exceeding seven days, counted from the notification of said agreement, which will contain a summary of the appeal for review and the response of the person in charge, if any, pointing out the common elements and points of controversy.

The conciliation may be held in person, by remote or local means of electronic communication or by any other means determined by the Institute or the Guarantor Agencies, as appropriate. In any case, the conciliation must be recorded by the means that allows its existence to be proven.

It is exempt from the conciliation stage, when the owner is a minor and any of the rights contemplated in the Law for the Protection of the Rights of
Girls, Boys and Adolescents, linked to the Law and the Regulation, unless they have duly accredited legal representation;

II. Once the possibility of conciliation has been accepted by both parties, the Institute and the Guarantor Agencies, as appropriate, will indicate the place or means, day and time for holding a conciliation hearing, which must be held within the ten days following the The Institute or the Guarantor Agencies, as appropriate, have received the declaration of the will to conciliate from both parties, in which the interests between the owner and the person in charge will be sought.

The conciliator may, at any time during the conciliation stage, require the parties to present, within a maximum period of five days, the elements of conviction that he deems necessary for the conciliation.

The bankruptcy conciliator may suspend the hearing for one occasion when he deems it pertinent or at the request of both parties. In the event that the hearing is suspended, the conciliator will set a date and time for its resumption within the following five days.

The respective record will be drawn up from any conciliation hearing, stating the result thereof. In the event that the person in charge or the owner or their respective representatives do not sign the minutes, this will not affect its validity, and said refusal must be recorded;

III. If any of the parties does not attend the conciliation hearing and justifies their absence within a period of three days, they will be summoned to a second conciliation hearing, within a period of five days; in case you do not go to the latter, the review resource will continue. When any of the parties does not attend the conciliation hearing without any justification, the procedure will continue;

IV. If there is no agreement in the conciliation hearing, the review resource will continue;

v. If an agreement is reached, it will be recorded in writing and will be binding. The appeal for review will remain without matter and the Institute, or, as the case may be, the Guarantor Agencies, must verify compliance with the respective agreement, and

SAW. Compliance with the agreement will conclude the substantiation of the appeal for review, otherwise, the Institute will resume the procedure.

The period referred to in the following article of this Law will be suspended during the period of compliance with the conciliation agreement.

Article 108. The Institute and the Guarantor Agencies will resolve the appeal for review within a period not may exceed forty days, which may be extended up to twenty days only once.

Article 109. During the procedure referred to in this Chapter, the Institute and the Guarantor Agencies, as appropriate, must apply the substitution of the complaint in favor of the owner, as long as it does not alter the original content of the review resource, nor modify the facts or petitions set forth therein, as well as guarantee that the parties can present the arguments and records that support and motivate their claims.

Article 110. If in the writ of filing of the appeal for review the holder does not meet any of the requirements set forth in article 105 of this Law and the Institute and the Guarantor Agencies, as appropriate, do not have elements to remedy them, they They must require the owner, for a single occasion, the information that corrects the omissions within a period that may not exceed five days, counted from the day following the presentation of the document.

The holder will have a term that may not exceed five days, counted from the day following the notification of the prevention, to correct the omissions, with the warning that in case of not complying with the requirement, the document will be discarded. review appeal.

The prevention will have the effect of interrupting the term that the Institute and the Guarantor Agencies have to resolve the resource, so it will begin to be computed from the day following its release.

Article 111. The resolutions of the Institute or, where appropriate, of the Guarantor Agencies may:

I Dismiss or dismiss the appeal for review as inadmissible;

II. Confirm the response of the person in charge;

III. Revoke or modify the response of the person in charge, or

IV. Order the delivery of personal data, in case of omission of the person in charge.

The resolutions will establish, where appropriate, the deadlines and terms for their fulfillment and the procedures to ensure their execution. Those responsible must inform the Institute or, as the case may be, the Guarantor Agencies of compliance with their resolutions.

In the absence of a resolution by the Institute, or, as the case may be, by the Guarantor Bodies, the response of the person in charge will be understood as confirmed.

When the Institute, or, as the case may be, the Guarantor Agencies, determine during the substantiation of the appeal for review that a probable liability may have been incurred due to non-compliance with the obligations set forth in this Law and other provisions that are applicable in the matter , they must inform the internal control body or the competent body so that it can initiate, where appropriate, the respective liability procedure.

Article 112. The appeal for review may be dismissed as inadmissible when:

I It is untimely due to the expiration of the term established in article 103 of this Law;

II. The owner or his representative do not duly prove his identity and personality of the latter;

III. The Institute or, as the case may be, the Guarantor Agencies have previously made a final decision on the matter of the same;

IV. Not update any of the causes of the review resource provided for in article 104 of this Law;

v. An appeal or means of defense filed by the appellant, or, as the case may be, by the interested third party, against the act appealed against is being processed before the competent courts. Institute or Guarantor Agencies, as appropriate;

SAW. The appellant modifies or expands his request in the appeal for review, only with respect to the new contents, or

VII. The appellant does not prove legal interest.

The rejection does not imply the preclusion of the holder's right to file before the Institute or the Guarantor agencies, as appropriate, a new appeal for review.

Article 113. The appeal for review may only be dismissed when:

I The appellant expressly withdraws;

II. The appellant dies;

III. Once the appeal for review is admitted, any cause of inadmissibility is updated in the terms of this Law;

IV. The person in charge modifies or revokes his response in such a way that the appeal for review is no matter, or

v. The appeal for review remains without matter.

Article 114. The Institute and the Guarantor Agencies must notify the parties and publish the resolutions, in a public version, no later than the third day following their approval.

Article 115. The resolutions of the Institute and of the Guarantor Agencies shall be binding, final and unassailable for those responsible.

The holders may challenge said resolutions before the Judicial Power of the Federation through the Amparo Trial.

Article 116. In the case of the resolutions to the review resources of the Guarantor Agencies of the Federal Entities, individuals may choose to go before the Institute by filing the appeal of disagreement provided for in this Law or before the Judicial Power of the Federation through the Judgment of Amparo.

Chapter III

Of the Appeal of Disagreement before the Institute

Article 117. The holder, by himself or through his representative, may challenge the resolution of the appeal for review issued by the guarantor body before the Institute, through the appeal of disagreement.

The appeal for disagreement may be filed with the guarantor body that issued the resolution or with the Institute, within a term of fifteen days counted from the day following the date of notification of the contested resolution.

The Guarantor Agencies must send the appeal of disagreement to the Institute the day after receiving it; as well as the records that make up the procedure that gave rise to the contested resolution, which will be resolved by gathering the elements it deems appropriate.

Article 118. The appeal of disagreement will proceed against the resolutions issued by the Organisms Guarantors of the Federal Entities that:

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

II. Determine the non-existence of personal data, or

III. Declare the denial of personal data, that is:

a) Incomplete personal data is delivered;

b) Personal data is delivered that does not correspond to those requested;

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

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

and) The owner is dissatisfied with the costs of reproduction, shipping, or delivery times of personal data, or

f) It is oriented to a specific procedure that contravenes the provisions of article 54 of this Law.

Article 119. The only required and essential requirements in the writ of filing of the appeal of disagreement are:

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

II. The guarantor body that issued the contested resolution;

III. The name of the holder who appeals or of his representative and, where appropriate, of the interested third party, as well as his address or the means indicated to receive notifications;

IV. The date on which the resolution was notified to the holder;

v. The act that is appealed and the petitions, as well as the reasons or motives for disagreement;

SAW. If applicable, a copy of the resolution being challenged and the corresponding notification, and

VII. The documents that prove the identity of the holder and, where appropriate, the personality and identity of his representative.

The petitioner may accompany his writing with the evidence and other elements that he considers appropriate to submit to the Institute's judgment.

Article 120. The Institute will resolve the appeal of disagreement within a term that may not exceed thirty days counted from the day following the filing of the appeal of disagreement, a term that may be extended only once and up to an equal period.

Article 121. During the procedure referred to in this Chapter, the Institute must apply the substitution of the complaint in favor of the holder, as long as it does not alter the original content of the appeal of disagreement, nor modify the facts or petitions exposed in the same, as well as guarantee that the parties can present the arguments and evidence that support and motivate their claims.

Article 122. If in the writ of filing of the appeal of disagreement the holder does not comply with any of the requirements set forth in article 119 of this Law and the Institute does not have elements to correct them, it must require the holder, for a single occasion, the information that corrects the omissions within a period that may not exceed five days, counted from the day following the presentation of the document.

The holder will have a term that may not exceed fifteen days, counted from the day following the notification of the prevention, to correct the omissions, with the warning that in case of not complying with the requirement, the document will be discarded. disagreement appeal.

The prevention will have the effect of interrupting the period that the Institute has to resolve the appeal, therefore which will begin to be computed from the day following its discharge.

Article 123. Once the evidentiary stage is concluded, the Institute will make the proceedings of the procedure available to the parties and will grant them a period of five days to formulate allegations counted from the notification of the agreement referred to in this article.

Article 124. The resolutions of the Institute may:

I Dismiss or dismiss the appeal of disagreement;

II. Confirm the resolution of the guarantor agency;

III. Revoke or modify the resolution of the guarantor agency, or

IV. Order the delivery of personal data, in case of omission of the person in charge.

The resolutions will establish, where appropriate, the deadlines and terms for their fulfillment and the procedures to ensure their execution. The Guarantor Agencies must inform the Institute about compliance with their resolutions.

If the Institute does not resolve within the term established in this Chapter, the resolution that was appealed understand confirmed.

When the Institute determines during the substantiation of the non-conformity appeal, that a probable liability may have been incurred due to non-compliance with the obligations set forth in this Law and the other applicable provisions on the matter, it must inform the internal control body. or of the competent instance so that it initiates, where appropriate, the respective liability procedure.

The measures of urgency provided for in this Law, will be applicable for the purposes of compliance with the resolutions that fall on the resources of nonconformity. These enforcement measures must be established in the resolution itself.

Article 125. The motion for disagreement may be dismissed as inadmissible when:

I It is untimely due to the expiration of the term established in article 117 of this Law;

II. The Institute has previously made a final decision on the matter of the same;

III. The causes of origin of the appeal of disagreement, provided for in article 118 of this Law, are not updated;

IV. An appeal or means of defense filed by the owner, or, as the case may be, by the interested third party, against the appealed act is being processed before the Judicial Power, or

v. The non-conformist expands his request in the non-conformity resource, only with respect to the new contents.

Article 126. The motion for disagreement may only be dismissed when:

I The appellant expressly withdraws;

II. The appellant dies;

III. The guarantor body modifies or revokes its response in such a way that the appeal of disagreement is without matter, or

IV. Once the appeal is admitted, any cause of inadmissibility is updated in the terms of this Law.

Article 127. In the cases in which the resolution of the guarantor body is modified or revoked through the appeal for disagreement, it must issue a new ruling in accordance with the guidelines that were set when resolving the disagreement, within a period of fifteen days, counted from from the day following the day on which the resolution issued in the disagreement was notified or became known.

Article 128. It will correspond to the Guarantor Agencies, within the scope of their competence, to carry out the follow-up and surveillance of due compliance by the person responsible for the new resolution issued as a result of the non-conformity in terms of this Law.

Article 129. The resolutions of the Institute will be binding, final and unassailable for those responsible and the Guarantor Agencies.

The holders may challenge said resolutions before the Judicial Power of the Federation through the Amparo Trial.

Chapter IV

Of the Attraction of Review Resources

Article 130. For the purposes of this Law, the Plenum of the Institute, when approved by the majority of its Commissioners, ex officio or at the well-founded request of the Guarantor Agencies, may exercise the power of attraction to hear those appeals for review pending resolution on the protection of personal data, which due to its interest and importance so warrant and whose original competence corresponds to the Guarantor Agencies, in accordance with the provisions of this Law and other applicable regulations.

The appellants may make the Institute aware of the existence of appeals for review that it may be aware of ex officio.

With regard to the general guidelines and criteria of mandatory observance that the Institute must issue to determine the appeals for review of interest and importance that it is obliged to know, in accordance with the General Law of Transparency and Access to Public Information, additionally in In attracting appeals for review in matters of personal data protection, the following factors must be considered:

I The purpose of the processing of personal data;

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

III. The sensitivity of the personal data processed;

IV. The possible consequences that would derive from an improper or indiscriminate treatment of personal data, and

v. The relevance of the processing of personal data, in attention to the social or economic impact of the same and the public interest to know about the review resource attracted.

Article 131. For purposes of exercising the power of attraction referred to in this Chapter, the Institute will motivate and substantiate that the case is of such relevance, novelty or complexity, that its resolution may have a substantial impact on the solution of future cases. to guarantee the effective protection of the right to protection of personal data in possession of obligated subjects.

In the cases in which the guarantor body of the Federal Entity is the obliged subject appealed, it must notify the Institute, within a term that will not exceed three days, from the filing of the appeal. The Institute will attract and resolve said appeals for review, in accordance with the provisions of this Chapter.

Article 132. The reasons issued by the Institute to exercise the power to attract a case, will only constitute a preliminary study to determine if the matter meets the constitutional and legal requirements of interest and importance, in accordance with the previous precept, for which it will not be necessary that they form part of the substantive analysis of the matter.

Article 133. The Institute will issue guidelines and general criteria of mandatory observance that allow determining the appeals of interest and transcendence that it will be obliged to know, as well as the internal procedures for their processing, taking into account the maximum terms indicated for the appeal of review. .

Article 134. The faculty of attraction conferred on the Institute must be exercised in accordance with the following rules:

I When it is carried out ex officio, the Plenum of the Institute, when approved by the majority of its Commissioners, may exercise the attraction at any time, as long as the appeal for review has not been resolved by the competent guarantor agency, for which it will notify the parties and request the File from the corresponding guarantor agency, or

II. When the request for attraction is made by the guarantor body of the Federal Entity, it will have a period of no more than five days, except as provided in the last paragraph of article 105 of this Law, to request the Institute to analyze and, in your case, exercise the power of attraction on the matter put to your consideration.

Once said period has elapsed, the right of the respective guarantor body to make attraction request.

The Institute will have a period of no more than ten days to determine if it exercises the power of attraction, in In which case, it will notify the parties and request the File of the respective appeal for review.

Article 135. The request for the attraction of the appeal for review will interrupt the term that the Guarantor Agencies have to resolve it. The computation will continue from the day following the day on which the Institute has notified the determination not to attract the appeal for review.

Article 136. Prior to the decision of the Institute on the exercise of the power of attraction referred to in the previous article, the guarantor body of the Federal Entity to which the original knowledge of the matter corresponds, must exhaust the analysis of all the aspects whose study is prior to the substance of the matter, with the exception of the case in which the aspects of importance and transcendence derive from the origin of the resource.

If the Plenary of the Institute, when approved by the majority of its Commissioners, decides to exercise the power of attraction, it will be devoted to the knowledge or substantive study of the subject matter of the appeal for review attracted.

The Commissioner or Commissioners who at the time had voted against exercising the power of attraction, They will not be prevented from ruling on the merits of the matter.

Article 137. The resolution of the Institute will be final and unassailable for the guarantor agency and for the obligated subject in question.

At all times, individuals may challenge the resolutions of the Institute before the Judicial Power of the Federation.

Article 138. Only the Legal Advisor of the Government may file an appeal for review in matters of national security before the Supreme Court of Justice of the Nation, in the event that the resolutions of the Institute to the appeals described in this Title, may endanger the National security.

Said appeal for review in matters of national security will be processed in the terms established in the following Chapter V called "Review Appeal in matters of National Security", of this Title.

Chapter V

Of the Revision Resource in Matters of National Security

Article 139. The Legal Counselor of the Federal Government may file an appeal for review in matters of national security directly before the Supreme Court of Justice of the Nation, when he considers that the resolutions issued by the Institute endanger national security.

The appeal must be filed during the seven days following that in which the guarantor body notifies the resolution to the obligated subject. The Supreme Court of Justice of the Nation will determine, immediately, in its case, the suspension of the execution of the resolution and within the five days following the filing of the appeal it will decide on its admission or inadmissibility.

Article 140. In the writ of the appeal, the Federal Government's Legal Adviser must indicate the resolution being challenged, the grounds and reasons for which he considers that national security is endangered, as well as the necessary evidence.

Article 141. The reserved or confidential information that, if applicable, is requested by the Supreme Court of Justice of the Nation as it is essential to resolve the matter, must be kept as such and will not be available in the File, except in the exceptions provided for in article 120 of the General Law of Transparency and Access to Public Information.

At all times, the Ministers must have access to classified information to determine its nature, as required. Access will be given in accordance with the regulations previously established for the protection or safeguarding of information by the obligated subjects.

Article 142. The Supreme Court of Justice of the Nation will resolve with full jurisdiction, and in In any case, the forwarding will proceed.

Article 143. If the Supreme Court of Justice of the Nation confirms the meaning of the appealed resolution, the obliged subject must comply in the terms established by the corresponding provision of this Law.

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

Chapter VI

Of the Interpretation Criteria

Article 144. Once the resolutions issued on the occasion of the resources that are submitted to its jurisdiction have been enforced, the Institute may issue the interpretation criteria that it deems pertinent and that derive from what is resolved in them, in accordance with the provisions of the General Law of Transparency and Access to Public Information and other applicable regulations.

The Institute may issue guiding criteria for the Guarantor Agencies, which will be established by reiteration upon resolving three analogous cases consecutively in the same direction, by at least two thirds of the Plenary of the Institute, derived from resolutions that have caused status.

Article 145. The criteria will be composed of a heading, a text and the precedent or precedents that, in its case, originated its issuance.

All criteria issued by the Institute must contain a control code for proper identification.

TENTH TITLE

VERIFICATION POWER OF THE INSTITUTE AND GUARANTEE AGENCIES

Single Chapter

Verification Procedure

Article 146. The Institute and the Guarantor Agencies, within the scope of their respective powers, will have the authority to monitor and verify compliance with the provisions contained in this Law and other regulations that derive from it.

In the exercise of surveillance and verification functions, the personnel of the Institute or, as the case may be, of the Guarantor Agencies will be obliged to keep confidential the information to which they have access by virtue of the corresponding verification.

The person in charge may not deny access to the requested documentation for the purpose of a verification, or to your personal databases, nor can you invoke the reservation or confidentiality of the information.

Article 147. Verification may start:

I Ex officio when the Institute or the Guarantor Agencies have indications that lead to the presumption of founded and motivated existence of violations of the corresponding laws, or

II. By complaint of the holder when he considers that he has been affected by acts of the person in charge that may be contrary to the provisions of this Law and other applicable regulations, or, where appropriate, by any person when he is aware of alleged breaches of the obligations set forth in the this Law and other provisions that are applicable in the matter.

The right to file a complaint expires within a year from the day after the acts or omissions that are the subject of the complaint are made. When the acts or omissions are successive, the term will begin to count from the business day following the last act carried out.

The verification will not proceed in the cases of origin of the appeal for review or disagreement provided for in this Law.

The verification will not be admitted in the cases of origin of the appeal for review or disagreement, provided for in this Law.

Prior to the respective verification, the Institute or the Guarantor Agencies may carry out preliminary investigations, in order to have elements to found and motivate the respective initiation agreement.

Article 148. For the presentation of a complaint, greater requirements than those that they are described below:

I The name of the person filing the complaint, or, where appropriate, of their representative;

II. The address or means to receive notifications from the person denouncing;

III. The list of facts on which the complaint is based and the elements you have to prove your statement;

IV. The person in charge reported and their address, or where appropriate, the data for their identification and/or location;

v. The signature of the complainant, or where appropriate, of his representative. If you do not know how to sign, your fingerprint will suffice.

The complaint may be submitted in free writing, or through formats, electronic means or any other means established for this purpose by the Institute or the Guarantor Agencies, as appropriate.

Once the complaint is received, the Institute and the Guarantor Agencies, as appropriate, must acknowledge receipt of it. The corresponding agreement will be notified to the complainant.

Article 149. The verification will begin by means of a written order that establishes and motivates the origin of the action by the Institute or the Guarantor Agencies, which has the purpose of requesting from the person in charge the necessary documentation and information related to the presumed violation and/or make visits to the offices or facilities of the person in charge, or where appropriate, in the place where the respective personal databases are located.

For verification in instances of national security and public security, the resolution will require the approval of the Plenary of the Institute, by a qualified majority of its Commissioners, or of the members of the Guarantor Agencies of the Federal Entities, as appropriate; as well as a reinforced foundation and motivation of the cause of the procedure, having to ensure the information only for the exclusive use of the authority and for the purposes established in article 150.

The verification procedure must have a maximum duration of fifty days.

The Institute or the guarantor agencies may order precautionary measures, if from the relief of the verification they notice an imminent or irreparable damage in terms of personal data protection, as long as they do not prevent the fulfillment of the functions or the securing of databases of the obligated subjects.

These measures may only have a corrective purpose and will be temporary until the regulated entities carry out the recommendations made by the Institute or the Guarantor Agencies, as appropriate.

Article 150. The verification procedure will conclude with the resolution issued by the Institute or the Guarantor Agencies, in which the measures to be adopted by the person responsible will be established within the term determined by it.

Article 151. Those responsible may voluntarily submit to audits by the Institute or the Guarantor Agencies, as appropriate, whose purpose is to verify the adaptation, adequacy and effectiveness of the controls, measures and mechanisms implemented for compliance with the provisions provided for in this Law and other applicable regulations.

The audit report must rule on the adequacy of the measures and controls implemented by the person in charge, identify their deficiencies, as well as propose complementary corrective actions, or, if applicable, recommendations.

TITLE ELEVEN

ENFORCEMENT MEASURES AND RESPONSIBILITIES

Chapter I

Of the enforcement measures

Article 152. In order to comply with the resolutions issued by the Institute or the Guarantor Agencies, as appropriate, these agencies and the person in charge, if applicable, must observe the provisions of Chapter VI of Title Eight of the General Law of Transparency and Access to Public Information.

Article 153. The Institute and the Guarantor Agencies may impose the following enforcement measures to ensure compliance with its determinations:

I The public warning, or

II. The fine, equivalent to the amount of one hundred and fifty to one thousand five hundred times the daily value of the Measurement and Updating Unit.

The non-compliance of the obligated subjects will be disseminated in the portals of transparency obligations of the Institute and the Guarantor Agencies and considered in the evaluations carried out by them.

In the event that non-compliance with the determinations of the Institute and the Guarantor Agencies implies the alleged commission of a crime or one of the conducts indicated in article 163 of this Law, they must report the facts to the competent authority. Economic constraint measures may not be covered with public resources.

Article 154. If, despite the execution of the measures of urgency provided for in the previous article, the resolution is not complied with, compliance will be required from the hierarchical superior so that within a period of five days he is forced to comply without delay.

If non-compliance persists, enforcement measures established in the previous article will be applied. Once the term has elapsed, without compliance having been given, the competent authority regarding responsibilities will be given a hearing.

Article 155. The enforcement measures referred to in this Chapter must be applied by the Institute and the Guarantor Agencies, by themselves or with the support of the competent authority, in accordance with the procedures established by the respective laws.

Article 156. The fines set by the Institute and the Guarantor Agencies shall be made effective by the Tax Administration Service or the Finance Secretariats of the Federal Entities, as appropriate, through the procedures established by law.

Article 157. To qualify the enforcement measures established in this Chapter, the Institute and the Guarantor Agencies must consider:

I The seriousness of the fault of the person responsible, determined by elements such as the damage caused; indications of intent; the duration of non-compliance with the determinations of the Institute or Guarantor Agencies and the impact on the exercise of their powers;

II. The economic condition of the offender, and

III. The recurrence.

The Institute and the Guarantor Agencies will establish through general guidelines, the attributions of the areas in charge of qualifying the seriousness of the non-compliance with their determinations and of the notification and execution of the enforcement measures that they apply and implement, in accordance with the elements developed in this chapter.

Article 158. In case of recidivism, the Institute or the Guarantor Organizations may impose a fine equivalent to twice that determined by the Institute or the Guarantor Agencies.

A repeat offender will be considered to be one who, having incurred in an infraction that has been sanctioned, commits another of the same type or nature.

Article 159. The enforcement measures must be applied and implemented within a maximum period of fifteen days, counted from the notification of the enforcement measure to the offender.

Article 160. The public reprimand will be imposed by the Institute or the Guarantor Organizations and will be executed by the immediate hierarchical superior of the offender with whom it is related.

Article 161. The Institute or the Guarantor Agencies may require the offender to provide the necessary information to determine their economic condition, aware that if they do not provide it, the fines will be quantified based on the elements available, understood as those found in public registries, those that contain information media or their own Internet pages and, in general, anyone that evidences their condition, the Institute or the Guarantor Agencies being empowered to request that documentation that is considered essential for such effect to the competent authorities.

Article 162. Against the imposition of coercive measures, the corresponding appeal before the Judicial Power of the Federation, or in its case before the corresponding Judicial Power in the Federative Entities, proceeds.

Chapter II

of the sanctions

Article 163. They will be causes of sanction for non-compliance with the obligations established in the matter of this Law, the following:

I Act with negligence, intent or bad faith during the substantiation of requests for the exercise of ARCO rights;

II. Failure to comply with the attention deadlines provided for in this Law to respond to requests for the exercise of ARCO rights or to make the right in question effective;

III. Using, stealing, disclosing, hiding, altering, mutilating, destroying or rendering useless, in whole or in part, and in an improper manner, personal data that is in their custody or to which they have access or knowledge due to their employment, position or commission;

IV. Intentionally treating personal data in contravention of the principles and duties established in this Law;

v. Not having the privacy notice, or omitting in it any of the elements referred to in article 27 of this Law, as the case may be, and other provisions that are applicable in the matter;

SAW. Classify as confidential, with intent or negligence, personal data without complying with the characteristics indicated in the applicable laws. The sanction will only proceed when there is a prior resolution, which has been finalized, regarding the criteria for classifying personal data;

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

VII. Failure to establish security measures in the terms established in articles 31, 32 and 33 of this Law;

IX. Submit violations of personal data due to the lack of implementation of security measures according to articles 31, 32 and 33 of this Law;

X. Carry out the transfer of personal data, in contravention of the provisions of this Law;

XI. Obstruct the acts of verification of the authority;

XII. Create personal databases in violation of the provisions of article 5 of this Law;

XIII. Failure to abide by the resolutions issued by the Institute and the Guarantor Agencies, and

XIV. Failing to deliver the annual report and other reports referred to in article 44, section VII of the General Law of Transparency and Access to Public Information, or else, deliver the same in an extemporaneous manner.

The causes of responsibility provided for in sections I, II, IV, VI, X, XII, and XIV, as well as recidivism in the conduct provided for in the rest of the sections of this article, will be considered as serious for the purposes of its administrative sanction.

In the event that the alleged infraction was committed by a member of a political party, the investigation and, where appropriate, sanction, will correspond to the competent electoral authority.

Sanctions of an economic nature may not be covered with public resources.

Article 164. For the behaviors referred to in the previous article, the authority will be given a hearing. competent to impose or execute the sanction.

Article 165. The responsibilities that result from the corresponding administrative procedures, derived from the violation of the provisions of article 163 of this Law, are independent of those of the civil, criminal or any other type that may derive from the same facts. .

Said responsibilities will be determined, autonomously, through the procedures provided for in the applicable laws and the sanctions that, if applicable, are imposed by the competent authorities, will also be executed independently.

For such purposes, the Institute or the guarantor agencies may report to the competent authorities any act or omission that violates this Law and provide the evidence they deem pertinent, under the terms of the applicable laws.

Article 166. In the event of non-compliance by political parties, the Institute or competent guarantor body, will give a hearing, as appropriate, to the National Electoral Institute or to the local public electoral bodies of the competent Federal Entities, so that they resolve the appropriate, without prejudice to the sanctions established for political parties in the applicable laws.

In the case of probable infractions related to trusts or public funds, the Institute or competent guarantor body must give a view to the internal control body of the obligated subject related to these, when they are public servants, in order to implement the administrative procedures to which there is place.

Article 167. In those cases in which the alleged offender is a public servant, the Institute or the guarantor body must submit to the competent authority, together with the corresponding complaint, a File containing all the elements that support the presumed administrative liability.

The authority that knows the matter, must report the conclusion of the procedure and, where appropriate, the execution of the sanction to the Institute or the guarantor agency, as appropriate.

In order to substantiate the procedure cited in this article, the Institute, or the corresponding guarantor body, must prepare a complaint addressed to the comptroller, internal control body or equivalent, with the precise description of the acts or omissions that, in its opinion, consideration, affect the proper application of this Law and that could constitute a possible liability.

Likewise, it must prepare a file that contains all those elements of evidence that it considers pertinent to support the existence of the possible responsibility. For this purpose, the causal link between the disputed facts and the evidence presented must be proven.

The complaint and the File must be sent to the comptroller's office, internal control body or equivalent within fifteen days after the Institute or the corresponding guarantor body becomes aware of the facts.

Article 168. In the event that non-compliance with the determinations of the Guarantor Agencies implies the alleged commission of a crime, the respective guarantor agency must report the facts to the competent authority.

TRANSIENT

First. This Law shall enter into force the day after its publication in the Official Gazette of the Federation.

Second. The Federal Law of Transparency and Access to Public Information, the other federal laws and the current laws of the Federal Entities regarding the protection of personal data, must comply with the provisions set forth in this rule within a period of six months following counted from the entry into force of this Law.

In the event that the Congress of the Union or the Legislatures of the Federal Entities omit totally or partially to carry out the legislative adjustments that may take place, within the term established in the previous paragraph, this Law will be directly applicable, with the possibility to continue applying the pre-existing laws in a supplementary manner in everything that does not oppose it, until the condition imposed in this article is fulfilled.

Third. The Chamber of Deputies, the Legislatures of the Federal Entities, within the scope of their respective powers, must make the necessary budget provisions for the operation of this Law and establish the specific budget items in the Expenditure Budget of the Federation and in the Expenditure Budgets of the Federal Entities, as appropriate, for the fiscal year following its entry into force.

Bedroom. All provisions regarding the protection of personal data, federal, state and municipal nature, which contravene the provisions of this Law.

Fifth. The Institute and the Guarantor Agencies must issue the guidelines referred to in this Law and publish them in the Official Gazette of the Federation, or in their local Official Gazettes or Newspapers, respectively, no later than one year from the entry into force. of this Decree.

Sixth. The National System of Transparency, Access to Information and Protection of Personal Data must issue the National Program for the Protection of Personal Data referred to in this Law and publish it in the Official Gazette of the Federation, no later than one year from the entry into force of this Decree, regardless of the exercise of other powers arising from the General Law of Transparency and Access to Public Information.

Seventh. The corresponding obligated subjects must process, issue or modify their regulations no later than eighteen months after the entry into force of this Law.

Eighth. They may not be reduced or expanded in the regulations of the Federal Entities, the current procedures and deadlines applicable in the matter, to the detriment of the owners of personal data.

Mexico City, December 13, 2016.- Sen. **Pablo Escudero Morales,** President.- Dip. **Edmundo Javier Bolaños Aguilar,** President.- Sen. **Lorena Cuellar Cisneros,** Secretary.- Dip. **María Eugenia Ocampo Bedolla,** Secretary.- Signatures."

In compliance with the provisions of section I of Article 89 of the Political Constitution of the United Mexican States, and for its due publication and observance, I issue this Decree at the Residence of the Federal Executive Power, in Mexico City, at twenty-four January two thousand and seventeen.- **Enrique Peña Nieto.-** Signature.- The Secretary of the Interior, **Miguel Ángel Osorio Chong.- Signature .**