GENERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY SUBJECTS OBLIGED

CURRENT TEXT

New Law published in the Official Gazette of the Federation on March 20, 2025

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

CLAUDIA SHEINBAUM PARDO, President of the United Mexican States, to its inhabitants know:

That the Honorable Congress of the Union has been pleased to address me with the following

DECREE

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

THE GENERAL LAW OF TRANSPARENCY AND ACCESS TO PUBLIC INFORMATION; THE GENERAL LAW OF PROTECTION OF PERSONAL DATA HELD BY OBLIGED SUBJECTS; THE FEDERAL PROTECTION LAW PERSONAL DATA HELD BY PRIVATE INDIVIDUALS; AND ARTICLE 37, SECTION XV, IS AMENDED THE ORGANIC LAW OF THE FEDERAL PUBLIC ADMINISTRATION

Article One.- ……

Article Two.- The General Law on the Protection of Personal Data Held by Subjects is hereby **issued .** Obliged, to remain as follows:

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

FIRST TITLE

GENERAL PROVISIONS

Single Chapter

Of the Object of the Law

Article 1. This Law regulates Articles 6, Base A, and 16, second paragraph, of the Political Constitution of the United Mexican States, regarding the protection of personal data in the possession of obligated subjects, and its provisions are of public order of social interest and of general observance throughout the national territory.

Article 2. The purpose of this Law is:

I. Establish the bases, principles and procedures to guarantee the right of every person to the protection of their personal data, held by obligated subjects;

II. Distribute powers between the Secretariat and the Guarantor Authorities regarding the protection of personal data held by obliged subjects;

III. 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;

IV. Ensure compliance with the principles of personal data protection provided for in this document Law and other provisions that are applicable in the matter;

V. Protect personal data in the possession of any authority, entity, body and organization of the Executive, Legislative and Judicial Powers, autonomous bodies, trusts and public funds, of the Federation, political parties, the Federative Entities and the municipalities, with the purpose of regulating their due treatment;

VI. Ensure that every person can exercise the right to the protection of personal data;

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

VIII. Establish mechanisms to ensure compliance and effective enforcement of appropriate enforcement measures for conduct that violates the provisions of this Law.

Article 3. For the purposes of this Law, the following terms 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, process, and be responsible for or in charge of personal data;

II. **Guarantor authorities:** Control and disciplinary body of the Judiciary; the internal control bodies of the autonomous constitutional bodies; the internal comptroller's offices of the Congress of the Union; the National Electoral Institute, with regard to access to the protection of personal data by political parties; and the bodies in charge of internal comptrollership or their counterparts.
Executive, Legislative and Judicial Powers, as well as the autonomous constitutional bodies, of the Federative Entities;

III. **Privacy Notice:** Document available to the data subject, whether physically, electronically, or in any format generated by the data controller, from the moment in which their personal data is collected, in order to inform them of the purposes for which said data is processed;

IV. **Databases:** An ordered set of personal data relating to an identified or identifiable person, subject to certain criteria, regardless of the form or method of its creation, type of support, processing, storage and organization;

V. **Blocking:** Identification and retention of personal data once the purpose for which it was collected has been fulfilled, for the sole purpose of determining potential liabilities related to its processing, until the statutory or contractual limitation period for such processing expires. During this period, personal data may not be processed, and once this period has elapsed, they will be deleted from the corresponding database.

VI. **Transparency Committee:** Body referred to in article 39 of the General Law of Transparency and Access to Public Information;

VII. **Cloud computing:** A model for the external provision of on-demand computing services, which involves the provision of infrastructure, a platform, or software, distributed flexibly, through virtual procedures, on dynamically shared resources;

VIII. **Consent:** Manifestation of the free, specific and informed will of the data subject through which the processing of the data is carried out;

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

X. **Sensitive personal data:** Data that relates to the most intimate sphere of the data subject, or whose improper use could give rise to discrimination or pose a serious risk to discrimination. By way of example, but not limited to, sensitive personal data includes data that may reveal aspects such as racial or ethnic origin, current or future health status, genetic information, religious, philosophical, and moral beliefs, political opinions, and sexual preference.

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

XII. **Days:** Business days;

XIII. **Dissociation:** Procedure by which personal data cannot be associated with the data subject nor, due to their structure, content or degree of disaggregation, allow their identification;

XIV. **Security document:** Instrument that describes and provides a general account of the technical, physical and administrative security measures adopted by the controller to guarantee the confidentiality, integrity and availability of the personal data it holds;

XV. **Personal data protection impact assessment:** Document through which obligated subjects who intend to implement or modify public policies, programs, computer systems or platforms, electronic applications or any other technology that involves the intensive or relevant processing 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 data subjects, as well as the duties of those responsible and those in charge, provided for in the applicable legal provisions;

XVI. **Publicly accessible sources:** Those databases, systems, or files that, by law, may be publicly consulted when there is no impediment imposed by a restrictive rule and with no other requirement than, where applicable, the payment of a fee, contribution, or consideration. A source shall not be considered publicly accessible when the information contained therein was obtained or comes from an illicit source, in accordance with the provisions of this Law and other applicable legal provisions;

XVII. **Compensatory measures:** Alternative mechanisms to inform the data subjects of the privacy notice, through its dissemination through mass media or other broad-based media;

XVIII. **Security measures:** Set of actions, activities, controls or administrative, technical and physical mechanisms that allow the protection of personal data;

XIX. **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 staff awareness and training on personal data protection;

XX. **Physical security measures:** A set of actions and mechanisms to protect the physical environment of personal data and the resources involved in its processing. The following activities should be considered, but are not limited to:

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

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

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

d) Provide equipment containing or storing personal data with effective maintenance to ensure its availability and integrity;

XXI. **Technical security measures:** A set of actions and mechanisms that use hardware and software technology to protect the digital environment of personal data and the resources involved in its processing. The following activities should be considered, but are not limited to:

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

b) Generate a privilege scheme so that the user can carry out the activities required by his/her duties;

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

d) Manage communications, operations and storage media of resources computer scientists in the processing of personal data;

XXII. **Person in Charge:** A natural or legal person, public or private, outside the organization of the person responsible, who alone or jointly with others processes personal data on behalf of and for the account of the person responsible;

XXIII. **National Platform:** National Transparency Platform referred to in article 44 of the General Law on Transparency and Access to Public Information;

XXIV. **Referral:** All communication of personal data carried out exclusively between the controller and the person in charge, within or outside Mexican territory;

XXV. **Responsible:** Obligated subjects referred to in section XXVII of this article who decide on the processing of personal data;

XXVI. **Secretariat:** Anti-Corruption and Good Government Secretariat;

XXVII. Obligated Subjects: Any authority, entity, body and organization of the executive, legislative and judicial branches, autonomous bodies, political parties, trusts and public funds, at the federal, state and municipal level or in the territorial demarcations of Mexico City;

XXVIII. Deletion: Archival removal of personal data in accordance with the applicable legal provisions on archives, which results in the elimination, erasure or destruction of personal data under the security measures previously established by the controller;

XXIX. **Data Subject:** Subject to whom the personal data correspond;

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

XXXI. **Processing:** Any operation or set of operations carried out by manual or automated procedures applied to personal data, related to the obtaining, use, registration, organization, conservation, elaboration, utilization, communication, dissemination, storage, possession, access, handling, exploitation, disclosure, transfer or disposition of personal data, and

XXXII. Transparency Unit: Instance referred to in article 41 of the General Law of Transparency and Access to Public Information.

Article 4. This Law shall apply to any processing of personal data held on physical or electronic media, regardless of the form or method of its creation, type of media, processing, storage, and organization.

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

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

II. Telephone directories in terms of specific regulations;

III. Newspapers, gazettes or official bulletins, in accordance with the corresponding legal provisions;

IV. Social media, and

V. Public records in accordance with the provisions applicable to them.

For the assumptions listed in this article to be considered publicly accessible sources, they must be accessible by any person not impeded by a restrictive rule, or without any requirement other than, where applicable, the payment of a fee, right, or charge. A source will not be considered publicly accessible when the information it contains is or comes from an illicit source.

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

The right to the protection of personal data shall only be limited for reasons of national security, in accordance with the relevant law, public order, public health and safety provisions, or to protect the rights of third parties.

Article 7. As a general rule, sensitive personal data may not be processed unless the data subject has given express consent or, failing that, in the cases established in Article 16 of this Law.

In the processing of personal data of minors, the best interests of the girl must be given priority, child and adolescent, in terms of the applicable legal provisions.

Article 8. The application and interpretation of this Law shall 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 binding resolutions and sentences issued by specialized national and international bodies, always favoring the right to privacy, the protection of personal data and the broadest protection for individuals.

In the case of interpretation, the criteria, determinations, and opinions of national and international organizations regarding the protection of personal data may be taken into account.

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

The laws of the Federal Entities, within the scope of their respective powers, shall determine the provisions applicable to the Guarantor Authorities in the application and interpretation of this Law.

SECOND TITLE

PRINCIPLES AND DUTIES

Chapter I

Of the Principles

Article 10. The person responsible must observe the principles of legality, purpose, loyalty, consent, quality, proportionality, information and responsibility in the processing of personal data.

Article 11. The processing of personal data by the controller must be subject to the powers or powers conferred upon it by applicable regulations.

Article 12. All processing of personal data by the controller must be justified by specific, lawful, explicit, and legitimate purposes, related to the powers conferred upon them by applicable regulations.

The data controller may process personal data for purposes other than those established in the privacy notice, provided that it has the authority granted by applicable law and the data subject has given his or her consent, unless the data subject has been reported missing, in accordance with the terms set forth in this Law and other applicable provisions.

Article 13. The data controller shall not obtain and process personal data through deceptive or fraudulent means, and shall prioritize the protection of the data subject's interests and the reasonable expectation of privacy.

Article 14. When any of the exceptions provided for in Article 16 of this Law are not met, the data controller must obtain the prior consent of the data subject for the processing of personal data, which must be granted in the following manner:

I. Free: Without any error, bad faith, violence or fraud that could affect the manifestation of the will of the holder;

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

III. Informed: That the data subject is aware of the privacy notice prior to the processing of his or her personal data.

When obtaining the consent of minors or those who are under interdiction or declared incapacitated in accordance with applicable legal provisions, the rules of representation provided for in applicable civil legislation shall apply.

Article 15. Consent may be expressed expressly or tacitly. Express consent shall be deemed to be expressed when the will of the data subject is expressed verbally, in writing, by electronic or optical means, by unequivocal signs, or by any other technology.

Consent will be tacit when the privacy notice has been made available to the owner,
This does not express its will to the contrary.

As a general rule, tacit consent will be valid, unless applicable legal provisions require that the will of the data subject be expressly stated.

In the case of sensitive personal data, the data controller must obtain the data subject's express written consent for its processing, through his or her handwritten signature, electronic signature, or any other authentication mechanism established for this purpose, except in the cases provided for in Article 16 of this Law.

Article 16. The data controller shall not be obliged to obtain the data subject's consent for the processing of his or her personal data in the following cases:

- When applicable legislation so provides, such assumptions must be in accordance with the bases, principles and provisions established in this Law, and in no case may they contravene it;
- **II.** When transfers are made between controllers, they 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 the personal data;
- **III.** When there is a well-founded and motivated court order, resolution or mandate from a competent authority;
- **IV.** For the recognition or defense of the rights of the holder before the competent authority;
- **V.** When personal data is required to exercise a right or fulfill obligations arising from a legal relationship between the data subject and the data controller;
- **VI.** When there is an emergency situation that could potentially harm an individual in person or property;
- **VII.** When personal data is necessary to carry out processing for prevention, diagnosis or the provision of healthcare;
- **VIII.** When personal data appear in publicly accessible sources;
- **IX.** When personal data are subject to a prior dissociation procedure, or
- **X.** When the person holding the personal data is a person reported missing under the terms of the legal provisions on the matter.

Article 17. The person responsible must adopt the necessary measures to maintain accurate, complete, correct and updated the personal data in their possession, so that the veracity of the same is not altered.

It is presumed that personal data quality is met when it is provided directly by the data subject and until the data subject states and proves otherwise.

When personal data is no longer necessary for the purposes set forth in the privacy notice and which motivated its processing in accordance with applicable provisions, it must be deleted, after blocking it if necessary, and once the retention period for the data has expired.

The retention periods for personal data shall not exceed those necessary to fulfill the purposes for which they were processed. They shall comply with the applicable provisions in the relevant matter and consider the administrative, accounting, tax, legal, and historical aspects of the personal data.

Article 18. The data controller must establish and document the procedures for the conservation and, where appropriate, blocking and deletion of personal data that it carries out, which include the retention periods for said data, in accordance with the provisions of the previous article of this Law.

In the procedures referred to in the preceding paragraph, the controller must include mechanisms that allow it to comply with the deadlines set for the deletion of personal data, as well as to conduct a periodic review of the need to retain the personal data.

Article 19. The controller shall only process personal data that are adequate, relevant and strictly necessary for the purpose that justifies its processing.

Article 20. The data controller must inform the data subject, through the privacy notice, of the existence and main characteristics of the processing to which their personal data will be subjected, so that they can make informed decisions in this regard.

The privacy notice must be disseminated by the electronic and physical means available to the responsible party, Likewise, it must be made available in its simplified form.

In order for the privacy notice to efficiently fulfill its information function, it must be drafted and structured in a clear and simple manner.

When it is impossible to communicate the privacy notice to the data subject directly or it requires disproportionate efforts, the data controller may implement compensatory mass communication measures in accordance with the criteria issued for this purpose by the Secretariat.

Article 21. The privacy notice must contain, at least, the following information:

I. The name and address of the person responsible;

II. The personal data that will be processed, identifying those that are sensitive;

III. The legal basis that authorizes the controller to carry out the processing;

IV. The purposes of the processing for which the personal data are obtained, distinguishing those that require the consent of the data subject;

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

VI. The address of the Transparency Unit;

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

a) The authorities, powers, entities, bodies and government agencies of the three levels of government and the natural or legal persons to whom the personal data are transferred, and

b) The purposes of these transfers;

VIII. The mechanisms and means available so that the data subject, where applicable, can express his or her refusal to have his or her personal data processed for purposes and transfers of personal data that require the data subject's consent, and

IX. The means through which the controller will communicate changes to the privacy notice to the data subjects.

The mechanisms and means referred to in Section VIII of this article must be available so that the data subject can express his or her refusal to have his or her personal data processed for purposes or transfers that require his or her consent, prior to such processing taking place.

Article 22. The privacy notice in its simplified form must contain the information referred to in sections I, IV, VII and VIII of the previous article and indicate the site where the full privacy notice may be consulted.

The availability of the privacy notice referred to in this article does not exempt the data controller from its obligation to provide mechanisms for the data subject to be aware of the full content of the privacy notice.

Article 23. The controller must implement the mechanisms provided for in Article 24 of this Law to certify compliance with the principles, duties and obligations established herein and be accountable for the processing of personal data in its possession to the owner, the Secretariat or the guarantor authorities, as appropriate, in which case it must observe the Political Constitution of the United Mexican States and the international treaties to which the Mexican State is a party; insofar as this does not conflict with Mexican regulations, it may use national or international standards or best practices for such purposes.

Article 24. Among the mechanisms that the responsible party must adopt to comply with the principle of The responsibilities established in this Law are, at least, the following:

- Allocate authorized resources for this purpose for the implementation of personal data protection programs and policies;
- **II.** Develop personal data protection policies and programs that are mandatory and enforceable within the controller's organization;
- **III.** Implement a training and updating program for staff on obligations and other duties regarding personal data protection;
- **IV.** Periodically review personal data security policies and programs to determine any required modifications;
- **V.** Establish an internal and/or external monitoring and surveillance system, including audits, to verify compliance with personal data protection policies;
- **VI.** Establish procedures to receive and respond to questions and complaints from the owners;
- **VII.** Design, develop and implement 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 in this Law and any other applicable provisions on the matter, and
- **VIII.** Ensure 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 any other applicable laws.

Chapter II
Of Duties

Article 25. Regardless of the type of system in which the personal data are stored or the type of processing carried out, the controller must establish and maintain administrative, physical, and technical security measures to protect personal data against damage, loss, alteration, destruction, or unauthorized use, access, or processing, as well as guarantee its confidentiality, integrity, and availability.

Article 26. The security measures adopted by the person responsible must consider:

- 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 breach for the rights holders;
- **V.** The transfers of personal data that are made;
- **VI.** The number of holders;
- **VII.** Previous breaches in treatment systems, and
- **VIII.** The risk of the potential quantitative or qualitative value that personal data processed could have for a third party not authorized to possess it.

Article 27. In order to establish and maintain security measures for the protection of personal data, the
The responsible party must carry out at least the following interrelated activities:

- Create internal policies for the management and processing of personal data that 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 processing systems;
- **IV.** Conduct a risk analysis of personal data, considering the threats and vulnerabilities existing for personal data and the resources involved in its processing, such as, but not limited to, hardware, software, personnel of the controller, among others;

V. Conduct a gap analysis, comparing existing security measures against those missing in the responsible organization;

VI. Develop a work plan for implementing the missing security measures, as well as measures for daily compliance with personal data management and processing policies;

VII. Monitor and periodically review the security measures implemented, as well as the threats and violations to which personal data are subject, and

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

Article 28. Actions related to security measures for the processing of personal data must be documented and contained in a management system.

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

Article 29. The person responsible must prepare a security document containing, at least, the following:

I. The inventory of personal data and processing systems;

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

III. Risk analysis;

IV. Gap analysis;

V. The work plan;

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

VII. The general training program.

Article 30. The person responsible must update the security document when the following events occur:

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

II. As a result of a continuous improvement process, 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 31. In the event of a security breach, the data controller must analyze the causes of the breach and implement preventive and corrective actions in its work plan to adapt security measures and the processing of personal data, if applicable, to prevent the breach from recurring.

Article 32. In addition to those indicated in the respective laws and applicable regulations, the following shall be considered as security breaches, at any stage of data processing, at least the following:

I. Unauthorized loss or destruction;

II. Theft, loss or unauthorized copying;

III. Unauthorized use, access or processing, or

IV. Unauthorized damage, alteration or modification.

Article 33. The responsible party must keep a log of security breaches, describing the breach, the date it occurred, the reason for it, and the corrective actions implemented immediately and definitively.

Article 34. The responsible party must inform the holder without delay, and as appropriate, the Secretariat and the guarantor Authorities, of any violations that significantly affect property or moral rights, as soon as it is confirmed that the violation occurred and the responsible party has begun to take actions aimed at triggering a process of exhaustive review of the magnitude of the affectation, so that the affected holders can take the corresponding measures to defend their rights.

Article 35. The person responsible must inform the owner of at least the following:

I. The nature of the incident;

II. The personal data compromised;

III. Recommendations on measures that the data subject may adopt to protect his or her interests;

IV. Corrective actions carried out immediately, and

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

Article 36. The controller must establish controls or mechanisms to ensure that all persons involved in any phase of the processing of personal data maintain confidentiality regarding such data, an obligation that will continue to exist even after their relationship with the controller has ended.

The foregoing, without prejudice to the provisions established in the provisions on access to public information.

THIRD TITLE

RIGHTS OF THE HOLDER PERSONS AND THEIR EXERCISE

Chapter I

Rights of Access, Rectification, Cancellation and Opposition

Article 37. At any time, the data subject or their representative may request from the data controller access, rectification, cancellation, or objection to the processing of their personal data, 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 any other rights.

Article 38. The data subject shall have the right to access his or her personal data in the possession of the responsible, as well as knowing the information related to the conditions and generalities of its treatment.

Article 39. The data subject shall have the right to request the data controller to rectify or correct his or her data. personal data, when these are found to be inaccurate, incomplete or not up to date.

Article 40. The data subject shall have the right to request the erasure of his or her personal data from the files, records, files, and systems of the data controller, so that they are no longer in the controller's possession and are no longer processed by the controller.

Article 41. The data subject may object to the processing of his or her personal data or demand that it cease when:

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

II. Your personal data are subject to automated processing, which produces undesired legal effects or significantly affects your interests, rights or freedoms, and is intended

to evaluate, without human intervention, certain personal aspects of the same or to analyze or predict, in particular, its professional performance, economic situation, health status, sexual preferences, reliability or behavior.

Chapter II

On the Exercise of the Rights of Access, Rectification, Cancellation and Opposition

Article 42. The reception and processing of requests for the exercise of ARCO rights made to those responsible shall be subject to the procedure established in this Title and other provisions applicable to the matter.

Article 43. To exercise ARCO rights, it will be necessary to prove the identity of the holder and, where applicable, the identity and personality under which the representative acts.

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

In the exercise of ARCO rights by minors or persons who are under interdiction or incapacitated, in accordance with civil laws, the rules of representation established in the same legislation shall apply.

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

Article 44. The exercise of ARCO rights is free of charge. Charges may only be made to recover the rights. reproduction, certification or shipping costs, in accordance with applicable regulations.

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

When the owner provides the magnetic, electronic medium or the mechanism necessary to reproduce personal data must be provided to the latter free of charge.

The information must be provided free of charge, when it involves the delivery of no more than twenty single sheets. Transparency units may exempt payment for reproduction and shipping depending on the socioeconomic circumstances of the data subject.

The data controller may not establish any service or means for submitting requests to exercise ARCO rights that entail a cost for the data subject.

Article 45. The responsible party must establish simple procedures that allow the exercise of ARCO rights, the response period for which must not exceed twenty days from the day following receipt of the request.

The period referred to in the previous paragraph may be extended once for up to ten days when so required. justify the circumstances, as long as the owner is notified within the response period.

If the exercise of ARCO rights is appropriate, the data controller must do so within a period not to exceed fifteen days from the day after the data subject is notified of the response.

Article 46. The application for the exercise of ARCO rights may not impose any requirements other than the following:

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

II. Documents proving the identity of the holder and, where applicable, the personality and identity of his or her representative;

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

IV. A clear and precise description of the personal data in respect of which you seek to exercise any of the ARCO rights, unless it is the right of access;

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

VI. Any other element or document that facilitates the location of personal data, if applicable.

In the case of a request for access to personal data, the data subject must indicate the method in which they prefer the data to be reproduced. The data controller must respond to the request in the manner requested by the data subject, unless there is a physical or legal impossibility that limits the ability to reproduce the personal data in that manner. In this case, the data controller must offer alternative methods for providing the personal data, providing reasons and justifications for such action.

In the event that the data protection request does not satisfy any of the requirements referred to in this article, and the Secretariat or the Guaranteeing Authorities do not have the elements to correct it, the data subject shall be warned within five days following the submission of the request to exercise ARCO rights, on one occasion only, to correct the omissions within a period of ten days counted from the day following the notification.

If the deadline has elapsed without addressing the prevention, the request to exercise ARCO rights will be considered not submitted.

The prevention will have the effect of interrupting the time that those responsible have to resolve the request to exercise ARCO rights.

In relation to a cancellation request, the owner must indicate the reasons that motivate him/her to request it.
the deletion of your personal data from the files, records or databases of the controller.

In the case of a request to object, the data subject must state the legitimate reasons or the specific situation that led them to request cessation of processing, as well as the harm or damage that continued processing would cause or, where applicable, the specific purposes for which they need to exercise the right to object.

Applications for the exercise of ARCO rights must be submitted to the Transparency Unit of the competent authority, through written documents, forms, electronic media, or any other means established for this purpose by the Secretariat or the Guarantor Authorities, within the scope of their respective powers.

The person responsible must process all requests for the exercise of ARCO rights and deliver the acknowledgment of
corresponding receipt.

The Secretariat and the Guarantor Authorities, according to their area of competence, may establish forms,
systems and other simplified methods to facilitate the exercise of ARCO rights by holders.

The means and procedures enabled by the data controller to respond to requests for the exercise of ARCO rights must be easily accessible and offer the broadest possible coverage, taking into account the profile of the data subjects and the manner in which they maintain daily or regular contact with the data controller.

Article 47. When the data controller is not competent to handle the request for the exercise of ARCO rights, he must inform the data subject of this situation within three days of the submission of the request and, if possible, direct him to the competent data controller.

If the data controller declares that the personal data does not exist in its files, records, systems, or files, this declaration must be included in a resolution from the Transparency Committee confirming the absence of the personal data.

In the event that the responsible party notices that the request for the exercise of ARCO rights corresponds to a
rights other than those provided for in this Law, must redirect the route by informing the holder.

Article 48. When the provisions applicable to certain personal data processing establish a specific process or procedure to request the exercise of ARCO rights, the controller must inform the data subject about the existence of the same, within a period of no more than five days following the presentation of the request for the exercise of ARCO rights, so that the latter may decide whether to exercise their rights through the specific process, or through the procedure that the controller has established.

institutionalized to handle requests for the exercise of ARCO rights in accordance with the provisions established in this Chapter.

Article 49. The only reasons in which the exercise of ARCO rights will not be appropriate are:

I. When the owner or his/her representative is not duly accredited to do so;

II. When the personal data are not in the possession of the controller;

III. When there is a legal impediment;

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

V. When judicial or administrative proceedings are obstructed;

VI. When there is a resolution from a competent authority that restricts access to personal data or does not allow rectification, cancellation or opposition thereof;

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

VIII. When the person responsible is not competent;

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

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

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

XII. When personal data is part of the information that entities subject to the financial regulation and supervision of the obliged subject have provided to the latter, in compliance with requests for such information about their operations, organization, and activities.

In all of the above cases, the responsible party must inform the owner of the reason for their decision within the period of up to twenty days referred to in the first paragraph of Article 45 of this Law, and by the same means in which the request was made, accompanying, where appropriate, any relevant evidence.

Article 50. Against the refusal to process any request for the exercise of ARCO rights or due to the lack of response from the responsible party, the appeal for review referred to in Article 86 of this Law may be filed.

Chapter III

On Data Portability

Article 51. When personal data are processed electronically in a structured and commonly used format, the data subject 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 for further use of the data.

Where the data subject has provided personal data and the processing is based on consent or a contract, they shall have the right to transmit such personal data and any other information they have provided and which is stored in an automated processing system to another system in a commonly used electronic format, without hindrance from the data controller from whom the personal data are obtained.

TITLE FOUR

RELATIONSHIP BETWEEN THE PERSON IN CHARGE AND THE PERSON IN CHARGE

Single Chapter

Person in Charge and Responsible Person

Article 52. The person in charge must carry out the activities of processing personal data without having any decision-making power over the scope and content thereof, and must limit their actions to the terms set by the controller.

Article 53. The relationship between the controller and the person in charge must be formalized by means of a contract or any other legal instrument decided by the controller, in accordance with the applicable legal provisions, and which allows for the accreditation of its existence, scope and content.

The contract or legal instrument decided by the responsible party must provide for 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 controller;

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

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

IV. Inform the controller when a breach occurs of the personal data that he or she processes on his or her instructions;

V. Maintain confidentiality regarding the personal data processed;

VI. Delete or return the personal data being processed once the legal relationship with the controller has been fulfilled, provided that there is no legal provision requiring the retention of the personal data, and

VII. Refrain from transferring personal data except when the data controller so determines, or the communication results from subcontracting, or by express mandate of the competent authority.

Agreements between the controller and the person in charge related to the processing of personal data must not contravene this Law and other applicable provisions, as well as the provisions of the corresponding privacy notice.

Article 54. When the person in charge fails to comply with the instructions of the controller and decides on his or her own decision regarding the processing of personal data, he or she shall assume the role of controller and the corresponding legal consequences in accordance with the legislation applicable to the subject matter.

Article 55. The person in charge may, in turn, subcontract services that involve the processing of personal data on behalf of the controller, provided that the latter has expressly authorized it. In this case, the subcontracted person will assume the role of person in charge under the terms of this Law and other provisions applicable to the matter.

When the contract or legal instrument formalizing the relationship between the controller and the person in charge provides that the latter may, in turn, subcontract services, the authorization referred to in the previous paragraph shall be deemed to have been granted pursuant to the provisions of these provisions.

Article 56. Once the express authorization of the responsible party has been obtained, the person in charge must formalize the relationship acquired with the subcontracted person through a contract or any other legal instrument that he decides, in accordance with the regulations applicable to him, and that allows to prove the existence, scope and content of the provision of the service in terms of the provisions of this Chapter.

Article 57. The data controller may contract or join cloud computing services, applications, and infrastructure, and other matters that involve the processing of personal data, provided that the external provider guarantees personal data protection policies equivalent to the principles and duties established in this Law and other applicable provisions on the matter.

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

Article 58. For the processing of personal data in cloud computing services, applications and infrastructure and other matters, in which the controller adheres to them through general contracting conditions or clauses, the data subject may only use those services in which the provider:

I. Comply with at least the following:

a) Have and apply personal data protection policies that are in line with the principles and duties that correspond to the provisions of this Law and other applicable legal provisions;

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 you to assume the ownership or property of the information on which the service is provided, and

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

II. Have mechanisms in place, at least, to:

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

b) Allow the controller to limit the type of processing of personal data about which it is processed. provides the service;

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

d) Ensure the deletion of personal data once the service provided to the controller has concluded and the controller has been able to recover them, and

e) Prevent access to personal data by persons who do not have access privileges, or, in the case of a well-founded and motivated request from a competent authority, inform the controller of this fact.

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

TITLE FIVE

COMMUNICATIONS OF PERSONAL DATA

Single Chapter

On Transfers and Remissions of Personal Data

Article 59. Any transfer of personal data, whether national or international, is subject to the consent of the owner, except for the exceptions provided for in articles 16, 60 and 64 of this Law.

Article 60. All transfers must be formalized by the signing of contractual clauses, collaboration agreements, or any other legal instrument, in accordance with the regulations applicable to the data controller, which allows for the demonstration of 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 carried out between responsible parties 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 made at the request of a foreign authority or competent international organization in its capacity as recipient, provided that the powers between the transferring controller and the recipient are homologous or the purposes that motivate the transfer are analogous or compatible with those that gave rise to the processing by the transferring controller.

Article 61. When the transfer is national, the recipient of the personal data must process the personal data, committing to guarantee its confidentiality and will only use it for the purposes for which it was transferred, in accordance with the provisions of the privacy notice that will be communicated to him by the person responsible. transferor.

Article 62. The data controller may only transfer or forward personal data outside the national territory when the third party recipient or the person in charge is obliged to protect the personal data in accordance with the principles and duties established by this Law and the provisions applicable to the matter.

Article 63. In any transfer of personal data, the controller must inform the recipient of the data personal the privacy notice according to which the personal data of the owner are processed.

Article 64. The controller may transfer personal data without requiring the consent of the data subject in the following cases:

I. When the transfer is provided for in this Law or other laws, conventions or international treaties to which the Mexican State is a party;

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

V. When the transfer is necessary for medical prevention or diagnosis, the provision of healthcare, medical treatment or the management of healthcare services, provided that such purposes are accredited;

VI. When the transfer is necessary for the maintenance or fulfillment of a legal relationship between the controller and the owner;

VII. When the transfer is necessary by virtue of a contract entered into or to be entered into in the interest of the data subject, by the data controller and a third party;

VIII. When it concerns cases in which the controller is not obliged to obtain the consent of the data subject for the processing and transfer of his or her personal data, in accordance with the provisions of Article 16 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 from complying with the applicable obligations provided for in this Chapter.

Article 65. National and international transfers of personal data between the controller and the person in charge do not require the data subject to be informed or to have his or her consent.

TITLE SIX

PREVENTIVE ACTIONS IN PERSONAL DATA PROTECTION

Chapter I

Best Practices

Article 66. In order to comply with the obligations set forth in this Law, the responsible party may develop or adopt, individually or in agreement with other responsible parties, managers or organizations, best practice schemes that have the following objectives:

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 holders;

IV. Facilitate transfers of personal data;

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

VI. Demonstrate to the Secretariat or the guarantor authorities compliance with applicable regulations regarding the protection of personal data.

Article 67. Any scheme of best practices that seeks validation or recognition by the The Secretariat or the Guarantor Authorities shall:

I. Comply with the criteria and parameters issued for this purpose by the Secretariat or the corresponding Guarantor Authority according to its area of competence, and

II. To be notified to the Secretariat or the Guarantee Authorities in accordance with the procedure established in the parameters indicated in the previous section, so that they may be evaluated and, where appropriate, validated or recognized and registered in the registry referred to in the last paragraph of this article.

The Secretariat or the Guarantor Authorities, depending on their area of expertise, must issue the operating rules for the registries in which those validated or recognized best practice schemes will be registered.
The Guarantor Authorities may register the best practice schemes they have recognized or validated in the registry administered by the Secretariat, in accordance with the rules established by the latter.

Article 68. When the controller intends to implement or modify public policies, computer systems or platforms, electronic applications or any other technology that, in its judgment and in accordance with this Law, involves the intensive or significant processing of personal data, it must conduct an impact assessment on the protection of personal data and submit it to the Secretariat or the Guarantor Authorities, according to their area of competence, which may issue non-binding recommendations specialized in the area of personal data protection.

The content of the personal data protection impact assessment shall be determined by the Secretariat or the Guaranteeing Authority, within its scope of competence.

Article 69. For the purposes of this Law, it will be considered that there is an intensive treatment or relevant 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 are intended to be made.

Article 70. The Secretariat or the Guaranteeing Authority, within its scope of competence, may issue additional criteria based on objective parameters that determine that there is intensive or relevant processing 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 light of its social or economic impact, or the public interest pursued.

Article 71. Obligated subjects that carry out an impact assessment on the protection of personal data must submit it to the Secretariat or the Guarantor Authorities, according to their area of competence, thirty days prior to the date on which they intend to put into operation or modify public policies, computer systems or platforms, electronic applications or any other technology, so that they may issue the corresponding non-binding recommendations.

Article 72. The Secretariat or the Guarantor Authorities, depending on their area of competence, must issue, where appropriate, non-binding recommendations on the personal data protection impact assessment submitted by the controller.

The deadline for issuing the recommendations referred to in the previous paragraph will be within thirty days from the day following the submission of the personal data protection impact assessment.

Article 73. When, in the opinion of the obligated subject, the effects intended to be achieved with the possible implementation or modification of public policies, computer systems or platforms, electronic applications or any other technology that involves the intensive or significant processing of personal data may be compromised, or when it involves emergency or urgent situations, it will not be necessary to carry out an impact assessment on the protection of personal data.

Chapter II

From the Databases Held by Security, Procurement and Administration of Justice Instances

Article 74. The obtaining and processing of personal data, in terms of the provisions of this Law, by the competent obligated subjects in instances of security, prosecution and administration of justice, is limited to those cases and categories of data that are necessary and proportional for the exercise of the

functions related to national security, public safety, or for the prevention or prosecution of crimes.
They must be stored in the databases established for this purpose.

Authorities that access and store personal data collected by individuals in compliance with the corresponding legal provisions must comply with the provisions set forth in this Chapter.

Article 75. 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, law enforcement and administration of justice bodies, the principles established in Title Two of this Law must be complied with.

Private communications are inviolable. Only the federal judicial authority, at the request of the federal authority authorized by law or the head of the Public Prosecutor's Office of the corresponding federal entity, may authorize the intervention of any private communication.

Article 76. 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 the protection of personal data against damage, loss, alteration, destruction or use, access or processing.
unauthorized.

TITLE SEVEN

PERSONAL DATA PROTECTION RESPONSIBLE PARTIES IN THE POSSESSION OF SUBJECTS OBLIGED

Chapter I

Transparency Committee

Article 77. Each responsible party shall have a Transparency Committee, which shall be composed and operate in accordance with the provisions of the General Law on Transparency and Access to Public Information and other applicable legal provisions.

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

Article 78. For the purposes of this Law and without prejudice to other powers conferred upon it in the regulations applicable to it, the Transparency Committee will have the following functions:

- Coordinate, supervise and carry out the necessary actions to guarantee the right to the protection of personal data in the organization of the controller, in accordance with the provisions of this document.
Law and other applicable provisions on the matter;
- **II.** Establish, where appropriate, internal procedures to ensure the greatest efficiency in the management of requests for the exercise of ARCO rights;
- **III.** Confirm, modify or revoke decisions declaring the nonexistence of personal data, or denying the exercise of any of the ARCO rights for any reason;
- **IV.** Establish and supervise the application of specific criteria that are necessary for better compliance with this Law and other applicable provisions on the matter;
- **V.** Supervise, in coordination with the competent areas or administrative units, compliance with the measures, controls and actions provided for in the security document;
- **VI.** Follow up and comply with the resolutions issued by the Secretariat or the Guarantor Authorities, as appropriate;
- **VII.** Establish training and updating programs for public servants in matters of personal data protection, and
- **VIII.** To notify the internal supervisory body or equivalent body in cases where it becomes aware, in the exercise of its powers, of a suspected irregularity regarding certain personal data processing, particularly in cases involving a declaration of non-existence made by those responsible.

Chapter II

From the Transparency Unit

Article 79. Each responsible party shall have a Transparency Unit that shall be integrated and operate in accordance with the provisions of the General Law on Transparency and Access to Public Information, which shall also have the following functions:

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

II. Manage requests for the exercise of ARCO rights;

III. Establish mechanisms to ensure that personal data is only delivered to the data subject or his or her duly accredited representative;

IV. Inform the data subject or his/her representative of the amount of costs to be covered for the reproduction and transmission of personal data, based on the provisions of the applicable legal provisions;

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

VI. Apply quality assessment instruments to the management of requests for the exercise of ARCO rights, and

VII. Advise the areas assigned to the controller on matters of personal data protection.

Data controllers who, in the exercise of their substantive functions, carry out significant or intensive processing of personal data may appoint a personal data protection officer specialized in the subject matter. The officer will carry out the duties mentioned in this article and will be part of the Transparency Unit.

Obligated entities will promote agreements with specialized public institutions that could assist them in receiving, processing, and delivering responses to information requests more efficiently, in the indigenous language, Braille, or any other accessible format.

Article 80. The person responsible shall ensure that persons with any type of disability or care groups priority, may exercise, under equal circumstances, their right to the protection of personal data.

TITLE EIGHT

Guarantor Authorities

Chapter I

From the Secretariat

Article 81. The Secretariat shall have the following powers:

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

II. Interpret this Law in the administrative sphere;

III. To hear and resolve appeals for review filed by the holders, in accordance with the provisions of this Law and other applicable provisions on the matter;

IV. To hear and resolve, ex officio or at the reasoned request of the guarantor authorities, the appeals for review that merit it due to their interest and significance, in terms of the provisions of this document. Law and other provisions that are applicable in the matter;

V. Know, substantiate and resolve verification procedures;

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

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

VIII. Coordinate with the competent authorities so that requests for the exercise of rights ARCO and the appeals for review that are submitted in an indigenous language, shall be addressed in the same language;

IX. Guarantee, within the scope of their respective competence, accessibility conditions so that data subjects belonging to priority attention groups can exercise, under equal circumstances, their right to the protection of personal data;

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

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

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

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

XIV. Manage the registry of best practice schemes referred to in this Law and issue their operating rules;

XV. Issue, where appropriate, non-binding recommendations corresponding to the personal data protection impact assessment submitted to it;

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

XVII. Carry out the corresponding assessments of the best practice schemes that are notified to them, in order to decide on the appropriateness of their recognition or validation and registration in the registry of best practice schemes, as well as promote their adoption;

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

XIX. Enter into agreements with data controllers to develop programs aimed at standardizing personal data processing in specific sectors, enhancing personal data protection, and making any improvements to relevant practices;

XX. Define and develop the certification system for personal data protection, in accordance with the parameters set forth in this Law;

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

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

XXIII. Promote training and updating in personal data protection among data controllers;

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

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

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

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

XXVIII. Promote and encourage the exercise and protection of the right to the protection of personal data through the implementation and administration of the National Platform;

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

XXX. Design, monitor and, where appropriate, operate the system of good practices in the area of personal data protection, as well as the certification system in this area, through general provisions issued for such purposes;

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

XXXII. Any other powers conferred by this Law and other applicable regulations.

Chapter II

From the Guarantor Authorities

Article 82. The provisions of the General Law on Transparency and Access to Public Information and other applicable legal provisions shall apply to the integration, appointment procedure and operation of the Guarantor Authorities.

Article 83. For the purposes of this Law and without prejudice to other powers conferred upon them in accordance with the legal provisions applicable to them, the Guarantor Authorities shall have the following powers:

I. To hear, substantiate and resolve, within the scope of their respective powers, appeals for review filed by the holders, in accordance with the provisions of this Law and other applicable legal provisions;

II. Submit a reasoned petition to the Secretariat to hear appeals for review that merit it due to their interest and significance, in accordance with the provisions of this Law and other applicable legal provisions;

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

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

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

VI. Guarantee, within the scope of their respective powers, accessibility conditions so that data subjects belonging to priority care groups can exercise, under equal circumstances, their right to the protection of personal data;

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

VIII. To inform the competent authorities of the probable liability arising from non-compliance with the obligations provided for in this Law and in other legal provisions applicable in this matter;

IX. Sign collaboration agreements with the Secretariat to achieve the objectives set forth in this Law and other applicable legal provisions;

X. Monitor, within the scope of their respective powers, compliance with this Law and other applicable legal provisions;

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

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

XIII. Promote training and updating in personal data protection among data controllers;

XIV. Request the cooperation of the Secretariat in the terms of article 81, section XXVII of this document Law, and

XV. Issue, where appropriate, non-binding recommendations corresponding to the personal data protection impact assessment submitted to it.

Chapter III

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

Article 84. Those responsible shall collaborate with the Secretariat and the Guarantor Authorities, as appropriate, to continuously train and update all public servants assigned to them in matters of personal data protection, through the provision of courses, seminars, workshops, and any other form of teaching and training deemed relevant.

Article 85. The Secretariat and the Guarantor Authorities, within the scope of their respective powers, shall:

I. Promote the inclusion of content on the right to personal data protection, as well as a culture of its exercise and respect, in the programs and curricula, books, and materials used in educational institutions at all levels and modalities in the State;

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

III. Promote the creation of spaces for social and citizen participation that encourage the exchange of ideas between society, citizen representative bodies, and decision-makers.

TITLE NINE

OF THE CHALLENGE PROCEDURE

Chapter I

From the Review Appeal

Article 86. The holder or his/her representative may file an appeal for review before the Secretariat or the Guarantor Authorities, as appropriate, or before the Transparency Unit that has heard the request for the exercise of ARCO rights within a period that may not exceed fifteen days from the notification of the response, through the following means:

I. In writing at the address of the Secretariat or the Guarantor Authorities, as appropriate, or at the authorized offices established for this purpose;

II. By registered mail with return receipt requested;

III. By formats issued for this purpose by the Secretariat or the guarantor Authorities, as appropriate;

IV. By electronic means authorized for such purpose, or

V. Any other means established for this purpose by the Secretariat or the Guarantor Authorities, as appropriate.

It will be presumed that the owner accepts that notifications be made to him/her through the same channel as submitted his/her written document, unless he/she proves that he/she has indicated a different one to receive notifications.

Article 87. The holder may prove his or her 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 Secretariat or the Guarantor Authorities, as appropriate, through an agreement published in the Official Gazette of the Federation or in the official gazettes of the Federal Entities.

The use of an advanced electronic signature or any electronic instrument that replaces it will exempt you from submitting a copy of your identification document.

Article 88. When the owner acts through a representative, the latter 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 subscribers' identifications, or public instrument, or declaration in personal appearance of the holder and the representative before the Secretariat or the Guarantor Authorities, and

II. If it is a legal entity, by public instrument.

Article 89. The filing of the appeal for review related to personal data of deceased persons, It may be carried out by a person who proves to have a legal or legitimate interest.

Article 90. In the substantiation of the appeals for review, the notifications issued by the Secretariat and the Guarantor authorities, as appropriate, will take effect on the same day they are carried out.

Notifications may be made:

I. Personally in the following cases:

a) It is the first notification;

b) It is a request for an act from the party that must comply with it;

c) It is a request for reports or documents;

d) It is 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 Secretariat or the Guarantor Authorities, as appropriate, by agreement published in the Official Gazette of the Federation or official newspapers or gazettes of the Federative Entities, when it concerns requirements, summons, requests for reports or documents and resolutions that may be challenged;

III. By ordinary postal mail or by ordinary email when it concerns acts other than those indicated in the previous sections, or

IV. By court, when the person to be notified cannot be reached at their address, or when their address or that of their representative is unknown.

Article 91. The calculation of the periods indicated in this Title shall begin to run from the day following the date on which the corresponding notification took effect.

Once the deadlines set for the parties have expired, any rights that should have been exercised within them shall be deemed lost, without the need for a notice of default by the Secretariat.

Article 92. The owner, the person in charge or any authority must respond to the requirements of information within the timeframes and terms that the Secretariat and the Guarantor Authorities, as appropriate, establish.

Article 93. When the owner, the person responsible or any authority refuses to attend to or comply with the requirements, requests for information and documentation, summons, subpoenas or proceedings notified by the Secretariat and the Guarantor Authorities, as appropriate, or to facilitate the performance of the proceedings that have been ordered, or hinders their actions, as appropriate, they will be deemed to have lost their right to assert it at any other time during the procedure and the Secretariat and the Guarantor Authorities, as appropriate, will consider the facts of the procedure to be true and will resolve with the elements available to them.

Article 94. In the substantiation of appeals for review, the parties may offer the following evidence:

I. The public documentary;

II. The private documentary;

III. The inspection;

IV. The expert opinion;

V. The testimonial;

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

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

VIII. The legal and human presumption.

The Secretariat and the Guarantor Authorities, as appropriate, may obtain any evidence they deem necessary, with no limitations other than those established in the applicable legislation.

Article 95. Once the period provided for in Article 45 of this Law for responding to a request for the exercise of ARCO rights has elapsed without the request having been issued, the holder or, where applicable, his or her representative may file an appeal for review within fifteen days following the expiration of the period for responding.

Article 96. The appeal for review shall be admissible in the following cases:

I. Personal data is classified as confidential without meeting the characteristics indicated in the applicable legal provisions;

II. Declare the nonexistence of the personal data;

III. The person responsible is declared incompetent;

IV. Incomplete personal data is provided;

V. Personal data is provided that does not correspond to what was requested;

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

VII. Failure to respond to a request for the exercise of ARCO rights within the time limits established in this Law and other applicable provisions on the matter;

VIII. Personal data is delivered or made available in a manner or format other than that requested, or in an incomprehensible format;

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

X. The exercise of ARCO rights is hindered, despite having been notified of their origin;

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

XII. In other cases provided for by applicable legislation.

Article 97. The only requirements that must be met in the written appeal for review will be the following:

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

II. The name of the person appealing or his/her representative and, where applicable, the third party concerned, as well as the address or means indicated for receiving notifications;

III. The date on which the response was notified to the owner, or, in the absence of a response, the date on which the request for the exercise of ARCO rights was submitted;

IV. The act being appealed and the points being requested, as well as the reasons or motives for disagreement;

V. If applicable, a copy of the contested response and the corresponding notification, and

VI. Documents proving the identity of the holder and, where applicable, the personality and identity of his or her representative.

The appeal for review may be accompanied by evidence and other elements that the holder considers appropriate to submit to the judgment of the Secretariat or, where appropriate, the Guarantor Authorities.

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

Article 98. Once the appeal for review has been admitted, the Secretariat or, where appropriate, the Guarantor Authorities They may seek conciliation between the owner and the person responsible.

If an agreement is reached, it will be recorded in writing and will be binding. The appeal for review will be dismissed, and the Secretariat or, where appropriate, the Guarantor Authorities must verify compliance with the respective agreement.

Article 99. Once the appeal for review has been admitted and without prejudice to the provisions of Article 59 of this Law, the Secretariat or the Guaranteeing Authority shall promote conciliation between the parties, in accordance with the following procedure:

yo. The parties shall be required to express, by any means, their willingness to reach an agreement within a period of no more than seven days from the date of notification of said agreement. This agreement shall contain a summary of the appeal and the response of the responsible party, if any, indicating the common elements and points of controversy.

The conciliation may be held in person, remotely, electronically, or by any other means determined, as appropriate. In any case, the conciliation must be documented by any means that allows its existence to be proven.

The conciliation stage is exempt when the holder is a minor and any of the rights contemplated in the General Law on the Rights of Girls, Boys and Children has been violated.
Adolescents and other applicable legal provisions, unless they have duly accredited legal representation;

II. Once the expression of the will to reconcile has been received from both parties, the Secretariat or the Guaranteeing Authority, as appropriate, will indicate the place or means, day and time for the holding of a conciliation hearing in which an attempt will be made to reconcile the interests between the owner and the responsible party. This hearing must be held within ten days of receiving the aforementioned expression.

The Secretariat or the Guarantor Authority, in its capacity as conciliator, may, at any time during the conciliation stage, require the parties to submit, within a maximum period of five days, any evidence it deems necessary for the conciliation.

The conciliator may suspend the hearing for one occasion when she deems appropriate, or at the request of both parties. If the hearing is suspended, the conciliator will set a date and time for its resumption within the following five days.

Minutes shall be kept of every conciliation hearing, recording the outcome. If the responsible party or the person in charge, or their respective representatives, do not sign the minutes, this will not affect their validity, and such refusal must be recorded.

III. If either party fails to attend the conciliation hearing and justifies their absence within three days, they will be summoned to a second conciliation hearing within five days. In case

If either party does not attend the latter, the appeal for review will continue. If either party fails to attend the conciliation hearing without justification, the procedure will continue;

IV. If there is no agreement at the conciliation hearing, the appeal for review will continue;

V. If an agreement is reached, it will be recorded in writing and will be binding. The appeal for review will be dismissed, and the Secretariat or, where appropriate, the Guarantor Authorities must verify compliance with the respective agreement.

VI. Compliance with the agreement will conclude the review appeal; otherwise, the Secretariat or the Guaranteeing Authority will resume the procedure.

Article 100. The Secretariat or the Guarantor Authorities shall resolve the appeal for review within a period of no more than may exceed forty days, which may be extended up to twenty days only once.

The period referred to in the preceding paragraph shall be suspended during the period of compliance with the conciliation agreement.

Article 101. During the procedure referred to in this Chapter, the Secretariat or the Guarantor Authorities, as appropriate, must apply the substitution of the complaint in favor of the person holding the claim, provided that it does not alter the original content of the appeal for review, nor modify the facts or requests set forth therein, as well as guarantee that the parties can present the arguments and evidence that support and motivate their claims.

Article 102. If in the written submission of the appeal for review the holder does not comply with any of the requirements provided for in article 97 of this Law and the Secretariat and the Guarantor Authorities, as appropriate, do not have the elements to correct them, the latter must request from the holder, on one occasion only, the information that corrects the omissions within a period that may not exceed five days, counted from the day following the submission of the written submission.

The holder will have a period not to exceed five days, starting from the day following notification of the warning, to correct the omissions, with the warning that, if the requirement is not complied with, the appeal for review will be dismissed.

The prevention will have the effect of interrupting the period of time that the Secretariat and the Guarantor Authorities have to resolve the appeal, so it will begin to be computed from the day after its resolution.

Article 103. The resolutions of the Secretariat or, where appropriate, of the Guarantor Authorities 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 controller, or

IV. Order the delivery of personal data, in case of omission by the controller.

The resolutions shall establish, where applicable, the deadlines and timeframes for compliance and the procedures to ensure their execution. Those responsible must inform the Secretariat or, where appropriate, the Guarantee Authorities of compliance with their resolutions.

In the absence of a resolution by the Secretariat, or where appropriate, by the guarantor Authorities, it will be understood the response of the person in charge has been confirmed.

When the Secretariat or, where appropriate, the Guarantor Authorities determine during the substantiation of the review appeal that probable liability may have been incurred for failure to comply with the obligations provided for in this Law and other applicable legal provisions on the matter, they must inform the internal control body or the competent authority so that it may initiate, where appropriate, the respective liability procedure.

Article 104. The appeal for review may be dismissed as inadmissible when:

I. It is untimely because the period established in article 86 of this Law has elapsed;

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

III. The Secretariat or, where appropriate, the Guarantor Authorities have previously made a final decision on the subject matter thereof;

IV. None of the grounds for appeal for review provided for in Article 96 of this Law are updated;

V. Any appeal or means of defense filed by the appellant or, where appropriate, by the interested third party, against the contested act before the competent courts is being processed.
Secretariat or the Guarantor Authorities, as appropriate;

VI. The appellant modifies or expands his/her request in the appeal for review, solely with respect to the new content, or

VII. The appellant does not prove legal interest.

Dismissal does not imply the preclusion of the right of the holder to file a complaint with the Secretariat or the Guarantor Authorities, as appropriate, a new appeal for review.

Article 105. The appeal for review may only be dismissed when:

I. The appellant expressly withdraws;

II. The appellant dies;

III. Once admitted, any cause of inadmissibility is updated under the terms of this Law;

IV. The person responsible modifies or revokes his response in such a way that it becomes without substance, or

V. I ran out of matter.

Article 106. The Secretariat and the Guarantor Authorities must notify the parties and publish the resolutions, in public version, no later than the third day following its issuance.

Article 107. The resolutions of the Secretariat and the Guarantor Authorities shall be binding, final and unassailable to those responsible.

The holders may challenge these resolutions before the judges and courts specialized in personal data matters established by the Federal Judicial Branch through the amparo trial.

Chapter II

From the Appeal for Review in Matters of National Security

Article 108. The person in charge of the Legal Counsel of the Federal Executive may file a review appeal on matters of national security directly before the Supreme Court of Justice of the Nation, when he or she considers that the resolutions issued by the Secretariat endanger national security.

The appeal must be filed within seven days of the date on which the guarantor authority notifies the obligated party of the decision. The Supreme Court of Justice of the Nation shall immediately, if appropriate, suspend the execution of the decision, and within five days of the filing of the appeal, it shall decide whether it is admissible or inadmissible.

Article 109. In the appeal, the head of the Legal Counsel of the Federal Executive Branch must state the resolution being challenged, the grounds and reasons why he or she believes national security is endangered, as well as the necessary evidence.

Article 110. Any reserved or confidential information requested by the Supreme Court of Justice of the Nation because it is essential to resolve the matter must be kept confidential and will not be available in the file, except for the exceptions provided for in Article 119 of the General Law on Transparency and Access to Public Information.

At all times, Ministers must have access to classified information to determine its nature, as required. Access will be granted in accordance with the legal provisions applicable to the safeguarding of information by obliged entities.

Article 111. The Supreme Court of Justice of the Nation shall resolve with full jurisdiction and, in no case, the forwarding will proceed.

Article 112. If the Supreme Court of Justice of the Nation confirms the meaning of the appealed resolution, the subject obliged party must comply with the terms of the provisions of this Law.

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

Chapter III

Of the Criteria of Interpretation

Article 113. Once the resolutions issued in connection with the appeals submitted to its jurisdiction have become final, the Secretariat may issue the interpretation criteria it deems pertinent and which derive from the resolutions therein.

The Secretariat may issue guiding criteria for the Guarantor Authorities, which will be established by reiteration when resolving three consecutive similar cases in the same sense, arising from resolutions that have become final.

Article 114. The criteria shall consist of a heading, a text and the precedent or precedents that, where applicable, have originated their emission.

Every criterion issued by the Secretariat must contain a control key for proper identification.

TITLE TEN

FACULTY OF VERIFICATION

Single Chapter

From the Verification Procedure

Article 115. The Secretariat and the Guarantor Authorities, within the scope of their respective powers, shall have the power to monitor and verify compliance with the provisions contained in this Law and other provisions derived from it.

In the exercise of their oversight and verification functions, the Secretariat's staff or, where applicable, the Guarantor Authorities shall be required to maintain confidentiality regarding the information to which they have access by virtue of the corresponding verification.

The person responsible may not deny access to the documentation requested for verification or to its personal databases, nor may it invoke the confidentiality or reserve of the information.

Article 116. Verification may be initiated:

I. Ex officio when the Secretariat or the guarantor Authorities have evidence that gives rise to a well-founded and motivated presumption of the existence of violations of the corresponding laws, or

II. By filing a complaint by the owner when they consider that they have been affected by acts of the controller that may be contrary to the provisions of this Law and other applicable legal provisions or, where appropriate, by any person when they have knowledge of alleged breaches of the obligations provided for in this Law and other applicable provisions on the matter.

The right to file a complaint expires one year after the day following the occurrence of the acts or omissions that are the subject of the complaint. When the acts or omissions are successive, the period begins to run from the business day following the last act.

Verification will not be carried out and will not be admitted in the cases where the appeal for review provided for in this Law is admissible.

Prior to the respective verification, the Secretariat or the guarantor Authorities may carry out investigations prior, in order to have elements to establish and motivate the respective start agreement.

Article 117. For the filing of a complaint, no greater requirements may be requested than those that are The following are described below:

I. The name of the person making the complaint or, where applicable, his or her representative;

II. The address or means of receiving notifications from the person making the complaint;

III. The statement of facts on which the complaint is based and the elements available to prove your claim;

IV. The person reported responsible and his address or, where appropriate, the data for his identification and/or location, and

V. The signature of the reporting person or, where applicable, their representative. If they cannot sign, a 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 Secretariat or the guarantor Authorities, as appropriate.

Once the complaint has been received, the Secretariat and the Guarantor Authorities, as appropriate, must accuse receipt thereof. The corresponding agreement will be notified to the reporting person.

Article 118. Verification shall begin with a written order that establishes and justifies the appropriateness of the action by the Secretariat or the guarantor Authorities, which aims to request from the responsible party the necessary documentation and information related to the alleged violation and/or to carry out visits to the offices or facilities of the responsible party or, where appropriate, to the place where the respective personal databases are located.

For verification purposes in national security and public security instances, the resolution shall require a reinforced rationale and motivation for the cause of the procedure, and the information shall be secured for the exclusive use of the authority and for the purposes established in Article 119 of this Law.

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

The Secretariat or the guarantor authorities may order precautionary measures if, based on the verification, they find imminent or irreparable harm to the protection of personal data, provided that they do not impede the performance of the functions or the security of the databases of the obligated subjects.

These measures may only have a corrective purpose and will be temporary until then the obligated subjects carry out the recommendations made by the Secretariat or the Guarantor Authorities as appropriate.

Article 119. The verification procedure shall conclude with the resolution issued by the Secretariat or the guarantor Authorities, which shall establish the measures to be adopted by the responsible party within the period determined by the Secretariat.

Article 120. Those responsible may voluntarily submit to audits by the Secretariat or the guarantor authorities, as appropriate, for the purpose of verifying the adaptation, adequacy and effectiveness of the controls, measures and mechanisms implemented for compliance with this Law and other applicable legal provisions.

The audit report must assess the adequacy of the measures and controls implemented by the responsible party, identify any deficiencies, and propose additional corrective actions or recommendations, as appropriate.

TITLE ELEVENTH

ENFORCEMENT MEASURES AND RESPONSIBILITIES

Chapter I

Of the Coercive Measures

Article 121. In order to comply with the resolutions issued by the Secretariat or the guarantor Authorities, as appropriate, the provisions of Chapter V of Title Eight of the General Law on Transparency and Access to Public Information must be observed.

Article 122. The Secretariat or the guarantor Authorities may impose the following enforcement measures for ensure compliance with its decisions:

I. Public reprimand, or

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

Non-compliance by obliged subjects will be disseminated on the transparency obligations portals of the Secretariat and the guarantor authorities and considered in the evaluations they carry out.

If failure to comply with the decisions of the Secretariat or the guarantor authorities implies the alleged commission of a crime or one of the acts described in Article 132 of this Law, the facts must be reported to the competent authority. Financial coercion measures may not be covered by public funds.

Article 123. If, despite the execution of the enforcement measures provided for in the previous article, the resolution is not complied with, the hierarchical superior shall be required to comply so that, within five days following notification of the resolution, he or she shall compel the superior to comply without delay.

Once the deadline has elapsed and compliance has not been met, the competent authority in matters of administrative responsibilities.

Article 124. The enforcement measures referred to in this Chapter must be applied by the Secretariat and the Guarantor Authorities, either on their own or with the support of the competent authority.

Article 125. The fines set by the Secretariat and the Guarantor Authorities shall be enforced by the Tax Administration Service or the Finance Secretariats of the Federal Entities, as appropriate, through the procedures established in the applicable legal provisions.

Article 126. In order to qualify the enforcement measures established in this Chapter, the Secretariat and the guarantor Authorities must consider:

I. The seriousness of the fault of the responsible party, determined by elements such as the damage caused, the indications of intentionality, the duration of the non-compliance with the determinations of the Secretariat or the guarantor Authorities, and the impact on the exercise of their powers;

II. The economic condition of the offender, and

III. Recidivism.

The Secretariat or the Guarantor Authorities shall establish, through general guidelines, the powers of the areas responsible for assessing the seriousness of non-compliance with their determinations and for the notification and execution of enforcement measures that they apply and implement, in accordance with the elements developed in this Chapter.

Article 127. In case of repeat offense, the Secretariat or the Guarantor Authorities may impose a fine. equivalent to up to double.

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

Article 128. Enforcement measures must be applied and implemented within a maximum period of fifteen days, counted from the moment the offender is notified.

Article 129. Public reprimand will be imposed by the Secretariat or the guarantor Authorities and will be executed by the immediate superior of the offender.

Article 130. The Secretariat or the Guarantor Authorities may require the offender to provide the information necessary to determine his/her economic condition, being warned that, in the event of not providing the same, the fines will be quantified based on the elements available, understood as those that are

found in public records, those contained in information media or their own Internet pages and, in general, any that demonstrates their status, with the Secretariat or the Guarantor Authorities being empowered to request any documentation deemed essential for such purpose from the competent authorities.

Article 131. The imposition of enforcement measures may be appealed before the judges and courts specializing in personal data matters established by the Judicial Branch of the Federation or, where appropriate, before the corresponding Judicial Branch in the Federal Entities.

Chapter II

Of the Sanctions

Article 132. The following shall be grounds for sanctions for failure to comply with the obligations established in the matter of the present Law, the following:

I. Acting with negligence, fraud or bad faith during the processing of requests for the exercise of ARCO rights;

II. Failure to comply with the deadlines for responding to requests for the exercise of ARCO rights or to enforce the right in question, as provided for in this Law;

III. Use, remove, disclose, hide, alter, mutilate, destroy or render useless, in whole or in part and in an improper manner, personal data that is in your custody or to which you have access or knowledge due to your employment, position or commission;

IV. Intentionally processing personal data in violation of the principles and duties established in this Law;

V. Failure to have a privacy notice, or omitting from it any of the elements referred to in Article 21 of this Law, as the case may be, and other provisions that are applicable in the matter;

VI. Fraudulently or negligently classifying personal data as confidential without meeting the criteria specified in the applicable legal provisions. The sanction will only be imposed when a prior ruling has become final regarding the criteria for classifying personal data;

VII. Failure to comply with the duty of confidentiality established in Article 36 of this Law;

VIII. Failure to establish security measures in accordance with the provisions of Articles 25, 26 and 27 of this Law;

IX. Present violations of personal data due to the lack of implementation of security measures in accordance with articles 25, 26 and 27 of this Law;

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

XI. Obstructing the acts of verification of the authority;

XII. Creating personal databases in violation of the provisions of Article 5 of this Law;

XIII. Failure to comply with the resolutions issued by the Secretariat or the guarantor Authorities, and

XIV. Failing to submit the annual report and other reports referred to in Article 40, Section VI of the General Law on Transparency and Access to Public Information, or submitting them late.

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

If the alleged violation was committed by a member of a political party, the investigation and, where appropriate, sanction will be the responsibility of the competent electoral authority.

Financial sanctions may not be covered with public resources.

Article 133. For the conduct referred to in the previous article, the competent authority will be notified to to impose or execute the sanction.

Article 134. Liabilities arising from the corresponding administrative procedures, in accordance with the provisions of Article 132 of this Law, are independent of those of a civil, criminal or any other nature that may arise from the same facts.

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

For such purposes, the Secretariat or the guarantor authorities may report to the competent authorities any act or omission that violates this Law and provide the evidence they deem relevant, in accordance with the applicable laws.

Article 135. In the event of non-compliance by political parties, the Secretariat or the competent guarantor Authority shall notify, as appropriate, the National Electoral Institute or the local public electoral bodies of the competent Federal Entities so that they may resolve the matter, without prejudice to the sanctions established for political parties in the applicable laws.

In the case of potential violations related to public trusts or funds, the Secretariat or the competent guarantor authority must notify the internal control body or equivalent of the corresponding obligated subject so that it can implement the appropriate administrative procedures.

Article 136. In cases where the alleged offender is a public servant, the Secretariat or the Guaranteeing Authority must send to the competent authority, along with the corresponding complaint, a file containing all the elements that support the alleged administrative responsibility.

The authority that is aware of the matter must report on the conclusion of the procedure and, where appropriate, on the execution of the sanction to the Secretariat or the Guarantor Authority, as appropriate.

In order to carry out the procedure referred to in this article, the Secretariat or the corresponding Guarantee Authority must prepare the following:

I. Complaint addressed to the comptroller's office, internal control body or equivalent, with a precise description of the acts or omissions that, in its opinion, affect the proper application of this document.
Law and that could constitute a potential liability, and

II. File containing all the evidence considered relevant to support the existence of possible liability, and which proves the causal link between the disputed facts and the evidence presented.

The complaint and the file must be submitted to the Comptroller's Office, internal oversight body, or equivalent within fifteen days of the Secretariat or the corresponding Guarantor Authority becoming aware of the facts.

Article 137. The guarantor authority must report non-compliance with the determinations it issues and that involve the alleged commission of a crime before the competent authority.

Article Three and Article Four.- .....

Transients

First.- This Decree will enter into force on the day following its publication in the Official Gazette of the Federation, with the exception of what is provided in the Third Transitory Provision of this instrument.

Second.- Upon the entry into force of this Decree, the following provisions are repealed:

I. The Federal Law on the Protection of Personal Data Held by Private Parties, published in the Official Gazette of the Federation on July 5, 2010;

II. The General Law on Transparency and Access to Public Information, published in the Official Gazette of the Federation on May 4, 2015, and its subsequent amendments;

III. The Federal Law on Transparency and Access to Public Information, published in the Official Gazette of the Federation on May 9, 2016, and its subsequent amendments;

IV. The General Law on the Protection of Personal Data Held by Obligated Subjects, published in the Official Gazette of the Federation on January 26, 2017, and

V. The Agreement approving the Annual Program for Verification and Institutional Support for compliance with obligations regarding access to information and transparency by federally obligated entities, corresponding to the 2025 fiscal year, was published in the Official Gazette of the Federation on January 21, 2025.

Third.- Articles 71 and 72 of the General Law on Transparency and Access to Public Information will enter into force when the Federal Economic Competition Commission and the Federal Telecommunications Institute are extinguished in accordance with the provisions of the Tenth and Eleventh transitory provisions of the "Decree by which various provisions of the Political Constitution of the United Mexican States are reformed, added to and repealed, in matters of organic simplification", published in the Official Gazette of the Federation on December 20, 2024.

For the purposes of the preceding paragraph, the Federal Economic Competition Commission and the Federal Telecommunications Institute must make available to the public and update the information referred to in Article 72, Sections II and V, respectively, of the Federal Law on Transparency and Access to Public Information, which is repealed by virtue of this Decree.

Fourth.- The mentions, powers or functions contained in other laws, regulations and, in general, in any normative provision, regarding the National Institute of Transparency, Access to Information and Protection of Personal Data shall be understood to have been made or conferred to the public entities that acquire such powers or functions, as appropriate.

Fifth.- The labor rights of public servants of the National Institute of Transparency, Access to Information and Protection of Personal Data will be respected, in accordance with applicable legislation.
The human resources available at the aforementioned Institute will become part of the Anti-Corruption, Good Governance and Transparency Secretariat for the People.

The National Institute for Transparency, Access to Information, and Personal Data Protection will transfer the resources corresponding to the value of the inventory or staffing table of positions to the Ministry of Finance and Public Credit within twenty business days following the entry into force of this Decree, so that this agency can take the appropriate actions, in accordance with applicable legal provisions.

Public servants of the National Institute for Transparency, Access to Information and Protection of Personal Data who cease to provide their services to the aforementioned Institute and who are required to file a declaration of assets and interests, in accordance with applicable legal provisions, shall do so using the systems of the Secretariat for Anti-Corruption and Good Governance authorized for such purposes or through the means it determines and in accordance with the regulations applicable to the Federal Public Administration. The foregoing also applies to individuals who have served as public servants at the aforementioned Institute and who, as of the date this Decree enters into force, have yet to comply with this obligation.

Persons who, within the ten days prior to the entry into force of this Decree, have served as public servants of the National Institute for Transparency, Access to Information and Protection of Personal Data, including Commissioners, must submit an administrative record of institutional and individual delivery-receipt, as appropriate, to the public servant designated by the Anti-Corruption and Good Government Secretariat and in accordance with the regulations applicable to the Federal Public Administration, in the systems of the aforementioned agency enabled for such purposes or in the means it determines, with the understanding that the delivery made does not imply any release from any responsibilities that may be determined by the competent authority later.

Sixth.- The material resources available to the National Institute for Transparency, Access to Information and Protection of Personal Data will be transferred to the Secretariat for Anti-Corruption and Good Governance within twenty business days following the entry into force of this Decree.

Seventh.- The National Institute for Transparency, Access to Information and Protection of Personal Data will transfer financial resources to the Ministry of Finance and Public Credit, in accordance with applicable legal provisions.

Likewise, the National Institute for Transparency, Access to Information, and Protection of Personal Data must provide the aforementioned agency with the information and forms necessary to compile the Public Accounts and other reports for the first quarter, in accordance with applicable legal provisions, within ten business days following the entry into force of this Decree.

Eighth.- The internal and external records, registries and systems that comprise the National Transparency Platform of the National Institute for Transparency, Access to Information and Protection of Personal Data, as well as the computer systems used by said Institute, including those no longer in use but containing historical records, including their documentation and ownership, will be transferred to the Anti-Corruption and Good Governance Secretariat within fifteen business days following the entry into force of this Decree.

Ninth.- Procedures initiated prior to the entry into force of this Decree before the National Institute for Transparency, Access to Information and Protection of Personal Data, regarding access to public information, shall be substantiated before Transparency for the People in accordance with the applicable provisions in force at the time of their initiation.

Legal defense before administrative, jurisdictional, and judicial authorities regarding administrative and legal acts issued by the National Institute for Transparency, Access to Information, and Protection of Personal Data regarding access to public information will be carried out by Transparency for the People.

Transparency for the People may refer to the competent guarantor authority those matters that are mentioned in the preceding paragraphs that it is up to them according to the scope of their powers to address them.

Tenth.- Procedures initiated prior to the entry into force of this Decree before the National Institute for Transparency, Access to Information and Protection of Personal Data, in matters of personal data or any other than those mentioned in the previous transitional provision, shall be substantiated in accordance with the provisions in force at the time of their initiation before the Anti-Corruption and Good Government Secretariat referred to in this Decree.

Legal defense before administrative, jurisdictional, or judicial authorities of administrative and legal acts issued by the National Institute for Transparency, Access to Information, and Protection of Personal Data, regarding personal data or any other matters other than those mentioned in the previous transitional provision, as well as the monitoring of those currently in progress, including criminal and labor proceedings, will be carried out by the Anti-Corruption and Good Governance Secretariat.

The Anti-Corruption and Good Governance Secretariat may refer to the competent guarantor authority those matters mentioned in the preceding paragraphs that correspond to it according to the scope of its powers for its attention.

Eleventh.- Municipalities may comply with their obligations regarding transparency and access to information, in accordance with the provisions of the Tenth Transitory Provision of the General Law on Transparency and Access to Public Information, which is repealed by this Decree.

Twelfth.- The head of the Federal Executive Branch shall issue the corresponding adjustments to the regulations and other applicable provisions, including the Internal Regulations on Transparency for the People, within ninety calendar days following the entry into force of this Decree, in order to harmonize them with the provisions herein.

Thirteenth.- The files and archives that upon the entry into force of this Decree are in the charge of the National Institute of Transparency, Access to Information and Protection of Personal Data for the exercise of its substantive powers, competences or functions, in accordance with the General Law of Archives and other applicable legal provisions, will be transferred to the Anti-Corruption and Good Government Secretariat within twenty business days following the entry into force of this Decree.

The Anti-Corruption and Good Governance Secretariat, within thirty calendar days following receipt of the files and records mentioned in the preceding paragraph, may transfer them to the corresponding authority.

Fourteenth.- The Internal Control Body of the National Institute for Transparency, Access to Information and Protection of Personal Data is hereby dissolved and its matters and procedures that are under its charge upon the entry into force of this Decree, as well as the files and archives, shall be transferred to the Internal Control Body of the Anti-Corruption and Good Government Secretariat within twenty business days following its entry into force, and shall be processed and resolved by said body in accordance with the legal provisions in force at the time of its commencement.

Fifteenth.- For the purposes of the provisions of the Fifth, Sixth, Seventh, Eighth and Thirteenth transitional provisions of this Decree, the Plenary of the National Institute of Transparency, Access to Information and Protection of Personal Data must integrate, on the date of publication of this instrument, a Transfer Committee made up of the Commissioners of the aforementioned Institute and eleven public servants of the same with at least the level of Area Director or equivalent, who have knowledge of or are in charge of the matters mentioned in the transitional provisions themselves.

The Transfer Committee will be in place for a period of 30 calendar days, during which its members will work with the various competent authorities to address the matters outlined in the aforementioned transitional provisions and to carry out any other actions deemed necessary for such purposes.

Sixteenth.- The Council of the National System of Access to Public Information must be established no later than sixty calendar days after the entry into force of this Decree, following a call for this purpose issued by the Anti-Corruption and Good Government Secretariat.

Until the legislatures of the corresponding federal entities harmonize their legal framework regarding access to public information in accordance with the provisions of the Fourth Transitional Provision of the Decree amending, adding to, and repealing various provisions of the Political Constitution of the United Mexican States, regarding organic simplification, published in the Official Gazette of the Federation on December 20, 2024, the person holding the local executive branch in question will be a member of the Council of the National System for Access to Public Information.

Seventeenth.- The person holding the position of Executive Secretary of the Council of the National System of Access to Public Information will propose the rules of operation and functioning indicated in article 25, section XV, of the General Law of Transparency and Access to Public Information, to be approved at the installation of said Council.

Eighteenth.- The oversight and discipline body of the Judiciary; the internal oversight bodies of the autonomous constitutional bodies; the internal comptroller's offices of the Congress of the Union; the National Electoral Institute; the Federal Center for Conciliation and Labor Registration; and the Federal Conciliation and Arbitration Court must, within a maximum period of thirty calendar days from the date this Decree enters into force, make the necessary adjustments to their internal regulations to comply with the provisions of this instrument.

For the purposes of this transitional provision, each and every one of the procedures, processes and other means of appeal established in this instrument and other applicable regulations are suspended for a period of ninety calendar days from the date of entry into force of this Decree, with the exception of the reception and response to requests for information processed through the National Transparency Platform by the authorities mentioned in the previous paragraph.

Nineteenth.- Until the legislatures of the federative entities issue legislation to harmonize their legal framework in accordance with this Decree, the bodies that guarantee them will continue to operate and carry out the powers conferred on the local guarantor authorities, as well as the bodies in charge of internal oversight or their counterparts in the legislative and judicial branches, as well as the autonomous constitutional bodies of the federative entities themselves in this Law.

Twentieth.- The Federal Judicial Branch shall establish District Courts and Circuit Collegiate Courts specializing in matters of access to public information and protection of personal data, within a period of no more than one hundred and twenty calendar days from the date of entry into force of this Decree, to which the amparo trials in these matters that are pending for resolution shall be referred.

For the purposes of this transitional provision, the procedural deadlines and time limits for amparo proceedings regarding access to public information and the protection of personal data that are pending before District Courts and Circuit Collegiate Courts are hereby suspended for a period of one hundred and eighty calendar days from the date of entry into force of this Decree.

Mexico City, March 20, 2025.- Sen. Imelda Castro Castro, Vice President.- Rep. Sergio Carlos Gutiérrez Luna, President.- Sen. Verónica Noemí Camino Farjat, Secretary.- Rep. José Luis Montalvo Luna, 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, on March 20, 2025. - **Claudia Sheinbaum Pardo,** President of the United Mexican States. - Signature. - Lcda. **Rosa Icela Rodríguez Velázquez,** Secretary of the Interior.

Rubric.