**FEDERAL LAW FOR THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES**

CHAMBER OF DEPUTIES OF THE H. CONGRESS OF THE UNION
General Secretariat
Parliamentary Services Secretariat

*New Law DOF 20-03-2025*

# FEDERAL LAW FOR THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES

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

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

**CLAUDIA SHEINBAUM PARDO**, President of the United Mexican States, to its inhabitants be it known:

That the Honorable Congress of the Union, has been so kind as to address to me 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 FOR THE PROTECTION OF PERSONAL DATA IN POSSESSION OF OBLIGATED SUBJECTS; THE FEDERAL LAW FOR THE PROTECTION OF PERSONAL DATA IN POSSESSION OF PRIVATE PARTIES; AND THE AMENDMENT OF ARTICLE 37, SECTION XV, OF THE ORGANIC LAW OF THE FEDERAL PUBLIC ADMINISTRATION ARE HEREBY ENACTED.**

**Article One and Article Two.-** .....

**Article Three.-** The Federal Law for the Protection of Personal Data in Possession of Private Parties is hereby **enacted**, to read as follows:

## FEDERAL LAW FOR THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES

### Chapter I

### General Provisions

**Article 1.** This Law is of public order and of general observance throughout the national territory and its purpose is the protection of personal data in possession of private parties, with the purpose of regulating its legitimate, controlled and informed processing, in order to guarantee the privacy and the right to informational self-determination of individuals.

The following are exempted from the application of this Law:

**I.** Credit reporting companies under the provisions of the Law to Regulate Credit Reporting Companies and other applicable provisions, and

**II.** Persons who carry out the collection and storage of personal data, which is exclusively for personal use, and without the purpose of disclosure or commercial use.

**Article 2.** For the purposes of this Law, the following definitions shall apply:

**I.** **Privacy Notice:** Document available to the data subject in physical, electronic or any other format generated by the data controller, from the moment in which his/her personal data is collected, in order to inform him/her of the purposes of the processing thereof, in accordance with Article 14 of this Law;

**II.** **Databases:** An ordered set of personal data referring to an identified or identifiable person conditioned to determined criteria, regardless of the form or modality of its creation, type of support, processing, storage and organization;

**III.** **Blocking:** Identification and preservation of personal data once the purpose for which they were collected has been fulfilled, for the sole purpose of determining possible liabilities in connection with their processing, until the legal or contractual statute of limitations period. During this period, personal data may not be processed and, after this period has elapsed, they will be cancelled in the corresponding database;

**IV.** **Consent:** Manifestation of the free, specific and informed will of the data subject by means of which the data is processed;

**V.** **Personal Data:** Any information concerning an identified or identifiable person. A person is considered identifiable when his identity can be determined directly or indirectly through any information;

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

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

**VIII.** **Days:** Business days;

**IX.** **Dissociation:** Procedure by which personal data cannot be associated with the data subject or allow, due to its structure, content or degree of disaggregation, the identification of the data subject;

**X.** **Public access source:** Those databases, systems or files that by law may be publicly consulted when there is no impediment by a limiting rule, and with no other requirement than, as the case may be, the payment of a consideration, fee or contribution. It shall not be considered a source of public access when the information contained therein is obtained or has an unlawful origin, in accordance with the provisions established by this Law and other applicable legal provisions;

**XI.** **Law:** Federal Law for the Protection of Personal Data in Possession of Private Parties;

**XII.** **Processor person:** Natural or legal person who alone or jointly with others processes personal data on behalf of the data controller;

**XIII.** **Regulation:** Regulation of the Federal Law for the Protection of Personal Data in Possession of Private Parties;

**XIV.** **Data Controller:** Regulated subjects referred to in section XVI of this article;

**XV.** **Secretariat:** Anticorruption and Good Governance Secretariat;

**XVI.** **Regulated subjects:** Individuals or private legal entities that carry out the processing of personal data;

**XVII.** **Third Party:** Natural or legal person, national or foreign, other than the data subject or the data controller for the data;

**XVIII.** **Data Subject:** Person to whom the personal data corresponds;

**XIX.** **Processing:** Any operation or set of operations carried out by means of manual or automated procedures applied to personal data, related to the collection, use, recording, organization, preservation, storage, processing, use, communication, dissemination, storage, possession, access, handling, use, disclosure, transfer or disposal of personal data, and

**XX.** **Transfer:** Any communication of personal data within or outside Mexican territory, made to a person other than the data subject, the data controller or the processor.

**Article 3.** The principles and rights provided for in this Law shall have as a limit as to their observance and exercise, the protection of national security, public order, safety and health, as well as the rights of third parties.

**Article 4.** In the absence of express provision in this Law, the provisions of the Federal Code of Civil Procedures and the Federal Law of Administrative Procedure shall be applied in a supplementary manner.

For the substantiation of proceedings for the protection of rights, verification and imposition of sanctions, the provisions contained in the Federal Law of Administrative Procedure will be observed.

## Chapter II

## Personal Data Protection Principles

**Article 5.** The data controller shall observe the principles of legality, purpose, loyalty, consent, quality, proportionality, information and responsibility in the processing of personal data.

**Article 6.** Personal data shall be collected and processed in a lawful manner in accordance with the provisions of this Law and other applicable legal provisions.

The data controller shall not obtain and process personal data through deceitful or fraudulent means, and shall give priority to the protection of the interests of the data subject and the reasonable expectation of privacy, understood as the trust placed by any person in another, that the personal data provided will be processed in accordance with what they agreed in the terms established by this Law.

**Article 7.** Any processing of personal data shall be subject to the consent of the data subject, except for the exceptions provided for in this Law.

Consent may be express or tacit. It shall be understood that consent is express when the will of the data subject is expressed verbally, in writing, by electronic or optical means, unequivocal signs or by any other technology.

The consent will be tacit when, having made the privacy notice available to the data subject, he/she does not express his/her will to the contrary.

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

Financial or patrimonial data shall require the express consent of the data subject, except for the exceptions referred to in Articles 9 and 36 of this Law.

Consent may be revoked at any time without retroactive effect. To revoke consent, the data controller shall, in the privacy notice, establish the mechanisms and procedures to do so.

**Article 8.** In the case of sensitive personal data, the data controller shall obtain the express written consent of the data subject for the processing thereof, by means of his autograph signature, electronic signature, or any authentication mechanism established for such purpose.

Databases containing sensitive personal data may not be created without justifying the creation of such databases for legitimate and specific purposes, in accordance with the activities or explicit purposes pursued by the regulated entity.

**Article 9.** The data controller shall not be obliged to obtain the consent of the data subject for the processing of personal data when:

**I.** A legal provision so provides;

**II.** The personal data is contained in publicly available sources;

**III.** The personal data is subjected to a prior disassociation procedure;

**IV.** The personal data is required to exercise a right or fulfill obligations arising from a legal relationship between the data subject and the data controller;

**V.** An emergency situation exists that could potentially harm an individual's person or property;

**VI.** The personal data are indispensable to carry out a treatment for medical care, prevention, diagnosis, provision of health care, or management of health services, as long as the data subject is not in a position to grant consent, in the terms established by the General Health Law and other applicable legal provisions, and that such data processing is carried out by a person subject to professional secrecy or equivalent obligation, or

**VII.** There is a court order, resolution or mandate founded and motivated by a competent authority.

**Article 10.** The data controller shall ensure that the personal data contained in the databases are accurate, complete, correct and updated for the purposes for which they were collected.

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

The data controller shall be obliged to delete the data related to the breach of contractual obligations, once a period of seventy-two months has elapsed, counted from the calendar date on which the breach occurs.

**Article 11.** The processing of personal data shall be limited to the fulfillment of the purposes set forth in the privacy notice; however, if the data controller intends to process the data for a purpose other than those set forth in the privacy notice, the consent of the data subject shall be required to be obtained again.

**Article 12.** The processing of personal data shall be that which is necessary, adequate and relevant in relation to the purposes set forth in the privacy notice; for sensitive personal data, the data controller shall make reasonable efforts to limit the period of processing of such data so that it is the minimum necessary.

**Article 13.** The data controller shall ensure compliance with the principles of personal data protection established by this Law, and shall adopt the necessary and sufficient measures for its application, as well as to guarantee that the privacy notice made known to the data subject is respected at all times by the data controller or by third parties with whom it has a legal relationship.

**Article 14.** The data controller shall have the obligation to inform the data subject, through the privacy notice, of the existence and main characteristics of the processing to which his or her personal data will be subjected, so that he or she may make informed decisions in this respect.

**Article 15.** The privacy notice shall contain, at least, the following information:

**I.** The identity and address of the data controller;

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

**III.** The purposes of the processing of personal data, distinguishing those that require the consent of the data subject;

**IV.** The options and means offered by the data controller to the data subjects to limit the use or disclosure of the data;

**V.** The mechanisms, means and procedures to exercise the ARCO rights, pursuant to the provisions of this Law, and

**VI.** The procedure and means by which the data controller will inform the data subjects of changes to the privacy notice, in accordance with the provisions of this Law.

**Article 16.** The data controller must make the privacy notice available to the data subjects, through printed, digital, visual, audio or any other technology in the following manner:

**I.** When personal data is obtained in person through printed formats, it must be disclosed at that time, unless the notice has been provided beforehand, and

**II.** When personal data is obtained by any electronic, optical, sound, visual or any other technology, it must be provided in its simplified form, which must contain at least the information referred to in sections I to IV of the preceding article, and indicate the site where the comprehensive privacy notice may be consulted.

**Article 17.** When the data have not been obtained directly from the data subject, the data controller shall inform him/her of the change in the privacy notice.

The provisions of the preceding paragraph do not apply when the processing is for historical, statistical or scientific purposes.

When it is impossible to disclose the privacy notice to the data subject directly or this requires disproportionate efforts, the data controller may implement compensatory measures in terms of the Regulations of this Law.

**Article 18.** Every data controller shall establish and maintain administrative, technical and physical security measures to protect personal data against damage, loss, alteration, destruction or unauthorized use, access or processing.

The data controllers shall not adopt lesser security measures than those they maintain for the handling of their information. Likewise, the existing risk, the possible consequences for the data subjects, the sensitivity of the data and the technological development shall be taken into account.

**Article 19.** Security breaches occurring at any stage of the processing of personal data that significantly affect the economic or moral rights of the data subjects shall be immediately reported by the data controller, so that he/she may take the corresponding measures to defend his/her rights.

**Article 20.** The controller or third party shall establish controls or mechanisms whose purpose is to ensure that all persons involved in any phase of the processing of personal data shall maintain confidentiality with respect to such data, an obligation that shall subsist even after the end of their relationship with the controller or third party.

## Chapter III

## On the Rights of the Data Subjects

**Article 21.** Any data subject or, as the case may be, its legal representative, may exercise the ARCO rights provided for in this Law.

The exercise of any of the ARCO rights is not a prerequisite nor does it prevent the exercise of another.

Personal data must be safeguarded in such a way as to allow the exercise of these rights without delay.

**Article 22.** The data subject will have the right to access his/her personal data in the possession of the data controller, as well as to know the information related to the conditions and generalities of its processing, through the privacy notice.

**Article 23.** The data subject shall have the right to request the rectification or correction of his personal data, when they are inaccurate, incomplete or outdated.

**Article 24.** The data subject shall at all times have the right to request the cancellation of his or her personal data from the files, records, files and systems of the data controller, so that such data are no longer in the possession of the data controller.

The cancellation of personal data will give rise to a blocking period after which the data will be deleted, the data controller may keep them exclusively for the purposes of the liabilities arising from the processing.

The blocking period will be equivalent to the statute of limitations period of the actions derived from the legal relationship on which the processing is based under the terms of the applicable law on the matter, and once the data has been cancelled, notice will be given to the data subject.

When the personal data had been transmitted prior to the date of rectification or cancellation and continue to be processed by third parties, the data controller shall inform them of such request for rectification or cancellation, so that they may proceed to carry it out as well.

**Article 25.** The data controller shall not be obliged to cancel personal data when:

**I.** It refers to the parties to a private, social or administrative contract and is necessary for its development and performance;

**II.** Must be treated by law;

**III.** Obstructs judicial or administrative proceedings related to tax obligations, the investigation and prosecution of crimes or the updating of administrative sanctions;

**IV.** Are necessary to protect the legally protected interests of the data subject;

**V.** Are necessary to carry out an action in the public interest;

**VI.** They are necessary to comply with an obligation legally acquired by the data subject, and

**VII.** Are the object of processing for prevention or for medical diagnosis or the management of health services, provided that such processing is carried out by a health professional subject to a duty of confidentiality.

**Article 26.** The data subject shall have the right at any time and for legitimate reasons to object to the processing of his data or to demand the cessation of such processing when:

**I.** There is legitimate cause and his/her specific situation so requires, which must justify that even though the processing is lawful, it must cease in order to prevent its persistence from causing him/her harm or damage, or

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

The exercise of the right to object shall not be applicable in those cases in which the processing is necessary for the fulfillment of a legal obligation imposed on the data controller.

## Chapter IV

## Exercise of Access, Rectification, Cancellation and Opposition Rights

**Article 27.** The data subject or his/her legal representative may request the data controller at any time to exercise his/her ARCO rights with respect to the personal data concerning him/her.

**Article 28.** The request for the exercise of ARCO rights shall contain and be accompanied by the following:

**I.** The name of the data subject and its address or any other means to receive notifications;

**II.** Documents proving the identity of the data subject or, as the case may be, the personality and identity of its representative;

**III.** The clear and precise description of the personal data with respect to which the exercise of any of the ARCO rights is sought, except in the case of the right of access;

**IV.** The description of the ARCO right that is intended to be exercised, or what the data subject is requesting, and

**V.** Any other element or document that facilitates the location of personal data.

**Article 29.** Every data controller shall promote the protection of personal data within the organization and shall designate a person, or personal data department, who shall process the requests of the data subjects for the exercise of the rights referred to in this Law.

**Article 30.** In the case of requests for the exercise of the right to rectify personal data, the data subject must indicate, in addition to the provisions of Article 29 of this Law, the modifications to be made and provide the documentation supporting the request.

**Article 31.** The data controller will communicate to the data subject, within a maximum period of twenty days from the date on which the request for the exercise of the ARCO rights was received, the determination adopted, in order that, if appropriate, the same may be made effective within fifteen days following the date on which the response is communicated. In the case of requests for the exercise of the right of access to personal data, the delivery will be made upon proof of the identity of the data subject or legal representative, as appropriate.

The aforementioned terms may be extended only once for an equal period, provided that the circumstances of the case so justify.

**Article 32.** The obligation of access to personal data shall be deemed to be fulfilled when such data is made available to the data subject; or, by means of the issuance of simple copies, electronic documents or any other means determined by the data controller in the privacy notice.

In the event that the data subject requests access to the data from a person who is presumed to be the data controller and this person turns out not to be the data controller, it shall be sufficient for the data subject to be so informed by any of the means referred to in the preceding paragraph, in order for the request to be deemed to have been complied with.

**Article 33.** The causes in which the exercise of the ARCO rights shall not be applicable and therefore the data controller may deny the same are:

**I.** When the data subject or the legal representative is not duly accredited to do so;

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

**III.** When the rights of a third party are violated;

**IV.** When there is a legal impediment, or the resolution of a competent authority, which restricts access to personal data, or does not allow the rectification, cancellation or opposition of the same, and

**V.** When the rectification, cancellation or opposition has been previously made.

The refusal referred to in this article may be partial when any of the requirements described in the request for the exercise of the ARCO rights of the data subject or his/her representative are not found in any of the aforementioned causes, in which case the data controller will carry out the required access, rectification, cancellation or opposition.

In all the above cases, the data controller must inform the reason for its decision and communicate it to the data subject, or if applicable, to the legal representative, within the deadlines established for such purpose, by the same means by which the request for the exercise of the ARCO rights was carried out, accompanying, if applicable, the evidence that may be relevant.

**Article 34.** The exercise of ARCO rights is free of charge; charges may only be made to recover the costs of reproduction, copies or mailing.

When the data subject provides the magnetic or electronic media or the necessary mechanism to reproduce the personal data, such data shall be delivered free of charge to the data subject.

When the same person or his/her representative repeats his/her request in a period of less than twelve months, the costs will not be greater than three times the current Unit of Measurement and Updating, unless there are substantial modifications to the privacy notice that motivate new consultations.

## Chapter V

## Data Transfer

**Article 35.** When the data controller intends to transfer personal data to national or foreign third parties, other than the processor, he/she shall inform them of the privacy notice and the purposes to which the data subject subjected his/her data processing.

The processing of the data will be done in accordance with the terms of the privacy notice, which will contain a clause indicating whether or not the data subject accepts the transfer of his/her data, likewise, the third party receiver will assume the same obligations that correspond to the data controller for transferring the data.

**Article 36.** National or international transfers of data may be carried out without the consent of the data subject when they fall within any of the following cases:

**I.** The transfer is provided for in a Law or Treaty to which Mexico is a party;

**II.** The transfer is necessary for prevention or medical diagnosis, the provision of health care, medical treatment or the management of health services;

**III.** The transfer is made to controlling companies, subsidiaries or affiliates under the common control of the data controller, or to a parent company or to any company of the same group of the data controller that operates under the same internal processes and policies;

**IV.** 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;

**V.** The transfer is necessary or legally required for the safeguarding of a public interest, or for the procurement or administration of justice;

**VI.** The transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and

**VII.** The transfer is necessary for the maintenance or fulfillment of a legal relationship between the data controller and the data subject.

## Chapter VI

## Self-regulation

**Article 37.** Individuals or legal entities may agree among themselves or with civil or governmental, national or foreign organizations, binding self-regulation schemes on the subject, which complement the provisions of this Law. Such schemes shall contain mechanisms to measure their effectiveness in data protection, consequences and effective corrective measures in the event of non-compliance.

Self-regulatory schemes may take the form of codes of ethics or good professional practice, trust seals or other mechanisms, and shall contain specific rules or standards to harmonize the processing of data carried out by members and facilitate the exercise of the rights of data subjects. Such schemes shall be notified simultaneously to the corresponding authorities and to the Secretariat.

## Chapter VII

## From the Secretariat

**Article 38.** The Secretariat, for the purposes of this Law, shall have the purpose of disseminating knowledge of the right to the protection of personal data in Mexican society, promoting its exercise and overseeing the due observance of the provisions set forth in this Law and deriving from the same; in particular those related to compliance with obligations on the part of the subjects regulated by this ordinance.

**Article 39.** The Secretariat has the following attributions:

**I.** To monitor and verify compliance with the provisions contained in this Law, within the scope of its competence, with the exceptions provided by law;

**II.** To interpret this Law in the administrative field;

**III.** Provide technical support to the data controllers who request it, for compliance with the obligations established in this Law;

**IV.** To issue criteria and recommendations, in accordance with the applicable provisions of this Law, for the purpose of its functioning and operation;

**V.** Disseminate international standards and best practices in information security, taking into account the nature of the data, the purposes of the processing, and the technical and economic capacities of the data controller;

**VI.** To hear and resolve the procedures for the protection of rights and verification indicated in this Law and to impose sanctions as appropriate;

**VII.** Cooperate with other supervisory authorities and national and international organizations, in order to cooperate in data protection matters;

**VIII.** To attend international forums within the scope of this Law;

**IX.** Elaborate privacy impact studies prior to the implementation of a new personal data processing modality or the implementation of substantial modifications to existing processing;

**X.** Disseminate knowledge of the obligations regarding the protection of personal data and provide training to the obligated parties, and

**XI.** Any other duties conferred by this Law and other applicable ordinances.

## Chapter VIII

## Rights Protection Procedure

**Article 40.** The procedure shall be initiated at the request of the data subject or his or her legal representative, clearly stating the content of his or her claim and the provisions of this Law that are considered to have been violated. The request for data protection must be filed with the Secretariat within fifteen days following the date on which the response is communicated to the data subject by the data controller.

In the event that the data subject does not receive a response from the data controller, the data protection request may be filed as of the expiration of the response period provided for the data controller. In this case, it will be sufficient for the data subject to attach

to his/her data protection request the document proving the date on which he/she filed the request for access, rectification, cancellation or opposition.

The request for data protection will also proceed in the same terms when the data controller does not deliver the requested personal data to the data subject, or does so in an incomprehensible format, refuses to make modifications or corrections to the personal data, the data subject is not satisfied with the information delivered because he/she considers it is incomplete or does not correspond to the requested information.

Once the request for data protection has been received by the Secretariat, it will be forwarded to the data controller so that, within fifteen days, it may issue a response, offer the evidence it deems pertinent and state in writing what it deems appropriate.

The Secretariat shall admit the evidence it deems pertinent and shall proceed with its examination. Likewise, it may request from the data controller such other evidence as it deems necessary. Once the evidence has been presented, the Secretariat shall notify the data controller of its right to present its arguments, if it deems it necessary, within five days following notification.

For the due conduct of the procedure, the Secretariat will decide on the data protection request formulated, after analyzing the evidence and other elements of conviction it deems pertinent, such as those derived from the hearing or hearings held with the parties.

The Regulations of the Law shall establish the form, terms and time periods in accordance with which the procedure for the protection of rights shall be carried out.

**Article 41.** The request for data protection may be filed in writing or through the forms of the electronic system provided for such purpose by the Secretariat, and shall contain the following information:

**I.** The name of the data subject or, as the case may be, of his legal representative, as well as of the interested third party, if any;

**II.** The name of the data controller before which the request for access, rectification, cancellation or opposition of personal data was filed;

**III.** The address to hear and receive notifications;

**IV.** The date on which the response of the data controller was made known, unless the proceeding is initiated based on the provisions of Article 45 of this Law;

**V.** The acts that motivate your data protection request, and

**VI.** Any other elements that are deemed appropriate to make known to the Secretariat.

The form and terms in which the identity of the data subject or the legal representation must be accredited shall be established in the Regulations.

Likewise, the request for data protection must be accompanied by the request and the response being appealed or, as the case may be, the data allowing its identification.

In case of lack of response it will only be necessary to submit the application.

In the event that the request for data protection is filed by means other than electronic means, it must be accompanied by sufficient copies of the transfer.

**Article 42.** The maximum term for issuing the decision in the procedure for the protection of rights shall be fifty days, counted from the date of filing the request for data protection. When there is just cause, the Secretariat may extend this period once and for up to the same period.

**Article 43.** In the event that the resolution for the protection of rights is favorable to the data subject, the data controller shall be required to enforce the exercise of the rights subject to protection within ten days following the notification or, where justified, within a longer period established in the resolution itself, and shall inform the Secretariat in writing of such compliance within the following ten days.

**Article 44.** In the event that the request for data protection does not satisfy any of the requirements referred to in Article 41 of this Law, and the Secretariat does not have the elements to remedy it, the data subject will be notified within twenty days following the filing of the request for data protection, on a single occasion, in order to remedy the omissions within a period of five days. Once the term has elapsed without the prevention having been addressed, the request for data protection shall be deemed not to have been filed. The prevention will have the effect of interrupting the term the Secretariat has to resolve the data protection request.

**Article 45.** The Secretariat shall make up for deficiencies in the complaint in cases where this is required, provided that it does not alter the original content of the request for access, rectification, cancellation or objection of personal data, nor does it modify the facts or requests set forth therein or in the request for data protection.

**Article 46.** The resolutions of the Secretariat may:

**I.** To dismiss or reject the request for data protection as inadmissible;

**II.** Confirm, revoke or modify the data controller's response, or

**III.** Order the delivery of personal data, in case of omission of the data controller.

**Article 47.** The request for data protection shall be dismissed as inadmissible when:

**I.** The Secretariat is not competent;

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

**III.** The Secretariat has previously heard the request for data protection against the same act and made a final decision with respect to the same appellant;

**IV.** An appeal or means of defense filed by the data subject or, as the case may be, by the interested third party, against the act appealed before the Secretariat, is being processed before the competent courts;

**V.** It is an offensive or unreasonable data protection request, or

**VI.** It is extemporaneous because the term established in Article 40 of this Law has elapsed.

**Article 48.** The request for data protection shall be dismissed when:

**I.** The data subject dies;

**II.** The data subject expressly desists;

**III.** Once the request for data protection has been admitted, a cause of inadmissibility arises, and

**IV.** For any reason the same is without subject matter.

**Article 49.** The Secretariat may at any time during the procedure seek conciliation between the data subject and the data controller.

If a conciliation agreement is reached between both parties, it shall be recorded in writing and shall be binding. The request for data protection will be without subject matter and the Secretariat will verify compliance with the respective agreement.

For purposes of the conciliation referred to herein, the procedure established in the Regulations of this Law shall apply.

**Article 50.** Once the request for data protection has been filed in the absence of a response to a request for the exercise of the ARCO rights by the data controller, the Secretariat shall give notice to the data controller so that, within a period not exceeding ten days, it may prove that it has responded in due time and form to the request, or else provide a response to the same. In the event that the response complies with the request, the request for data protection shall be deemed inadmissible and the Secretariat shall dismiss it.

In the second case, the Secretariat will issue its resolution based on the content of the original request and the response of the data controller referred to in the preceding paragraph.

If the resolution of the Secretariat referred to in the preceding paragraph determines that the request is admissible, the data controller will proceed to comply with it, at no cost to the data subject, and the data controller must cover all costs generated by the corresponding reproduction and mailing expenses.

**Article 51.** Against the resolutions of the Secretariat, private parties may file an amparo proceeding. Amparo proceedings shall be heard by specialized judges and courts under the terms of Article 94 of the Political Constitution of the United Mexican States.

**Article 52.** All decisions of the Secretariat shall be susceptible to public disclosure in public versions, eliminating those references to the data subject that identify him/her or make him/her identifiable.

**Article 53.** The data subjects who consider that they have suffered damage or injury to their property or rights as a consequence of non-compliance with the provisions of this Law by the data controller or the processor, may exercise the rights they deem pertinent for the purposes of the appropriate compensation, in terms of the corresponding legal provisions.

## Chapter IX

## Verification Procedure

**Article 54.** The Secretariat shall verify compliance with this Law and the regulations derived therefrom. The verification may be initiated ex officio or at the request of a party.

The ex officio verification will proceed when there is non-compliance with resolutions issued in connection with the rights protection procedures referred to in the preceding Chapter or when it is presumed that violations of this Law have been committed.

**Article 55.** In the verification procedure, the Secretariat shall have access to the information and documentation it deems necessary, in accordance with the resolution that motivates it.

Public servants shall be obliged to keep confidential the information they learn from the corresponding verification.

The Regulations shall develop the form, terms and time periods in which the procedure referred to in this Article shall be carried out.

## Chapter X

## Procedure for the Imposition of Sanctions

**Article 56.** If on the occasion of the processing of the procedure for the protection of rights or the verification procedure carried out by the Secretariat, the Secretariat becomes aware of an alleged breach of any of the principles or provisions of this Law, it shall initiate the procedure for the imposition of sanctions.

**Article 57.** The procedure for the imposition of penalties shall commence with the notification made by the Secretariat to the alleged offender, regarding the facts that led to the initiation of the procedure, and shall grant him a term of fifteen days to submit evidence and state in writing what he deems appropriate. In the event the evidence is not submitted, the Secretariat will decide in accordance with the elements of conviction available to it.

The Secretariat shall admit such evidence as it deems pertinent and shall proceed to the presentation thereof. Likewise, it may request from the alleged infringing person such other evidence as it deems necessary. Once the evidence has been presented, the Secretariat shall notify the alleged infringer of its right to present its arguments, if it deems it necessary, within five days following notification.

The Secretariat, after analyzing the evidence and other elements of conviction that it deems pertinent, shall issue a final decision within fifty days following the date on which the sanctioning procedure was initiated. Such resolution shall be notified to the parties.

When there is justified cause, the Secretariat may extend this period once and for up to an equal period.

The Regulations will develop the form, terms and deadlines in which the procedure for the imposition of sanctions will be substantiated, including the presentation of evidence and allegations, the holding of hearings and the closing of the investigation.

## Chapter XI

## Infringements and Penalties

**Article 58.** The conducts carried out by the data controller shall constitute violations of this Law:

**I.** Failure to comply with the request for the exercise of the data subject's ARCO rights, without a well-founded reason, in the terms provided in this Law;

**II.** Acting with negligence or malice during the substantiation of requests for the exercise of ARCO rights;

**III.** Fraudulently declaring the non-existence of personal data, when it exists totally or partially in the databases of the data controller;

**IV.** Processing personal data in contravention of the principles set forth in this Law;

**V.** Omitting in the privacy notice, any or all of the elements referred to in Article 15 of this Law;

**VI.** Keeping inaccurate personal data when it is attributable to the data controller, or not carrying out the legally required rectifications or cancellations of the same when the rights of the data subjects are affected;

**VII.** Failure to comply with the warning referred to in Section I of Article 59 of this Law;

**VIII.** Failure to comply with the duty of confidentiality established in Article 20 of this Law;

**IX.** Substantially changing the original purpose of the data processing, without observing the provisions of Article 11 of this Law;

**X.** Transferring data to third parties without communicating to them the privacy notice containing the limitations to which the data subject has subjected the disclosure of such data;

**XI.** Violate the security of databases, premises, programs or equipment, when it is attributable to the data controller;

**XII.** To carry out the transfer or assignment of personal data, outside the cases in which it is permitted by law;

**XIII.** Collect or transfer personal data without the express consent of the data subject, in those cases in which such consent is required;

**XIV.** Obstructing the acts of verification of the authority;

**XV.** Collecting data in a misleading and fraudulent manner;

**XVI.** Continuing with the illegitimate use of personal data when the cessation of such use has been requested by the Secretariat or the data subjects;

**XVII.** Process personal data in a way that affects or prevents the exercise of the ARCO rights established in Article 16 of the Political Constitution of the United Mexican States;

**XVIII.** Create databases in contravention of the provisions of Article 8, second paragraph of this Law, and

**XIX.** Any failure of the data controller to comply with the obligations established in terms of the provisions of this Law.

**Article 59.** Violations of this Law shall be sanctioned by the Secretariat with:

**I.** The warning for the data controller to carry out the acts requested by the data subject, under the terms provided by this Law, in the cases provided for in section I of the preceding article;

**II.** Fine of 100 to 160,000 times the Unit of Measurement and Updating, in the cases provided for in sections II to VII of the preceding article;

**III.** Fine of 200 to 320,000 times the Unit of Measurement and Updating, in the cases provided for in sections VIII to XVIII of the preceding article, and

**IV.** In the event that the violations mentioned in the preceding paragraphs persist, an additional fine will be imposed ranging from 100 to 320,000 times the Unit of Measurement and Updating. In the case of violations committed in the processing of sensitive data, the penalties may be increased up to two times the established amounts.

**Article 60.** The Secretariat shall state the grounds and reasons for its resolutions, considering:

**I.** The nature of the data;

**II.** The notorious inappropriateness of the refusal of the data controller to perform the acts requested by the data subject, in terms of this Law;

**III.** The intentional or unintentional nature of the action or omission constituting the infraction;

**IV.** The economic capacity of the data controller, and

**V.** Recidivism.

**Article 61.** The penalties set forth in this Chapter shall be imposed without prejudice to the resulting civil or criminal liability.

**Chapter XII**

**Offenses Concerning the Improper Processing of Personal Data**

**Article 62.** A prison term of three months to three years shall be imposed on anyone who, being authorized to process personal data, with a profit motive, causes a security breach to the databases under his/her custody.

**Article 63.** A prison term of six months to five years shall be imposed on anyone who, for the purpose of obtaining an undue profit, processes personal data by means of deception, taking advantage of the error in which the data subject or the person authorized to transmit such data is found.

**Article 64.** In the case of sensitive personal data, the penalties referred to in this Chapter shall be doubled.

**Article Four.-** .....

**Transitory**

**First.-** This Decree shall enter into force on the day following its publication in the Official Gazette of the Federation, with the exception of the provisions set forth in the Third transitory provision of this instrument.

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

**I.** The Federal Law for the Protection of Personal Data in Possession of 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 for the Protection of Personal Data in Possession of Obligated Subjects, published in the Official Gazette of the Federation on January 26, 2017, and

**V.** The Agreement approving the Annual Program of Verification and Institutional Accompaniment for the compliance with the obligations regarding access to information and transparency by the federal compelled subjects, corresponding to the fiscal year 2025, published in the Official Gazette of the Federation on January 21, 2025.

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

For 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 this Decree.

**Fourth.-** The mentions, attributions or functions contained in other laws, regulations and, in general, in any normative provision, with respect to the National Institute of Transparency, Access to Information and Protection of Personal Data shall be understood as made or conferred to the public entities that acquire such attributions or functions, as the case may be.

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

The National Institute of Transparency, Access to Information and Protection of Personal Data will transfer the resources corresponding to the value of the inventory or payroll to the Ministry of Finance and Public Credit, within twenty working days from the entry into force of this Decree, in order for such agency to carry out the corresponding actions, in accordance with the applicable legal provisions.

The public servants of the National Institute for Transparency, Access to Information and Protection of Personal Data who cease to render their services in the aforementioned Institute and who are required to file a statement of assets and interests, in accordance with the applicable legal provisions, shall do so in the systems of the Anticorruption and Good Governance Secretariat enabled for such purposes or in the means determined by the latter and in accordance with the regulations applicable to the Federal Public Administration. The foregoing is also applicable to persons who have served as public servants in the aforementioned Institute and who, as of the date of entry into force of this Decree, have yet to comply with such obligation.

Persons who within 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 handover, as appropriate, to the public servant that the Anticorruption and Good Governance Secretariat designates and in accordance with the regulations applicable to the Federal Public Administration, in the systems of the referred agency enabled for such purposes or in the means that it determines, in the understanding that the delivery that is made does not imply any release of responsibilities that could be determined by the competent authority at a later date.

**Sixth.-** The material resources of the National Institute of Transparency, Access to Information and Protection of Personal Data shall be transferred to the Anticorruption and Good Governance Secretariat, within twenty working days following the entry into force of this Decree.

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

Likewise, the National Institute for Transparency, Access to Information and Protection of Personal Data must deliver to the aforementioned agency the information and formats necessary to integrate the Public Account and other reports corresponding to the first quarter, in accordance with the applicable legal provisions, within ten working days following the entry into force of this Decree.

**Eighth.-** The internal and external records, lists and systems that make up 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 that are no longer in use but contain historical records, including their documentation and data subjectship, shall be transferred to the Anticorruption and Good Governance Secretariat within fifteen working days following the entry into force of this Decree.

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

The legal defense before administrative, jurisdictional and judicial authorities of the administrative and legal acts issued by the National Institute of Transparency, Access to Information and Protection of Personal Data, in matters of 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 mentioned in the preceding paragraphs that correspond to it in accordance with the scope of its powers for its attention.

**Tenth.-** Proceedings initiated prior to the entry into force of this Decree before the National Institute of Transparency, Access to Information and Protection of Personal Data, in matters of personal data or any other different from those mentioned in the preceding transitory provision, shall be substantiated in accordance with the provisions in force at the time of their initiation before the Anti-Corruption and Good Governance Secretariat referred to in this Decree.

The legal defense before administrative, jurisdictional or judicial authorities of the administrative and legal acts issued by the National Institute of Transparency, Access to Information and Protection of Personal Data, in matters of personal data or any other different from those mentioned in the preceding transitory provision, as well as the follow-up of those in process, including criminal and labor proceedings, will be carried out by the Anticorruption and Good Governance Secretariat.

The Anticorruption 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.-** The municipalities may comply with their obligations regarding transparency and access to information, in terms of the provisions of the Tenth transitory provision of the General Law of Transparency and Access to Public Information, which is repealed by virtue of this Decree.

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

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

The Anticorruption and Good Governance Secretariat, within thirty calendar days from the receipt of the files and archives mentioned in the preceding paragraph, may transfer them to the corresponding authority.

**Fourteenth.-** The Internal Control Organ of the National Institute of Transparency, Access to Information and Protection of Personal Data is hereby terminated and its matters and procedures that at the entry into force of this Decree are in its charge, as well as the files and archives, shall be transferred to the Internal Control Organ of the Anticorruption and Good Governance Secretariat within twenty working days following its entry into force, and shall be processed and resolved by said organ in accordance with the legal provisions in force at the time of its commencement.

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

The Transfer Committee will be in effect for a period of 30 calendar days, in which its members will participate with the various competent authorities to receive the matters indicated in the aforementioned transitory provisions and to carry out the other actions deemed necessary for such purposes.

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

Until such time as the legislatures of the corresponding federal entities harmonize their legal framework in matters of access to public information in terms of the provisions of the Fourth transitory provision of the Decree by which various provisions of the Political Constitution of the United Mexican States are amended, added and repealed, in matters of organic simplification, published in the Official Gazette of the Federation on December 20, 2024, the head of the local executive branch in question shall be a member of the Council of the National System of Access to Public Information.

**Seventeenth.-** The head of the Executive Secretariat of the Council of the National System of Access to Public Information shall propose the rules of operation and functioning set forth 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 control and discipline body of the Judicial Branch; the internal control bodies of the autonomous constitutional bodies; the internal comptrollers of the Congress of the Union; the National Electoral Institute; the Federal Center for Labor Conciliation and Registration and the Federal Court of Conciliation and Arbitration must make the necessary adjustments to their internal regulations to comply with the provisions of this Decree within a maximum period of thirty calendar days from the date of entry into force of this Decree.

For purposes of the provisions of this transitory provision, each and every one of the formalities, procedures and other means of challenge, established in this instrument and other applicable regulations, are suspended for a period of ninety calendar days from the entry into force of this Decree, with the exception of the receipt and handling of requests for information that are processed through the National Transparency Platform by the authorities mentioned in the preceding paragraph.

**Nineteenth.-** Until such time as the legislatures of the federative entities issue legislation to harmonize their legal framework in accordance with this Decree, the guarantor agencies of such entities will continue to operate and perform the duties conferred to the local guarantor authorities, as well as to the bodies in charge of the internal comptroller or homologous bodies of the legislative and judicial branches, as well as the autonomous constitutional bodies of the federative entities themselves in this Law.

**Twentieth.-** The Judiciary of the Federation shall set up District Courts and Collegiate Circuit Courts specialized in matters of access to public information and protection of personal data, within a term of no more than one hundred and twenty calendar days as of the entry into force of this Decree, to which the amparo proceedings in such matters that are being processed for their resolution shall be referred.

For purposes of the provisions of this transitory provision, the terms and procedural terms of the amparo proceedings in matters of access to public information and protection of personal data that are being processed before District Courts and Collegiate Circuit Courts are suspended for a period of one hundred and eighty calendar days as of the entry into force of this Decree.

Mexico City, March 20, 2025.- Sen. Imelda Castro Castro Castro, Vice President.- Dip. Sergio Carlos Gutiérrez Luna, President.- Sen. Verónica Noemí Camino Farjat, Secretary.- Dip. José Luis Montalvo Luna, Secretary.- Rubrics**".**

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 hereby issue this Decree in the Residence of the Federal Executive Power, in Mexico City, on March 20, 2025.- **Claudia Sheinbaum Pardo**, President of the United Mexican States.- Rubric.- Lcda. **Rosa Icela Rodríguez Velázquez**, Secretary of the Interior.- Rubric.