



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

New DOF Law 20-03-2025

# FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA IN POSSESSION OF THE PRIVATE

## 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 OF PERSONAL DATA IN POSSESSION OF PRIVATE PARTIES; AND ARTICLE 37, SECTION XV, IS AMENDED THE ORGANIC LAW OF THE FEDERAL PUBLIC ADMINISTRATION**

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

**Article Three.-** The Federal Law on the Protection of Personal Data Held by Private Parties is hereby **issued**, to be as follows:

## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

### Chapter I

#### General Provisions

**Article 1.** This Law is of public order and of general observance throughout the national territory and aims to protect personal data held by individuals, with the aim of regulating their legitimate, controlled and informed processing, in order to guarantee privacy and the right to informational self-determination of individuals.

The following are exempt from the application of this Law:

- I. Credit information companies in the cases of the Law to Regulate Credit Information Companies Credit Information and other applicable provisions, and
- II. Persons who carry out the collection and storage of personal data, for exclusively 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 person who owns the information in physical, electronic or any other format generated by the controller, from the moment in which their personal data is collected, with the purpose of informing them of the purposes of the processing of said data, in accordance with article 14 of this Law;
- II. **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 their creation, type of support, processing, storage and organization;
- III. **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 expires. During this period, personal data may not be processed, and once this period has elapsed, they will be deleted from the corresponding database;



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

New DOF Law 20-03-2025

- IV. **Consent:** Manifestation of the free, specific and informed will of the person who owns the data through which the processing of the same is carried out;
- V. **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;
- WE. **Sensitive personal data:** Personal data that affects the most intimate sphere of the data subject, or whose improper use may give rise to discrimination or pose a serious risk to the data subject. 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.
- 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 nor, due to their structure, content or degree of disaggregation, allow their identification;
- X. **Publicly accessible source:** Those databases, systems, or files that, by law, may be publicly consulted when there is no impediment due to a restrictive rule, and with no requirement other 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 established by this Law and other applicable legal provisions;
- XI. **Law:** Federal Law on the Protection of Personal Data Held by Private Parties;
- XII. **Data Controller:** Natural or legal person who alone or jointly with others processes personal data on behalf of the controller;
- XIII. **Regulation:** Regulation of the Federal Law on the Protection of Personal Data Held by Private Parties;
- XIV. **Responsible:** Regulated subjects referred to in section XVI of this article;
- XV. **Secretariat:** Anti-Corruption and Good Government Secretariat;
- XVI. **Regulated subjects:** Private individuals or legal entities that carry out the processing of personal data;
- XVII. **Third:** Natural or legal person, national or foreign, other than the owner or the person responsible for the data;
- XVIII. **Holder:** Person to whom the personal data correspond;
- XIX. **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
- XX. **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 of the processing.

**Article 3.** The principles and rights provided for in this Law shall be limited, in terms of their observance and exercise, by the protection of national security, public order, safety and health, as well as the rights of third parties.

**Article 4.** In the absence of an express provision in this Law, the provisions of the Federal Code of Civil Procedure and the Federal Law of Administrative Procedure.

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

### Chapter II

#### Principles of Personal Data Protection



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

New DOF Law 20-03-2025

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

**Article 6.** Personal data must be collected and processed lawfully in accordance with the provisions of this Law and other applicable legal provisions.

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, understood as the trust that any person places in another, that the personal data provided will be processed in accordance with their agreement under the terms established by this Law.

**Article 7.** All 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 expressed expressly or tacitly. Express consent shall be deemed to be expressed when the data subject's wishes are 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.

Financial or asset data will require the express consent of the owner, 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 must establish the mechanisms and procedures for doing so in the privacy notice.

**Article 8.** In the case of sensitive personal data, the data controller must obtain the express written consent of the data subject for its processing, through his or her handwritten signature, electronic signature, or any other authentication mechanism established for this purpose.

Databases containing sensitive personal data may not be created without justification for their creation for legitimate, specific purposes consistent with the activities or explicit purposes pursued by the regulated entity.

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

- I. A legal provision so provides;
- II. Personal data are contained in publicly accessible sources;
- III. Personal data are subject to a prior dissociation procedure;
- IV. 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. There is an emergency situation that could potentially harm an individual in person or property;
- VI. The personal data are essential to carry out treatment for medical care, prevention, diagnosis, provision of health care, or management of health services, while the data subject is not in a position to give consent, in the terms established by the General Health Law and other applicable legal provisions and that said data processing is carried out by a person subject to professional secrecy or equivalent obligation, or
- VII. There is a well-founded and reasoned court order, resolution or mandate from a competent authority.

**Article 10.** The person responsible shall ensure that the personal data contained in the databases are accurate, complete, correct and up-to-date for the purposes for which they were collected.



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

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

The data controller shall be obliged to delete data relating to breaches of contractual obligations after a period of seventy-two months has elapsed, counting from the calendar date on which the breach occurred.

**Article 11.** The processing of personal data must be limited to fulfilling the purposes set forth in the privacy notice. However, if the data controller intends to process the data for a purpose other than those established in the privacy notice, the data subject's consent must be obtained again.

**Article 12.** The processing of personal data will be that which is necessary, adequate and relevant in relation to the purposes set forth in the privacy notice. For sensitive personal data, the controller must make reasonable efforts to limit the processing period to 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 their implementation, 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 the data subject has a legal relationship.

**Article 14.** The data controller shall be obligated to 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.

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

- I. The identity and address of the person responsible;
- II. The personal data that will be processed, 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 that the controller offers to the data subjects to limit the use or disclosure of the data;
- V. The mechanisms, means and procedures to exercise ARCO rights, in accordance with the provisions of this Law, and
- WE. The procedure and means by which the controller will notify the data subjects of changes to the privacy notice, in accordance with the provisions of this Law.

**Article 16.** The person responsible must make the privacy notice available to the owners, through printed, digital, visual, audio or any other technology formats as follows:

- I. When personal data is obtained in person through printed forms, it must be disclosed at that time, unless notice has been provided in advance, and
- II. When personal data is obtained by any electronic, optical, audio, visual, or other technological means, it must be provided in a simplified form, which must contain at least the information referred to in sections I to IV of the previous article, and indicate the site where the full privacy notice can be consulted.

**Article 17.** When the data has not been obtained directly from the owner, the person responsible must inform you of the change in the privacy notice.

The provisions of the previous paragraph do not apply when the processing is for historical purposes, statisticians or scientists.

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



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

New DOF Law 20-03-2025

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

Data controllers will not adopt lesser security measures than those they maintain for the management of their information. Furthermore, the existing risk, the potential consequences for data subjects, the sensitivity of the data, and technological developments will be taken into account.

**Article 19.** Any security breaches occurring at any stage of personal data processing that significantly affect the property or moral rights of the data subjects shall be immediately reported by the data controller, so that appropriate measures can be taken to defend their rights.

**Article 20.** The controller or third party must establish controls or mechanisms to ensure that all persons involved in any phase of personal data processing maintain confidentiality regarding such data, an obligation that will continue to exist even after their relationship with the controller or third party has ended.

### Chapter III

#### On the Rights of Personal Data Holders

**Article 21.** Any owner or, where appropriate, their legal representative, may exercise 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 any other.

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

**Article 22.** Data subjects shall have the right to access their personal data held by the data controller, as well as to know the information related to the conditions and generalities of their processing, through the privacy notice.

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

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

The cancellation of personal data will result in a blocking period, after which the data will be deleted. The data controller may retain it exclusively for the purposes of any responsibilities arising from the processing.

The blocking period will be equivalent to the statute of limitations for actions arising from the legal relationship underlying the processing, in accordance with the applicable law. Once the data has been cancelled, the data subject will be notified.

When personal data has been transmitted prior to the rectification or erasure date and continues to be processed by third parties, the data controller must inform them of this rectification or erasure request so that they can also proceed with it.

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

- I. It refers to the parts of a private, social or administrative contract and is necessary for its development and fulfillment;
- II. They must be treated by legal provision;
- III. Obstruct judicial or administrative proceedings related to tax obligations, the investigation and prosecution of crimes, or the updating of administrative sanctions;
- IV. They are necessary to protect the legally protected interests of the owner;



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

New DOF Law 20-03-2025

- V. They are necessary to carry out an action in the public interest;
- WE. They are necessary to comply with an obligation legally acquired by the holder, and
- VII. They are subject to treatment for prevention or medical diagnosis or the management of health services, provided that said treatment 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 oppose the processing.  
of your data or demand that it be stopped when:

- I. There is a legitimate cause and your specific situation requires it, which must justify that even if the treatment is lawful, it must cease to prevent its persistence from causing you harm or damage,  
the
- II. Your personal data may be subject to automated processing, which may produce unintended legal effects or significantly affect your interests, rights or freedoms, and which is intended to evaluate, without human intervention, certain personal aspects of your data or to analyze or predict, in particular, your professional performance, economic situation, health status, sexual preferences, reliability or behavior.

The right to object will not be exercised in cases where processing is necessary.  
for the fulfillment of a legal obligation imposed on the controller.

### Chapter IV

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

**Article 27.** The owner or his legal representative may request the responsible party at any time to exercise of ARCO rights, with respect to personal data that concerns you.

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

- I. The name of the holder and his/her address or any other means to receive notifications;
- II. Documents that prove the identity of the holder or, where applicable, the personality and identity of his or her representative;
- III. 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;
- IV. The description of the ARCO right that is intended to be exercised, or what the holder requests, 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 personal data person or department to process requests from data subjects for the exercise of the rights referred to in this Law.

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

**Article 31.** The data controller shall inform the data subject, within a maximum period of twenty days from the date on which the request for the exercise of ARCO rights was received, of the decision adopted, so that, if appropriate, it may be implemented within fifteen days following the date on which the response is communicated. In the case of requests to exercise the right of access to personal data, delivery shall be made upon verification of the identity of the data subject or legal representative, as appropriate.

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

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



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

In the event that the data subject requests access to the data from a person presumed to be the data controller and this person turns out not to be the data controller, it will be sufficient to notify the data subject by any of the means referred to in the previous paragraph, in order for the request to be considered fulfilled.

**Article 33.** The reasons in which the exercise of ARCO rights will not be admissible and therefore the responsible party may deny them are:

- I. When the owner or legal representative is not duly accredited to do so;
- II. When the personal data are not in the possession of the controller;
- III. When the rights of a third party are violated;
- IV. When there is a legal impediment, or a resolution from a competent authority, that restricts access to personal data, or does not allow rectification, cancellation or opposition thereof, 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 their representative are not met in any of the aforementioned cases, in which case the data controller will carry out the required access, rectification, cancellation or opposition.

In all of the above cases, the data controller must inform the data subject of the reason for their decision and notify the data subject, or, where applicable, the legal representative, within the established timeframes, using the same means used to submit the request for the exercise of ARCO rights, including, where applicable, any relevant evidence.

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

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

When the same data subject or their representative reiterates their request within a period of less than twelve months, the costs will not exceed three times the current Unit of Measurement and Update, unless there are substantial modifications to the privacy notice that motivate new inquiries.

### Chapter V

#### Data Transfer

**Article 35.** When the controller intends to transfer personal data to national or foreign third parties other than the person in charge, he or she must inform them of the privacy notice and the purposes to which the data subject subjected the processing.

Data processing will be carried out in accordance with the privacy notice, which will contain a clause indicating whether the data subject accepts or rejects the transfer of their data. Likewise, the third-party recipient will assume the same obligations as the data controller who transferred the data.

**Article 36.** National or international transfers of data may be carried out without the consent of the owner when they fall into any of the following situations:

- I. The transfer is provided for in a Law or Treaty to which Mexico is a party;
- II. The transfer is necessary for the prevention or diagnosis of medical conditions, 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 controller, or to a parent company or any company in the same group as the 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 to safeguard a public interest, or for the prosecution or administration of justice;



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

- WE. The transfer is necessary for the recognition, exercise or defense of a right in a judicial process, and
- VII. The transfer is necessary for the maintenance or fulfillment of a legal relationship between the controller and the owner.

### Chapter VI

#### On Self-Regulation

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

Self-regulation schemes may be translated into codes of ethics or good professional practice, trust seals, or other mechanisms, and will contain specific rules or standards that allow for the harmonization of data processing carried out by members and facilitate the exercise of data subjects' rights.

These schemes will be notified simultaneously to the corresponding authorities and to the Secretariat.

### Chapter VII

#### From the Secretariat

**Article 38.** For the purposes of this Law, the Secretariat shall have the purpose of disseminating knowledge of the right to the protection of personal data in Mexican society, promoting its exercise, and ensuring due observance of the provisions set forth in and derived from this Law, particularly those related to compliance with obligations by the entities regulated by this law.

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

- I. Monitor and verify compliance with the provisions contained in this Law, within the scope of its competence, with the exceptions provided for by law;
- II. Interpret this Law in the administrative sphere;
- III. Provide technical support to those responsible who request it, for the fulfillment of the obligations established in this Law;
- IV. Issue criteria and recommendations, in accordance with the applicable provisions of this Law, for the purposes 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 financial capabilities of the controller;
- WE. Know and resolve the procedures for the protection of rights and verification indicated in this Law and impose sanctions as appropriate;
- VII. Cooperate with other supervisory authorities and national and international bodies to assist in matters of data protection;
- VIII. Attend international forums within the scope of this Law;
- IX. Prepare privacy impact studies prior to the implementation of a new method of processing personal data or making substantial modifications to existing treatments;
- X. Disseminate knowledge of the obligations regarding the protection of personal data and provide training to obligated subjects, and
- XI. Any other powers conferred by this Law and other applicable regulations.

### Chapter VIII

#### From the Procedure for the Protection of Rights





## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

**Article 40.** The procedure shall be initiated at the request of the data subject or their legal representative, clearly stating the content of their claim and the provisions of this Law that are considered violated. The data protection request must be submitted to the Secretariat within fifteen days of the date on which the data controller communicates the response to the data subject.

If the data subject does not receive a response from the controller, the data protection request may be submitted after the response period established for the controller has expired. In this case, it will be sufficient for the data subject to accompany their data protection request with a document proving the date on which they submitted the request for access, rectification, erasure, or objection.

The data protection request will also proceed under the same terms when the data controller does not provide the data subject with the requested personal data, or does so in an incomprehensible format, refuses to make modifications or corrections to the personal data, or the data subject does not agree with the information provided because they consider it to be incomplete or does not correspond to the information requested.

Once the data protection request has been received by the Secretariat, it will be forwarded to the data controller so that, within fifteen days, they may issue a response, provide any evidence they deem relevant, and provide a written statement as appropriate for their rights.

The Secretariat will admit the evidence it deems relevant and proceed to present its case. It may also request any other evidence it deems necessary from the responsible party. Once the presentation of evidence has been completed, the Secretariat will notify the responsible party of their right to submit their arguments, if deemed necessary, within five days of notification.

To properly conduct the proceedings, the Secretariat will decide on the data protection request submitted after analyzing the evidence and other elements of conviction it deems relevant, such as those arising from the hearing(s) held with the parties.

The Regulations of the Law will establish the form, terms and deadlines according to which the rights protection procedure will be developed.

**Article 41.** The request for data protection may be submitted in writing or through the formats of the electronic system provided for this purpose by the Secretariat and must contain the following information:

- I. The name of the owner or, where applicable, that of his or her legal representative, as well as the interested third party, if any;
- II. The name of the person responsible for the request to access, rectify, cancel or oppose personal data;
- III. The address for hearing and receiving notifications;
- IV. The date on which the response from the responsible party was made known to the party, unless the procedure is initiated based on the provisions of Article 45 of this Law;
- V. The acts that motivate your request for data protection, and
- WE. Any other elements that are deemed appropriate to be brought to the attention of the Secretariat.

The manner and terms in which the identity of the holder or legal representative must be accredited shall be established in the Regulations.

Likewise, the data protection request must be accompanied by the request and the response being appealed or, where applicable, data that allows for your identification.

In the event of a lack of response, it will only be necessary to submit the application.

In the event that the data protection request is submitted through means other than electronic means, must be accompanied by sufficient transfer copies.



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

**Article 42.** The maximum period for issuing a decision in the data protection procedure shall be fifty days, counted from the date of submission of the data protection application. Where there is justified cause, the Secretariat may extend this period once and for up to an equal period.

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

**Article 44.** If the data protection request does not meet any of the requirements referred to in Article 41 of this Law, and the Secretariat does not have the necessary means to remedy the situation, the data subject shall be notified, within twenty days following the submission of the data protection request, on a single occasion, to remedy the omissions within a period of five days. If this period elapses without addressing the request, the data protection request shall be deemed not to have been submitted. The notification shall interrupt the period the Secretariat has to resolve the data protection request.

**Article 45.** The Secretariat shall remedy any deficiencies in the complaint where required, provided that it does not alter the original content of the request for access, rectification, cancellation, or opposition to personal data, nor modify the facts or requests set forth in the complaint or in the data protection request.

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

- I. Dismiss or dismiss the data protection request as inadmissible;
- II. Confirm, revoke or modify the response of the person responsible, or
- III. Order the delivery of personal data, in case of omission by the controller.

**Article 47.** The data protection request will be rejected as inadmissible when:

- I. The Secretariat is not competent;
- II. The holder or his representative does not duly prove his identity and personality of the latter;
- III. The Secretariat has previously heard the data protection request against the same act and made a final decision regarding the same appellant;
- IV. Any appeal or means of defense filed by the owner or, where appropriate, by the interested third party, against the contested act before the competent courts is being processed. Secretariat;
- V. It is an offensive or unreasonable data protection request, or
- WE. It is untimely because the period established in article 40 of this Law has elapsed.

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

- I. The title holder dies;
- II. The holder expressly withdraws;
- III. Once the data protection request has been admitted, a cause for inadmissibility arises, and
- IV. For whatever reason, it becomes void of substance.

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

If a conciliation agreement is reached between both parties, it will be recorded in writing and will have effect. binding. The data protection request will be void, and the Secretariat will verify compliance with the respective agreement.

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



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

**Article 50.** Once a data protection request has been submitted due to the lack of a response to a request in exercise of ARCO rights by the data controller, the Secretariat will notify the aforementioned data controller so that, within a period of no more than ten days, they may prove that they have responded in a timely manner to the request, or otherwise respond to it.  
If the response meets the request, the data protection request will be deemed inadmissible and the Secretariat must 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 person in charge referred to in the previous paragraph.

If the resolution of the Secretariat referred to in the previous paragraph determines the admissibility of the request, the responsible party will proceed with its fulfillment, at no cost to the owner, and the responsible party must cover all costs generated by the corresponding reproduction and shipping costs.

**Article 51.** Individuals may file an amparo suit against the Secretariat's resolutions. Amparo suits 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 resolutions of the Secretariat may be publicly disseminated in public versions, eliminating any references to the data subject that identify him or make him identifiable.

**Article 53.** Title holders who consider that they have suffered damage or injury to their property or rights as a result of non-compliance with the provisions of this Law by the responsible party or the person in charge, may exercise the rights they deem pertinent for the purposes of the appropriate compensation, in accordance with the corresponding legal provisions.

### Chapter IX

#### From the Verification Procedure

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

Ex officio verification will be carried out when there is non-compliance with resolutions issued in connection with procedures for the protection of rights referred to in the previous Chapter or when there is a well-founded and reasoned presumption of violations of this Law.

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

Public servants will be obliged to maintain confidentiality regarding the information they provide.  
know derived from the corresponding verification.

The Regulations shall develop the form, terms and deadlines under which the procedure referred to in this article will be carried out.

### Chapter X

#### From the Procedure for Imposition of Sanctions

**Article 56.** If, in the course of the rights protection procedure or the verification procedure carried out by the Secretariat, it becomes aware of a presumed non-compliance with any of the principles or provisions of this Law, it shall initiate the procedure for imposing sanctions.

**Article 57.** The procedure for imposing sanctions shall begin with the Secretariat notifying the alleged offender of the facts that led to the initiation of the procedure. The alleged offender shall be granted a period of fifteen days to provide evidence and submit written representations as appropriate. If the alleged offender fails to provide such evidence, the Secretariat shall decide based on the evidence at its disposal.

The Secretariat will admit the evidence it deems relevant and proceed to present its case. It may also request any other evidence it deems necessary from the alleged offender. Once the presentation of evidence has been completed, the Secretariat will notify the alleged offender of their right to present their arguments, if deemed necessary, within five days of notification.



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

The Secretariat, after analyzing the evidence and other elements of conviction it deems relevant, will make a final decision within fifty days of the date on which the sanctioning procedure began.

This resolution must 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 Regulation will develop the form, terms and deadlines in which the procedure for imposing taxes will be carried out. sanctions, including the presentation of evidence and arguments, the holding of hearings and the closure of investigations.

### Chapter XI

#### Of Infractions and Sanctions

**Article 58.** The following constitute violations of this Law:

- I. Failure to comply with the request for the exercise of the ARCO rights of the holder, without justified reason, in the terms provided for in this Law;
- II. Acting with negligence or fraud during the processing of requests for the exercise of ARCO rights;
- III. Deliberately declaring the non-existence of personal data, when it exists in whole or in part in the databases of the controller;
- IV. Processing personal data in violation of the principles set forth in this document Law;
- V. Omit in the privacy notice, some or all of the elements referred to in article 15 of this Law;
- WE. Maintaining inaccurate personal data when it is attributable to the controller, or failing to make the necessary corrections or cancellations 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 data processing, without observing the provisions of Article 11 of this Law;
- X. Transferring data to third parties without informing them of the privacy notice containing the limitations to which the data subject subjected the disclosure of the data;
- XI. Violating the security of databases, premises, programs or equipment, when it is attributable to the person responsible;
- XII. Carry out the transfer or assignment of personal data, except in cases where it is permitted by law;
- XIII. Collect or transfer personal data without the express consent of the data subject, in cases where this is required;
- XIV. Obstructing the acts of verification of the authority;
- XV. Collecting data in a deceptive and fraudulent manner;
- XVI. Continue with the illegitimate use of personal data when the cessation of the same has been requested by the Secretariat or the persons in charge;
- XVII. Process personal data in a manner that affects or impedes the exercise of ARCO rights established in Article 16 of the Political Constitution of the United Mexican States;
- XVIII. Create databases in violation of the provisions of article 8, second paragraph of this Law, and
- XIX. Any failure by the responsible party to comply with the obligations established under this Law.

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



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

- I. The warning for the responsible party to carry out the acts requested by the owner, in the terms provided by this Law, in the case of the cases provided for in section I of the previous article;
- II. Fine of 100 to 160,000 times the Unit of Measurement and Update, in the cases provided for in sections II to VII of the previous article;
- III. A fine of 200 to 320,000 times the Unit of Measurement and Update, in the cases provided for in sections VIII to XVIII of the previous article, and
- IV. If the violations cited in the preceding paragraphs persist repeatedly, an additional fine ranging from 100 to 320,000 times the Unit of Measurement and Update will be imposed. In the case of violations committed in the processing of sensitive data, the penalties may be increased up to twice the established amounts.

**Article 60.** The Secretariat shall base and justify its resolutions, considering:

- I. The nature of the data;
- II. The notorious inappropriateness of the responsible party's refusal to carry out the acts requested by the owner, in terms of this Law;
- III. The intentional or unintentional nature of the action or omission constituting the infringement;
- IV. The financial capacity of the person responsible, and
- V. Recidivism.

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

### Chapter XII

#### Crimes related to the Improper Processing of Personal Data

**Article 62.** Anyone who is authorized to process data shall be sentenced to three months to three years in prison. personal, for profit, causes a security breach to the databases under their custody.

**Article 63.** Anyone who, for the purpose of obtaining undue profit, processes personal data by deception, taking advantage of an error in the data subject's mind or the person authorized to transmit it, shall be punished with imprisonment of six months to five years.

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

**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 come into force when the Federal Economic Competition Commission and the Federal Institute of Economic Competition are extinguished.



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

New DOF Law 20-03-2025

Telecommunications in accordance with the provisions of the Tenth and Eleventh Transitional Provisions 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.

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 Protection of Personal Data 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.



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

New DOF Law 20-03-2025

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 must 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 of 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.



## FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE INDIVIDUALS

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

*New DOF Law 20-03-2025*

**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 said matters that are being processed shall be referred for resolution.

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 this Decree comes into force.

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. - **Rosa Icela Rodríguez Velázquez**, Secretary of the Interior.

Rubric.