

---

**EXECUTIVE BRANCH**  
**MINISTRY OF THE INTERIOR**

---

**DECREE issuing the Federal Law on Protection of Personal Data Held by Private Parties and amending Article 3, sections ii and vii, and Article 33, as well as the title of Chapter II of Title II of the Federal Law on Transparency and Access to Public Government Information.**

---

In the margin a seal with the national emblem, which reads: United Mexican States – Office of the President of the Republic.

**FELIPE DE JESÚS CALDERÓN HINOJOSA**, President of the United Mexican States, to its inhabitants; be it known:

That the Honorable Congress of the Union has sent me the following

**DECREE**

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

**THE FEDERAL LAW ON PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES IS ISSUED AND ARTICLE 3, SECTIONS II AND VII, AND ARTICLE 33, AS WELL AS THE TITLE OF CHAPTER II OF TITLE II OF THE FEDERAL LAW ON TRANSPARENCY AND ACCESS TO PUBLIC GOVERNMENT INFORMATION ARE AMENDED.**

**ARTICLE ONE.** The Federal Law on Protection of Personal Data held by Private Parties is issued.

**FEDERAL LAW ON PROTECTION OF PERSONAL DATA  
HELD BY PRIVATE PARTIES**

**CHAPTER I**

**General Provisions**

Article 1. This Law is of a public order and of general observance throughout the Republic, and has the purpose of protecting personal data held by private parties, in order to regulate its legitimate, controlled and informed processing, to ensure the privacy and the right to informational self-determination of individuals.

Article 2. The parties regulated under this Law are private parties, whether individuals or private legal entities, that process personal data, with the exception of:

- I. Credit reporting companies under the Law Regulating Credit Reporting Companies and other applicable laws, and
- II. Persons carrying out the collection and storage of personal data that is exclusively for personal use, and without purposes of disclosure or commercial use.

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

- I. Privacy Notice: Document in physical, electronic or any other format, generated by the data controller, that is made available to the data owner prior to the processing of his personal data, in accordance with Article 15 of this Law.
- II. Database: The ordered set of personal data concerning an identified or identifiable individual.
- III. Blocking: The labeling and retention of personal data once it has served the purpose for which it was collected, with the sole purpose of determining possible responsibilities in relation to its processing, until the end of the legal or contractual limitation period of said responsibilities. During this period, personal data may not be processed, and, once the period has ended, the data will be cancelled in the relevant database.
- IV. Consent: Expression of the will of the data owner by which data processing is enabled.
- V. Personal data: Any information concerning an identified or identifiable individual.
- VI. Sensitive personal data: Personal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs,

- union membership, political views, sexual preference.
- VII. Days: Working days.
- VIII. Dissociation: The procedure through which personal data cannot be associated with the data owner nor allow, by way of its structure, content or degree of disaggregation, identification thereof.
- IX. Data processor: The individual or legal entity that, alone or jointly with others, processes personal data on behalf of the data controller.
- X. Publicly available source: Those databases on which queries can be made by any person, without any requirement except, where appropriate, payment of a fee, in accordance with the Regulations to this Law.
- XI. Institute: Federal Institute for Access to Information and Data Protection, referred to in the Federal Law on Transparency and Access to Public Government Information.
- XII. Law: Federal Law on Protection of Personal Data Held by Private Parties.
- XIII. Regulations: The Regulations to the Federal Law on Protection of Personal Data Held by Private Parties.
- XIV. Data controller: Individual or private legal entity that decides on the processing of personal data.
- XV. Ministry: Ministry of Economy.
- XVI. Third party: Mexican or foreign individual or legal entity other than the data owner or data controller.
- XVII. Data owner: The individual to whom personal data relates.
- XVIII. Processing: Retrieval, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data.
- XIX. Transfer: Any data communication made to a person other than the data controller or data processor.

Article 4. The principles and rights under this Law will have, as a limit with regard to their observance and exercise, protection of national security, public order, health and safety as well as the rights of third parties.

Article 5. Where not expressly provided in this Law, the provisions of the Federal Code of Civil Procedure and the Federal Administrative Procedure Law will apply supplementarily.

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

## CHAPTER II

### Principles of Personal Data Protection

Article 6. Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law.

Article 7. Personal data must be collected and processed in a lawful manner in accordance with the provisions established by this Law and other applicable regulations.

Personal data must not be obtained through deceptive or fraudulent means.

In all processing of personal data, it is presumed that there is a reasonable expectation of privacy, understood as the trust any one person places in another for personal data provided to be treated pursuant to any agreement of the parties in the terms established by this Law.

Article 8. All processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law.

Consent will be express when such is communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications.

It will be understood that the data owner tacitly consents to the processing of his data when, once the privacy notice has been made available to him, he does not express objection.

Financial or asset data will require the express consent of the data owner, except as provided in Articles 10 and 37 of this Law.

Consent may be revoked at any time without retroactive effects being attributed thereto. For revocation of consent, the data controller must, in the privacy notice, establish the mechanisms and procedures for such action.

Article 9. In the case of sensitive personal data, the data controller must obtain express written consent from the data owner for processing, through said data owner's signature, electronic signature, or any authentication mechanism established for such a purpose.

Databases containing sensitive personal data may not be created without justification of their creation for purposes that are legitimate, concrete and consistent with the explicit objectives or activities pursued by the regulated party.

Article 10. Consent for processing of personal data will not be necessary where:

- I. Any Law so provides;
- II. The data is contained in publicly available sources;
- III. The personal data is subject to a prior dissociation procedure;
- IV. It has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller;
- V. There is an emergency situation that could potentially harm an individual in his person or property;
- VI. It is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data owner is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or
- VII. A resolution is issued by a competent authority.

Article 11. The data controller shall ensure that personal data contained in databases is relevant, correct and up-to-date for the purposes for which it has been collected.

When the personal data is no longer necessary for the fulfillment of the objectives set forth in the privacy notice and applicable law, it must be cancelled.

The controller of the database will be required to remove information relating to nonperformance of contractual obligations, after a period of seventy-two months counted from the calendar day on which said nonperformance arose.

Article 12. Processing of personal data must be limited to fulfillment of the purposes set out in the privacy notice. If the data controller intends to process data for another purpose which is not compatible or analogous to the purposes set out in the privacy notice, the data owner's consent must be obtained again.

Article 13. Processing of personal data will be done as necessary, appropriate and relevant with relation to the purposes set out in the privacy notice. In particular, for sensitive personal data, the data controller must make reasonable efforts to limit the processing period thereof to the minimum required.

Article 14. The data controller shall ensure compliance with the personal data protection principles established by this Law, and shall adopt all necessary measures for their application. The foregoing will apply even when this data has been processed by a third party at the request of the data controller. The data controller must take all necessary and sufficient action to ensure that the privacy notice given to the data owner is respected at all times by it or by any other parties with which it has any legal relationship.

Article 15. The data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice.

Article 16. The privacy notice must contain at least the following information:

- I. The identity and domicile of the data controller collecting the data;
- II. The purposes of the data processing;

- III. The options and means offered by the data controller to the data owners to limit the use or disclosure of data;
- IV. The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law;
- V. Where appropriate, the data transfers to be made, and
- VI. The procedure and means by which the data controller will notify the data owners of changes to the privacy notice, in accordance with the provisions of this Law.

For sensitive personal data, the privacy notice must expressly state that it is dealing with this type of data.

Article 17. The privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows:

- I. Where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior;
- II. Where personal data are obtained directly from the data owner by any electronic, optical, audio or visual means, or through any other technology, the data controller must immediately provide the data owner with at least the information referred to in sections I and II of the preceding article, as well as provide the mechanisms for the data owner to obtain the full text of the privacy notice.

Article 18. Where data has not been obtained directly from the data owner, the data controller must notify him of the change in the privacy notice.

The provisions of the preceding paragraph are not applicable where processing is done for historical, statistical or scientific purposes.

Where it is impossible to provide the privacy notice to the data owner or where disproportionate effort is involved considering the number of data owners, or the age of the data, with the authorization of the Institute, the data controller may implement compensatory measures in the terms of the Regulation for this Law.

Article 19. All responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing.

Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, risk involved, potential consequences for the data owners, sensitivity of the data, and technological development will be taken into account.

Article 20. Security breaches occurring at any stage of processing that materially affect the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights.

Article 21. The data controller or third parties involved in any stage of personal data processing must maintain confidentiality with respect to such data, and this obligation will continue even after the end of its/their relationship with the data owner or, as the case may be, with the data controller.

### CHAPTER III

#### Rights of Data Owners

Article 22. Any data owner, or, where appropriate, his legal representative, may exercise the rights of access, rectification, cancellation and objection under this Law. The exercise of any of these is not a prerequisite nor does it impede the exercise of another. Personal data must be preserved in such a way as to allow the exercise of these rights without delay.

Article 23. Data owners will have the right to access their personal data held by the data controller as well as to be informed of the privacy notice to which processing is subject.

Article 24. The data owner will have the right to rectify data if it is inaccurate or incomplete.

Article 25. The data owner will at all times have the right to cancel his personal data.

Cancellation of personal data will lead to a blocking period following which the data will be erased. The data controller may retain data exclusively for purposes pertaining to responsibilities arising from processing. The blocking period will be equal to the limitation period for actions arising from the legal relationship governing processing pursuant to applicable law.

Once the data is cancelled, the data owner will be notified.

Where personal data has been transmitted prior to the date of rectification or cancellation and continues to be processed by third parties, the data controller must notify them of the request for rectification or cancellation, so that such third parties also carry it out.

Article 26. The data controller will not be obligated to cancel personal data when:

- I. It relates to the parties of a private or administrative contract or partnership agreement and is necessary for its performance and enforcement;
- II. The law requires that it be processed;
- III. Such action hinders judicial or administrative proceedings relating to tax obligations, investigation and prosecution of crimes, or updating of administrative sanctions;
- IV. It is necessary to protect the legally protected interests of the data owner;
- V. It is necessary to carry out an action in the public interest;
- VI. It is necessary to fulfill an obligation legally undertaken by the data owner, and
- VII. It is subject to processing for medical diagnosis or prevention or health services management, provided such processing is done by a health professional subject to a duty of secrecy.

Article 27. Data owners will, at all times and for any legitimate reason, have the right to object to the processing of their data. Where appropriate, the data controller may not process such data owner's data.

#### **CHAPTER IV Exercise of Rights of Access, Rectification, Cancellation and Objection**

Article 28. The data owner or his legal representative may at any time make a request to the data controller for access, rectification, cancellation or objection in relation to the personal data concerning him.

Article 29. The access, rectification, cancellation or objection request must include the following:

- I. The data owner's name and address or other means to notify him of the response to his request;
- II. Documents establishing the identity or, where appropriate, legal representation of the data owner;
- III. A clear and precise description of the personal data with regard to which the data owner seeks to exercise any of the abovementioned rights.
- IV. Any other item or document that facilitates locating the personal data.

Article 30. All data controllers must designate a personal data person or department who will process requests from data owners for the exercise of the rights referred to in this Law. In addition, data controllers will promote protection of personal data within their organizations.

Article 31. In the case of requests for rectification of personal data, the data owner must indicate, in addition to that which is specified in the preceding article of this Law, the changes to be made, and provide documentation supporting the request.

Article 32. The data controller will notify the data owner, within a maximum of twenty days counted from the date of receipt of the request for access, rectification, cancellation or objection, of the determination made, so that, where appropriate, same will become effective within fifteen days from the date on which the notice is provided. For personal data access requests, delivery will be made upon proof of identity of the requesting party or legal representative.

The aforementioned time periods may be extended a single time by a period of equal length, provided that such action is justified by the circumstances of the case.

Article 33. The obligation to provide access to information will be fulfilled when the personal data is made

available to the data owner; or, by issuing uncertified copies, electronic documents or any other means established by the data controller in the privacy notice.

In the event that the data owner requests access to data from a person or entity who he presumes is the data controller and said person or entity proves not to be such, it will be sufficient for said person or entity to so indicate to the data owner by any of the means referred to in the preceding paragraph, for the request to be considered properly fulfilled.

Article 34. The data controller may deny access to personal data or refuse the rectification, cancellation or objection with relation thereto in the following cases:

- I. Where the requesting party is not the subject of the personal data, or the legal representative is not duly accredited for such purposes;
- II. Where the requesting party's personal data is not found in the data controller's database;
- III. Where the rights of a third party are adversely affected;
- IV. Where there is any legal impediment, or decision of a competent authority, restricting access to the personal data or not allowing the rectification, cancellation or objection with relation thereto, and
- V. Where the rectification, cancellation or objection has been previously performed.

The refusal referred to in this article may be partial, in which case the data controller will carry out the access, rectification, cancellation or objection requested by the data owner.

In all of the aforementioned cases, the data controller must notify the data owner, or, as appropriate, his legal representative, of its decision and the reason for such decision, within the periods established for such purposes, via the same means by which the request was made, attaching, where appropriate, any relevant evidence.

Article 35. The action of providing personal data will be free, and the data owner must only pay justified expenses of shipping or the cost of copying or providing data in other formats.

This right will be exercised by the data owner free of charge, upon proof of his identity to the data controller. However, if the same person repeats his request within a period of twelve months, costs will not be greater than three days of the General Current Minimum Wage in Mexico City, unless there are material changes to the privacy notice that prompt new queries.

The data owner may file a data protection request due to the response received or lack of response from the data controller, in accordance with the provisions of the following Chapter.

## **CHAPTER V**

### **Data Transfer**

Article 36. Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing.

Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data.

Article 37. Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases:

- I. Where the transfer is pursuant to a Law or Treaty to which Mexico is party;
- II. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management;
- III. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies;
- IV. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party;

- V. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
- VI. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and
- VII. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner.

## **CHAPTER VI AUTHORITIES**

### **SECTION I**

#### **The Institute**

Article 38. The Institute, for the purposes of this Law, will have the purpose of disseminating information on the right to personal data protection in Mexican society, promoting its exercise, and overseeing the due observance of the provisions of this Law and those arising herefrom; particularly those related to the fulfillment of obligations by the parties regulated by this Law.

Article 39. The Institute has the following responsibilities:

- I. To oversee and verify compliance with the provisions of this Law, within the scope of its competence, with the exceptions provided by the law;
- II. To interpret this Law in the administrative system;
- III. To provide technical support to the data controllers who so request for fulfillment of the obligations established by this Law;
- IV. To issue opinions and recommendations in accordance with the applicable provisions of this Law, for purposes of its functions and operation;
- V. To disseminate international best practices and standards for information security, in view of the nature of the data, the processing purposes, and the technical and financial capacity of the data controller.
- VI. Hear and issue decisions in rights protection and verification procedures as set forth in this Law, and impose penalties as appropriate;
- VII. Cooperate with other domestic and international bodies and supervisory authorities, in order to assist in the area of data protection;
- VIII. Submit an annual activity report to the Mexican Congress;
- IX. Participate in international forums in the area of this Law;
- X. Carry out studies of the impact on privacy prior to the implementation of new types of processing of personal data or material modification of existing types of processing;
- XI. Develop, promote and disseminate analyses, studies and research in the area of protection of personal data held by third parties and provide training to the obligated parties, and
- XII. Any other responsibilities under this Law and other applicable laws.

### **SECTION II**

#### **Regulatory Authorities**

Article 40. This Law will constitute the regulatory framework to be observed by agencies, in the areas of their respective responsibilities, for issuance of appropriate regulations, with the cooperation of the Institute.

Article 41. The Ministry, for purposes of this Law, will have the function of disseminating information on obligations relating to the protection of personal data to domestic private enterprise and international private enterprise with business activity in Mexico; it will promote best business practices around protection of personal data as an input for the digital economy, and national economic development as a whole.

Article 42. With regard to business databases, the regulations issued by the Ministry will apply only to databases that are automated or are part of an automation process.

Article 43. The Ministry has the following responsibilities:

- I. To disseminate information regarding the protection of personal data in the business world;
- II. To promote good business practices in the area of personal data protection;
- III. To issue the relevant guidelines for the content and scope of privacy notices in cooperation with the Institute referred to in this Law;

- IV. To issue, within the scope of its competence, the general administrative provisions referred to in Article 40, in cooperation with the Institute;
- V. To establish the necessary parameters for the proper development of the self-regulatory mechanisms and measures referred to in Article 44 of this Law, including the promotion of Mexican Standards and Official Mexican Standards, in cooperation with the Institute;
- VI. To maintain consumer registries in the area of personal data and verify their proper operation;
- VII. To execute agreements with chambers of commerce, associations and business organizations in general, in the area of personal data protection;
- VIII. To design and implement policies and coordinate studies for the modernization and efficient operation of electronic commerce, as well as to promote the development of the digital economy and information technologies in the area of personal data protection;
- IX. To participate in domestic and international trade forums in the area of personal data protection, or in events of a commercial nature, and
- X. Support events that contribute to increased awareness on personal data protection.

Article 44. Individuals or legal entities may establish agreements amongst themselves and with domestic or foreign civil or governmental organizations on self-regulatory schemes on the subject, complementing the provisions of this Law. Such schemes must include mechanisms to measure their effectiveness in protecting data, consequences and effective corrective measures in the case of nonfulfillment.

Self-regulatory schemes may be translated into codes of ethics or good professional practice, trust seals or other mechanisms, and will contain specific rules or standards enabling harmonization of data processing performed by adherents and facilitation of the exercise of data owners' rights. Notification of such schemes will be made simultaneously to the relevant sectoral authorities and the Institute.

## CHAPTER VII

### Rights Protection Procedure

Article 45. The procedure will be initiated by request from the data owner or his legal representative, clearly stating the content of his claim and the provisions of this Law deemed violated. The data protection request must be submitted to the Institute within fifteen days from the date on which the response from the data controller is communicated to the data owner.

In the event that the data owner does not receive a response from the data controller, the data protection request may be filed after the deadline for the data controller response has passed. In this case, it will be sufficient for the data owner to accompany its data protection request with the document that proves the date on which he filed the request for access, rectification, cancellation or objection.

The data protection request will also be allowed under the same terms when the data controller does not deliver the requested personal data to the data owner, or delivers it in an incomprehensible form, refuses to make changes or corrections to personal data, or where the data owner is not satisfied with the information delivered since he considers it is incomplete or does not match the information requested.

Upon receipt of the data protection request by the Institute, said request will be sent to the data controller, for said controller to, within fifteen days, issue a response, provide any evidence it deems relevant and make its formal arguments in writing.

The Institute will admit any evidence it deems relevant and introduce it. It may also request any other evidence it deems necessary from the data controller. After introduction of evidence, the Institute will notify the data controller of its right to, if it so considers necessary, present its arguments within five days of notification.

As required under the procedure, the Institute will issue a decision on the data protection request filed, after analyzing the evidence and other elements of proof it deems appropriate, as may be those that arise from the hearing(s) held with the parties.

The Regulations to the Law will establish the manner, conditions and periods under which the rights protection procedure will be carried out.

Article 46. The data protection request may be filed in writing or using the electronic system forms provided by the Institute for such a purpose, and must contain the following information:

- I. The name of the data owner or, where applicable, his legal representative, as well as that of any third party to the request;



- II. The name of the data controller to whom the request for personal data access, rectification, cancellation or objection was sent;
- III. Address to hear and receive notifications;
- IV. The date on which the response from the data controller was received, except where the procedure begins pursuant to the provisions of Article 50;
- V. The acts giving rise to the data protection request, and
- VI. Any other items considered appropriate to bring to the attention of the Institute.

The manner and terms in which the identity of the data owner or, as the case may be, the legal representative, must be documented will be established in the Regulations.

Furthermore, the data protection request will include the request and response being challenged or, where appropriate, any information enabling its identification. Where there has been no response, it will only be necessary to submit the request.

Where the data protection request is filed through non-electronic means, it must include sufficient copies for notification.

Article 47. The decision in the rights protection procedure must be issued within fifty days counted from the date of filing of the data protection request. Where there is good cause, the Plenum of the Institute may extend this deadline a single time for a period of equal length.

Article 48. Where the protection of rights decision is in favor of the data owner, the data controller will be ordered to, within ten days of notification or, where warranted, a longer period as set out in the decision, carry out all action required in accordance with the exercise of the rights subject to protection, and it shall report compliance therewith in writing to the Institute within the following ten days.

Article 49. If the data protection request fails to satisfy any of the requirements specified in Article 46 of this Law, and where the Institute lacks the information to remedy such omissions, the data owner will be instructed, a single time, within twenty working days following the filing of the data protection request, to remedy the omissions within five days. If the instructions are not followed by the deadline, the data protection request will be considered not filed. The instructions will have the effect of interrupting the period allowed for the Institute to issue a decision on the data protection request.

Article 50. The Institute will remedy the deficiencies in the complaint where required, provided it does not alter the original content of the request for personal data access, rectification, cancellation or objection, nor modify the facts or petitions set out in the same or in the data protection request.

Article 51. The decisions of the Institute may:

- I. Dismiss or reject the data protection request as without merit or inadmissible, or
- II. Affirm, reverse or amend the response of the data controller.

Article 52. The data protection request will be rejected as without merit or inadmissible where:

- I. The Institute lacks jurisdiction;
- II. The Institute has already heard the data protection request for the same act and issued a final decision with regard to the same petitioner;
- III. Any petition or legal action filed by the data owner is pending before the competent courts that may have the effect of amending or revoking the act in question;
- IV. The data protection request is offensive or irrational, or
- V. It is filed late.

Article 53. The data protection request will be dismissed where:

- I. The data owner dies;
- II. The data owner expressly withdraws the petition;
- III. After admission of the data protection request, grounds for inadmissibility arise.
- IV. Same becomes moot for any reason.

Article 54. The Institute may, at any time in the procedure, seek conciliation between the data owner and the data controller.

If a conciliation agreement is reached between the two, it will be recorded in writing and will have binding effect. The data protection request will become moot and the Institute will verify fulfillment of the respective agreement.

For the purposes of conciliation referred to herein, the procedure established in the Regulations to this Law will be followed.

Article 55. Where a data protection request is filed upon lack of response by the data controller to a request in the exercise of the rights of access, rectification, cancellation or objection, the Institute will serve notice on said data controller to, within ten days, prove it has responded in a timely manner to the request, or respond to it. If the response satisfies the request, the data protection request will be considered without merit and the Institute must dismiss it.

In this latter case, the Institute will issue its decision based on the content of the original request and the response of the data controller referred to in the preceding paragraph.

If the decision of the Institute referred to in the preceding paragraph determines that the request has merit, the data controller will proceed to fulfill it, at no charge to the data owner, where the data controller must bear all costs generated by the corresponding reproduction.

Article 56. Private parties may file a petition for annulment against decisions issued by the Institute with the Federal Tax and Administrative Court.

Article 57. All decisions of the Institute may be publicly released in public versions, eliminating any references to the data owner which identify him or make him identifiable.

Article 58. Data owners who feel they have suffered harm or damage to their property or rights as a result of a breach of the provisions of this Law by the data controller or data processor, may exercise the rights they deem appropriate for purposes of any applicable indemnity, in the terms of the relevant law.

## **CHAPTER VIII**

### **Verification Procedure**

Article 59. The Institute will verify compliance with this Law and the regulations derived herefrom. Verification may be initiated of its own motion or by petition of an interested party.

Verification of its own motion will be carried out in the event of nonfulfillment of decisions issued in rights protection procedures as referred to in the preceding Chapter, or where the existence of violations of this Law is presumed grounded in law and fact.

Article 60. In the verification procedure, the Institute will have access to all information and documentation it deems necessary, in accordance with the respective decision.

Federal public servants will be obliged to observe confidentiality of the information they have access to as a result of the relevant verification.

The Regulations will describe the form, terms and periods for the procedure referred to in this article.

## **CHAPTER IX**

### **Penalty Application Procedure**

Article 61. If, by virtue of a rights protection procedure or verification procedure carried out by the Institute, the Institute becomes aware of a presumed breach of any of the principles or provisions of this Law, it will initiate the procedure referred to in this Chapter in order to determine the appropriate penalty.

Article 62. The penalty application procedure will begin with notice sent by the Institute to the alleged offender with regard to the facts that originated the procedure and will grant a period of fifteen days to present evidence and state formal arguments in writing. Where no evidence is presented, the Institute will arrive at a decision through the evidence at its disposal.

The Institute will admit evidence it deems relevant and introduce it. In addition, it may request any other evidence it deems necessary from the alleged offender. After introduction of evidence, the Institute will notify the alleged offender of its right to, if it so considers necessary, present its arguments within five days of notification.

The Institute, after analyzing the evidence and other elements of proof it deems relevant, will issue a final decision within fifty days after the date on which it initiated the penalty procedure. Notice of this decision must be given to the parties.

Where there is good cause, the Plenum of the Institute may extend this deadline a single time for a period of equal length.

The Regulations will describe the form, terms and periods for the penalty application procedure, including presentation of evidence and arguments, hearings and end of proceedings.

## **CHAPTER X**

### **Violations and Penalties**

Article 63. The following acts carried out by the data controller are violations of this Law:

- I. Failure to satisfy the data owner's request for personal data access, rectification, cancellation or objection without well-founded reason, in the terms of this Law;
- II. Acting negligently or fraudulently in processing and responding to requests for personal data access, rectification, cancellation or objection;
- III. Fraudulently declaring the inexistence of personal data where such exists in whole or in part in the databases of the data controller;
- IV. Processing personal data in violation of the principles established in this Law;
- V. Omitting, in the privacy notice, any or all of the items referred to in Article 16 of this Law;
- VI. Maintaining inaccurate personal data when such action is attributable to the data controller, or failing to perform legally due rectifications or cancellations where the data owner's rights are affected;
- VII. Failure to comply with the notice referred to in section I of Article 64;
- VIII. Breaching the duty of confidentiality established in Article 21 of this Law;
- IX. Materially changing the original data processing purpose, without observing the provisions of Article 12;
- X. Transferring data to third parties without providing them with the privacy notice containing the limitations to which the data owner has conditioned data disclosure;
- XI. Compromising the security of databases, sites, programs or equipment, where attributable to the data controller;
- XII. Carrying out the transfer or assignment of personal data outside of the cases where it is permitted under this Law;
- XIII. Collecting or transferring personal data without the express consent of the data owner, in the cases where this is required;
- XIV. Obstructing verification actions of the authority;
- XV. Collecting data in a deceptive and fraudulent manner;
- XVI. Continuing with the illegitimate use of personal data when the Institute or the data owners have requested such use be ended;
- XVII. Processing personal data in a way that affects or impedes the exercise of the rights of access, rectification, cancellation and objection set forth in Article 16 of the Political Constitution of the United Mexican States;
- XVIII. Creating databases in violation of the provisions of Article 9, second paragraph, of this Law, and
- XIX. Any breach by the data controller of the obligations pertaining thereto as established in the provisions of this Law.

Article 64. Violations of this Law will be punished by the Institute as follows:

- I. A warning instructing the data controller to carry out the actions requested by the data owner, under the terms established by this Law, in the cases described in section I of the preceding article;
- II. A fine from 100 to 160,000 days of the Mexico City minimum wage, in the cases described in sections II to VII of the preceding article;
- III. A fine from 200 to 320,000 days of the Mexico City minimum wage, in the cases described in sections VIII to XVIII of the preceding article; and
- IV. In the event of repeated occurrences of the violations described in the preceding paragraphs, an additional fine will be imposed from 100 to 320,000 days of the current Mexico City minimum wage. With regard to violations committed in processing sensitive data, sanctions may be increased up to double the established amounts.

Article 65. The Institute will ground its decisions in law and fact, considering:

- I. The nature of the data;
- II. The evident impropriety of the refusal of the data controller to perform the actions requested by the data owner in the terms of this Law;
- III. The intentional or unintentional nature of the action or omission constituting the violation;
- IV. The financial position of the data controller, and
- V. Recurrence.

Article 66. The penalties specified in this chapter will be imposed without prejudice to any applicable civil or criminal liability.

## CHAPTER XI

### Crimes Relating to Unlawful Processing of Personal Data

Article 67. Three months to three years imprisonment will be imposed on any person who, authorized to process personal data, for profit, causes a security breach affecting the databases under his custody.

Article 68. Six months to five years imprisonment will be imposed on any person who, with the aim of achieving unlawful profit, processes personal data deceitfully, taking advantage of an error of the data owner or the person authorized to transmit such data.

Article 69. With regard to sensitive personal data, the penalties referred to in this chapter will be doubled.

## TRANSITORY PROVISIONS

ONE. This Decree will take effect on the day following its publication in the Federal Official Gazette.

TWO. The Federal Executive will issue the Regulations to this Law within one year following its entry into force.

THREE. Data controllers shall designate the personal data person or department referred to in Article 30 of the Law, and shall issue their privacy notices to personal data owners in accordance with the provisions of articles 16 and 17 within one year after this Law enters into force.

FOUR. Data owners may exercise, with data controllers, their rights of access, rectification, cancellation and objection, as set forth in Chapter IV of this Law; they may also initiate, as necessary, the rights protection procedure established in Chapter VII hereof, eighteen months after the entry into force of the Law.

FIVE. Pursuant to the provisions of Transitory Article Three of the Decree, adding section XXIX-O to Article 73 of the Political Constitution of the United Mexican States, published in the Federal Official Gazette on April 30, 2009, local regulations regarding the protection of personal data held by private parties are annulled, and any other provisions contrary to this Law are repealed.

SIX. References made prior to the entry into force of this Decree by laws, treaties and international agreements, regulations and other bodies of law to the Federal Institute of Access to Public Information, in the future will be understood as made to the Federal Institute for Access to Information and Protection of Personal Data.

SEVEN. Actions that, pursuant to the provisions of the Federal Law on Protection of Personal Data held by Private Parties, are to be carried out by the Federal Executive, will be subject to the approved budgets of the institutions concerned and the provisions of the Federal Budget and Fiscal Responsibility Law.

EIGHT. The Expenditure Budget of the Federation for Fiscal Year 2011 includes items deemed sufficient for the proper functioning of the Federal Institute for Access to Information and Data Protection with respect to this Law.

ARTICLE TWO. Article 3 sections II and VII, and Article 33, as well as the title of Chapter II of Title II of the Federal Law on Transparency and Access to Public Government Information are amended, to read as follows:

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

I...

II. Personal data: Any information concerning an identified or identifiable individual.

III to VI...

VII. Institute: The Federal Institute for Access to Information and Data Protection, established in Article 33 of this Law;

VIII to XV...

## CHAPTER II

### The Institute

**Article 33.** The **Institute** is a body of the Federal Public Administration, with operational, budgetary and decision-making autonomy, responsible for promoting and disseminating information regarding the exercise of the right to information, resolving on refusal of information access requests, and protecting personal data held by agencies and entities.

## TRANSITORY PROVISIONS

**SOLE PROVISION.** This Decree will take effect on the day following its publication in the Federal Official Gazette.

Mexico City, April 27, 2010. Deputy **Francisco Javier Ramirez Acuña**, Chair. Sen. **Carlos Navarrete Ruiz**, Chair. Deputy **Georgina Trujillo Zentella**, Secretary. Sen. **Renán Cleominio Zoreda Novelo**, Secretary. Signatures."

Pursuant to the provisions of Section I of Article 89 of the Constitution of the United Mexican States, and for its due publication and observance, I issue this Decree at the Residence of the Federal Executive in Mexico City, Federal District, on June Twenty-Eighth, Two Thousand and Ten. **Felipe de Jesús Calderón Hinojosa**.-Signature. Secretary of the Interior **Fernando Francisco Gómez Mont Urueta**. Signature.