



LEGAL UPDATE

January 4, 2012

REGULATIONS TO THE FEDERAL LAW FOR PROTECTION OF PERSONAL DATA IN POSSESSION OF INDIVIDUALS

On December 22, 2011, became effective the Regulations to the Federal Law for Protection of Personal Data in Possession of Individuals, published in the Official Gazette of the Federation on December 21, 2011 (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares* - the "Regulations"), which has the purpose of regulating the Federal Law for Protection of Personal Data in Possession of Individuals (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares* – the "Law"),

Following please find a general description of the most relevant aspects of the Regulations.

General Provisions¹

The Regulations are of general compliance to all the personal data recorded on physical and/or electronic hardware kept in any of the following forms: numeric, alphabetic, graphic, photographic, acoustic or of any other kind, concerning an identified or identifiable individual.

Bear in mind that the Regulations are applicable to the processing of personal data when (i) it is carried out in an establishment of the controller located in the Mexican territory, (ii) it is carried out by a processor notwithstanding its location, on behalf of a controller established in the Mexican territory; (iii) the processor is not established in the Mexican territory but it is bounded by the Mexican laws, as a consequence of an agreement or in terms of international laws, and (iv) the controller is not established in the Mexican territory and uses resources located in such territory, except if such resources are only used with transfer purposes, that not involve processing personal data. In this case, the controller shall appoint a representative with presence in Mexican territory or put into effect a mechanism that enables to comply with the legislation applicable to the controllers that process personal data.

For purposes of the aforementioned, the Regulations clarify that in the case of individuals their establishment is the main office of their business, the one used to carry out their activities or their home. In the case of legal entities their establishment is the place where the main administration office of their business can be found, in the case of legal entities residing abroad, their establishment is the place where the main administration office of their business can be found in Mexican territory, the one appointed by them or any regular premises that allows the real and effective execution of an activity.

Please note that the Regulations are not applicable to the information of (i) legal entities; (ii) individuals when acting as businessman or professionals and (iii) individuals that render services to a legal entity or to a businessman, when the information is related to their: name, last name, activities or position, address, email, telephone and facsimile; provided that such information is used for purposes of representing its employer or independent contractor.

¹ Articles 2, 3, 4, 5 6 and 7 of the Regulations.

In another matter and in connection with Article 2 of the Law it is important to note that the Regulations establish that it will not be considered as “personal use” the processing which purpose is to fulfill obligations under a legal relationship.

Following please find certain important definitions contained in the Regulations aside to those contained in the Law:

- a) **Identifiable Individual:** Any individual which identity can be determined, directly or indirectly, by means of any information, provided that a long period of time or disproportionate activities are not required;
- b) **Remittance:** Communication of personal data between the controller and the processor, within or outside of the Mexican territory;
- c) **Electronic Hardware:** Storage device which can only be accessed by the use of an equipment with electronic circuits that processes its content to examine, amend or store personal data, including microfilms; and
- d) **Physical Hardware:** Storage device intelligible at plain sight that does not need the use of any equipment to process its content to examine, amend or store personal data.

The Regulations consider as sources of public access, among others, the remote or local communication media, either electronic, optic or by means of any other technology, when the site where the personal data is stored has the purpose of providing information to the public and it is available to general consultation, telephone books, newspapers, gazettes and/or official bulletins, and mass social media, provided that its consultation can be carried out by any person without any limitation imposed by a law, or without further requirements different than the payment of a quote, fee or tariff. The processing of personal data obtained from these sources shall observe the reasonable expectation of privacy.

Personal Data Protection Principles

Below it is a brief reference to the most relevant matters provided in the Regulations in connection with the personal data protection principles.

- Consent Principle². The consent shall be prior to the processing of personal data if such is collected personally or directly from the data subject, or indirectly if the purposes of the processing are different to those previously approved by the data subject. The privacy policy shall include a mechanism that allows the data subject to refuse to the processing of its personal data for those purposes that are different to those necessary or that gave origin to the legal relationship with the controller. Article Second of the Transitory provisions of the Regulations establishes that it is not necessary to obtain the consent from the data subject when the personal data treated was collected prior to the effectiveness of the Law, provided that the privacy policy is made available to the data subject or a compensatory measure is adopted.

The obtainment of the implied or express consent of the data subject shall be:

- a) **Free:** without error, deceit, bad faith, violence or false conduct, that may affect the manifestation of the will by the data subject;
- b) **Specific:** related to one or various determined purposes that justify the processing; and
- c) **Informed:** the data subject shall know the privacy policy and the consequences of granting its consent.

² Articles 12, 14, 16, 18, 20 and 21 of the Regulations.

In addition, the express consent can be granted either verbally or written, but in either case it shall be “unmistakable“, considering that the existence of elements that evidence, without doubt, its granting are necessary. The controller shall prove the obtainment of the express consent. The controller shall make available simple and free means to express the consent only in those cases where the express consent is required by any law or regulation.

The withdrawal of the consent can be brought by any data subject or its representative, at any time, through simple and free means.

- Information Principle³. The privacy policy shall be simple, with the necessary information, clear and understandable and with structure and design that facilitate its understanding, and shall be delivered by the controller through physical, electronic, oral forms or with any other technology.

In the event that the personal data is collected indirectly and it is impossible to notify the privacy policy or it requires disproportionate efforts, bearing in mind the number of the data subjects and the oldness of the data, the controller may use compensatory measures in accordance with the general criteria issued by the Federal Institute for Information Access and Data Protection (*Instituto Federal de Acceso a la Información y Protección de Datos Personales en Posesión de los Particulares* - “IFAI”) or otherwise upon the authorization of the IFAI. The general criteria shall be issued by the IFAI no later than 3 months from the effectiveness of the Regulations.

- Quality Principle⁴. The personal data shall be accurate, complete, relevant, correct and updated. It is presumed that this principle is fulfilled when the personal data is obtained directly from the data subject and until the data subject declares or proves otherwise, or, the controller has in its possession contradictory evidence. The personal data shall be kept only for the necessary time to comply with the purposes of the processing. The controller shall establish and record the proceedings to preserve and, if applicable, block or erase the data and shall demonstrate that these proceedings are according to the Regulations or to the cancellation request.
- Purpose Principle⁵. The purposes provided in the privacy policy shall be specific regarding the purpose of the processing (certain). The controller shall distinguish the purposes that are necessary and that give origin to the legal relationship (“Necessary Purposes”), from those that are not (“Secondary Purposes”). The data subject may deny or revoke its consent and oppose to the processing of its data in connection with the Secondary Purposes, without terminating the processing regarding the Necessary Purposes. The processing for purposes that are different to those compatible or analogous to those provided in the privacy policy shall be valid upon the existence of a law or a regulation or the obtainment of a new consent.
- Loyalty Principle. The personal data shall be processed favoring the protection of the interests of the data subject and the reasonable expectation of privacy. Therefore, no misleading or fraudulent means shall be used to collect or process personal data, such as, deceit, bad faith or negligence in the information provided to the data subject about the processing of the personal data.
- Proportionality Principle. The controller shall only process the personal data that is necessary, adequate and relevant in connection with the purposes of its collection.
- Responsibility Principle⁶. The controller shall take care and will be accountable for the processing of the personal data that is under its custody or possession or for the one that was transferred to a processor. Therefore it shall adopt measures to guarantee its adequate processing, such as, drafting privacy policies and programs, carrying out training programs, establishing an internal and external surveillance system, among others.

³ Articles 24, 25 and 32 of the Regulations.

⁴ Articles 36, 37, 38 and 39 of the Regulations.

⁵ Articles 40, 41, 42 and 43 of the Regulations.

⁶ Articles 47 and 48 of the Regulations.

Processor⁷

The processor is the public or private individual or entity, national or foreign, that is not related with the controller and which relation to it is governed by an agreement or any other legal instrument that defines its activities and which proves the existence, scope and content of such relationship. The processor shall have certain obligations, among which we emphasize (i) processing only the personal data following the instructions of the controller; (ii) implementing security measures and (iii) keeping as confidential the personal data. The processor may subcontract services for the data processing upon previous authorization by the controller. The subcontractor will assume the same obligations of the processor and will carry out the processing on behalf of the controller.

Security Measures⁸

For purposes of Chapter III of the Regulations it will be understood that security measures are the control or group of controls of security to protect the personal data. The controller and the processor shall establish and keep the security measures (administrative, physical or technical) to protect the personal data independently to the processing system.

The security measures will be adopted considering, among others, the following factors (i) the inherent risk to the personal data; (ii) the sensitivity of the data and (iii) the possible consequences to the data subject.

To establish and maintain the security of the personal data the controller shall consider to implement, among others, the following actions (i) drafting of an inventory of the personal data and the processing systems of personal data; (ii) establish the functions and obligations of the persons that process personal data and (iii) training of the officers that will carry out the processing.

The Regulations consider as security breaches the following unauthorized activities (i) loss or destruction; (ii) theft, misplace or copying; (iii) use, access or processing or (iv) damage, alteration or amendment. In the event that a security breach may materially affect the financial or moral rights of the data subject, the controller shall at least inform him/her (i) the nature of the security breach; (ii) the personal data involved; (iii) the recommendations on the measures that can be taken to protect its interests, (iv) the corrective actions carried out immediately and (v) the means through which further information may be obtained.

The controller shall comply with the provisions contained in Chapter III (Security Measures) no later than 18 months from the effectiveness of the Regulations.

Transfer of Data⁹

The transfer involves the communication of personal data to a person different from the data subject, the controller or the processor. The controller and the receiving party shall demonstrate that the transfer was carried out in accordance with the Law and Regulations. All the transfers, either national or international, shall be informed to the data subjects, shall be subject to their consent by means of the privacy policy, save for the exceptions referred to the in the Law, and shall be limited to the purposes provided in such policy. National transfers shall be carried out provided that the aforementioned requirements are met that the recipient receives the privacy policy and the purposes applicable to the personal data received. On the other hand, international transfers will require that the recipient assumes the same obligations assumed by the controller, by means of an agreement or any other legal instrument.

Self-Regulatory Commitments¹⁰

⁷ Articles 49, 50, 51, 53 and 54 of the Regulations.

⁸ Articles 57, 60, 61, 63, 64 and 65 of the Regulations.

⁹ Articles 67, 68, 69, 71, 74 and 75 of the Regulations.

¹⁰ Articles 79, 81, 82, 83 and 84 of the Regulations.

Individuals or entities may agree among them or with civil or governmental organizations, national or foreign, schemes of self-regulatory commitments that complement the Law, the Regulations and any provisions issued by a governmental agency. The adhesion to and compliance with self-regulatory commitments shall be taken into consideration by the IFAI to mitigate penalties and to grant other incentives. These schemes shall take into account the parameters issued by the Secretariat of Economy (the “Secretariat”) and may include the certification of the controllers in personal data protection matters, certification which will be granted by a third party authorized to grant such certifications in accordance with the parameters which shall be issued by the Secretariat no later than 6 months from the effectiveness of the Regulations.

ARCO Rights¹¹

The exercise of an ARCO right shall not exclude the possibility of exercising any of the others, and shall not constitute a requirement to exercise any other right, and shall be exercised either by the data subject or its representative through the means established by the controller. The exercise of the ARCO rights shall be simple and at no cost, except for those costs associated with the delivery, reproductions and, if applicable, certifications of the documents.

The controller shall respond to all the requests of ARCO rights within the term of 20 days established by the Law, same which will be counted as from the day of the reception of the request. The controller may request for additional information, for one time and within the term of 5 days following to the reception of the request, when the information provided is not sufficient or is incorrect to attend the request or the documents referred to in the Law are not enclosed.

The response to the data subject shall only comprehend the data referred to in the request. The controller shall justify its denial to attend the exercise of ARCO rights and shall inform the right that the data subject has to initiate the protection data proceeding before the IFAI.

The Regulations establishes that the right to cancel may be exercised when the data subject considers that the controller is not fulfilling the principles and obligations provided in the Law and Regulations and shall be brought regarding the totality or only a portion of the personal data kept in a database.

The data subject may oppose to the processing of its personal data or shall demand the cease of the processing (i) when a legitimate cause and an specific situation requires so, same which shall be justified that even when the processing is legal, such shall cease to prevent that its persistence causes a damage to the data subject or (ii) to prevent the processing of personal data for certain purposes.

Decisions without the Intervention of Human Judgment

The controller shall notify the data subject of the processing that is carried out without the intervention of an individuals’ judgment to allow such subject to exercise its ARCO rights, if applicable.

Protection of Rights Proceeding

The request to start the protection of rights proceeding shall be filed before the IFAI by the data subject or its representative, either by means of a writ, the forms approved by the IFAI or the system put in place, within the term established in the Law.

The steps of the protection of rights proceeding are: (i) Filing, (ii) Admission, (iii) Service of Process, (iv) Admittance or Dismissal of Evidence, (v) Hearing, (vi) Pleadings, and (vii) Resolution.

A conciliation procedure may be started at any moment of such proceeding.

¹¹ Articles 87, 90, 93, 95, 96, 97, 100, 106 and 109 of the Regulations.

Verification Proceeding

The IFAI, with the purpose of confirming the compliance of the Law or of the regulations that may result from it, may begin a verification proceeding without a third party request (“*de oficio*”) or at the request of an interested party (“*a petición de parte*”), by means of an accusation filed before the IFAI upon the terms of the Regulations.

Determination of Penalties

Penalties may be imposed as a consequence of the protection of rights proceeding or the verification proceeding.

The official resolutions issued by the IFAI may be challenged by means of an annulment action carried out before the Federal Court of Tributary and Administrative Justice.

For further information in connection with this matter please contact:

Mexico City Office Mr. Jorge Leon Orantes jleon@s-s.mx and/or Ms. Paola Morales pmorales@s-s.mx, Tel.: (52 55) 52 79 54 00.

Monterrey Office: Mr. Cesar G. Cruz ccruz@s-s.mx and/or Mr. Diego Acosta dacosta@s-s.mx, Tel.: (52 81) 8133-6000.