OFFICIAL GAZETTE OF THE FEDERAL DISTRICT October 3, 2008

DECREE BY WHICH THE PERSONAL DATA PROTECTION LAW OF THE FEDERAL DISTRICT IS ISSUED

(On the upper margin a shield reads: **Mexico City** - Capital in Movement)

DECREE BY WHICH THE PERSONAL DATA PROTECTION LAW OF THE FEDERAL DISTRICT IS ISSUED

MARCELO LUIS EBRARD CASAUBON, Head of Government of the Federal District, for the knowledge of its inhabitants:

That the H. Legislative Assembly of the Federal District, IV Legislature, has addressed to me the following:

DECREE

(On the upper left margin the National Shield reads: UNITED MEXICAN STATES - **LEGISLATIVE ASSEMBLY OF THE FEDERAL DISTRICT**- IV LEGISLATURE)

LEGISLATIVE ASSEMBLY OF THE FEDERAL DISTRICT
IV LEGISLATURE

D E C R E E S

DECREE BY WHICH THE PERSONAL DATA PROTECTION LAW OF THE FEDERAL DISTRICT IS ISSUED

SOLE – The Personal Data Protection Law of the Federal District is issued, to remain as the following:

Personal Data Protection Law of the Federal District

TITLE ONE

GENERAL PROVISIONS FOR PUBLIC ENTITIES

SOLE CHAPTER

GENERAL PROVISIONS

Article 1.- This law is of public nature and of general interest and is aimed at establishing principles, rights, duties and procedures regulating protection and handling

of personal data in possession of public entities.

Article 2.- For the purposes of this Law, the following terms shall mean:

Personal data blockage: Personal data identification and confidentiality to prevent handling thereof;

Personal data assignment: Any data obtained by looking up any file, record, data base or bank, any published data contained therein, interconnection of data with other files and data communicated by any individual other than the interested party, as well as any data transfer or communication among public entities;

Personal data: Any numeral, in writing, alphabetical, graphic, and acoustic or an other type data pertaining to an individual, whether identified or identifiable. It is data, including but not limited to, on ethnic or racial origin, physical, morality or emotional features, love and family life, address, home telephone, unofficial e-mail, property, political opinions and ideology, believes, religious and philosophical convictions, health condition, sexual preference, fingerprint, DNA and social security, and other similar;

Public Entity: Legislative Assembly of the Federal District; the Higher Court of Justice of the Federal District; the Administrative-Law Court in the Federal District; the Electoral Court of the Federal District; Electoral Institute of the Federal District, Human Rights Commission of the Federal District; Board of Conciliation and Arbitration of the Federal District; Mexico City Mayor's Office; Agencies, Decentralized Entities, Political Subdivisions and Public Administration Entities of the Federal District; any Autonomous Institutions under the law; political parties, associations and groups; as well as those entities acknowledged by the local law as of public interest and using public spending; and any entities equal to public or private law legal entities, whether acting in aid of the above-mentioned bodies or using public spending in carrying out their activities;

Institute: The Institute for Access to Public information of the Federal District.

Interested Party: Any individual owner of the personal data which is the purpose of the handling set forth in this Law;

Public Information Office: It is the administrative unit receiving requests for access to, correction of, cancellation of and opposition to personal data in possession of public entities, that shall be in charge of handling those requests, pursuant to provisions in this Law and in the guidelines issued therefor by the Institute;

Dissociation Proceeding. It shall mean any personal data handling so that the information obtained may not be associated to an identified or identifiable individual;

Individual in Charge of the Personal Data System: Any individual making decisions on personal data protection and handling, as well as on the contents and purpose thereof;

Personal Data System: Any organized set of records, files, personal data bank or bases

of pubic entities, whatever their creation. storage, organization and access method or system;

Personal Data Handling: Any operation or set of operations carried out through related automated or physical proceedings related with obtaining, registering, organizing, blocking, preserving, preparing, using, assigning, disseminating, interconnecting or any other manner during access, correction, cancelation or opposition of personal data;

User.- It is the user authorized by a public entity to provide services thereto for personal data handling.

Article 3.- This law shall be construed pursuant to the Political Constitution of the United Mexican States, the Universal Declaration of Human Rights, International Pact on Civil and Political Rights, American Convention on Human Rights, and any other international instruments duly executed and ratified by the Mexican Government and construction thereof performed by the applicable international agencies.

Article 4.- Aspects not specifically provided in the proceedings referred to in this Law shall be governed as a substitute by the Administrative Proceedings for the Federal District, and in the absence thereof, by the Code of Civil Proceedings for the Federal District.

TITLE TWO

CUSTODY OF PERSONAL DATA CHAPTER IPRINCIPLES

Article 5.- Personal data systems in possession of public entities shall be governed by the following principles:

Legality: it means that possession and handling of the personal data systems shall exclusively fulfill the legal or regulatory capacities of each public entity and shall be obtained through any means provided for in those provisions. The personal data systems may not be aimed at purposes contrary to the laws or the public morality and under no circumstances they may be used for purposes differing or not compatible with the purposes causing them to be obtained. Any further data handling shall not be deemed incompatible for historic, statistical or scientific purposes.

Consent: it means the free will, unequivocal, specific o duly informed expression, whereby the interested party consents with the handling of his/her personal data.

Data Quality: Collected personal data shall be true, proper, pertinent and non-exceeding regarding the environment and purpose for which it was obtained. Data shall always be

updated so it truly reflects the interested party's present situation.

Confidentiality: it means guaranteeing that personal data or the personal data system may only be accessed by any interested party for handling purpose. It shall also mean the secrecy obligation by the individual in charge of the personal data system, as well as by users. Legal instruments regarding services contracted by the individual in charge of the personal data system, as well as the users, shall provide the obligation to guarantee security and confidentiality of personal data systems, as well as banning their use for purposes other than those for which contracting was executed, as well as those liquidated damages for breaching thereof. All the above-provided, without prejudice to duties set forth in other applicable provisions. Personal data is non-waivable, non-transferrable and non-assignable, consequently, it may not be transferred except for a legal provision or when consented by owner and that obligation shall survive even after the public entity relation with the personal data owner is terminated, and even after any labor relation between a public entity and the individual in charge of the personal data system or users is terminated. The individual in charge of the personal data system or the users may be relieved from the confidentiality duty through a court resolution and when founded reasons regarding public security, the national security or public health exist.

Security: It means guaranteeing that only the individual in charge of the personal data systems, or if any, the authorized users may undertake the personal data handling, by applying the proceedings established therefor.

Availability: Data shall be stored to allow exercise of access, correction, cancelation and opposition rights by interested party.

Period of time: Personal data shall be disposed of as soon as it is not required or pertinent any more for the purpose it had been collected. Excluded is any further handling to be applied to data for statistical or scientific purposes, provided the dissociation procedure is applied. Only personal data subject to historic purposes may be fully, and permanently preserved and subject to handling.

CHAPTER II

PERSONAL DATA SYSTEMS

Article 6.- Each public entity shall determine, through the head thereof, if any, or the competent body, if personal data systems shall be created, modified or deleted, in accordance with their relative territorial jurisdiction.

Article 7.- Preparation, handling and custody of personal data systems shall be governed by the following provisions:

I. Each public entity shall publish in the Official Gazette of the Federal District when creating, changing or deleting their personal data system;

II. When creating or changing personal data systems, they shall detail at least the following:

a) Purpose of the personal data system and provided uses thereof;

b) Any individuals or group of individuals of whom personal data is intended to be obtained or who are obliged to provide it;

c) The collection procedure of data of a personal nature;

d) Basic structure of the personal data system and detail of type of data included therein;

e) Any assignments the data may be subject to;

f) Agencies in charge of handling personal data system;

g) Administrative unit where the access, correction, cancelation or opposing rights may be exercised; and

h) Required protection level.

III. Provisions established to dispose of the personal data systems, destination of data contained therein shall be established or, if applicable, any stipulations provided for disposal thereof.

IV. When disposing of personal data, any information priorly submitted to dissociation proceedings for statistical or historic purposes may be excluded.

Article 8.- Personal data systems in possession of public entities shall be registered in the record determined therefor by the Institute.

The registry shall include at least the following information:

I. Name and position of the individual in charge and of users;

II. System purpose;

III.Type of personal data included in each system;

IV. Data collection method and data updating;

V. Destination of data and individuals or legal entities to whom data may be transmitted;

VI. Method to interrelate any registered information;

VII. Period of time to keep data, and

VIII. Security measures.

Article 9.- When public entities collect personal data, those entities shall priorly, expressly, accurately and unequivocally inform the interested party the following:

I. Availability of a personal data system, personal data handling, purpose for obtaining data, and data addressees;

II.The mandatory or optional feature to answer any questions made thereto;

III. Consequences for obtaining personal data, for a refusal to provide data or for data that is not correct;

IV. The possibility that data is disseminated, in which case the interested party shall expressly consent thereto, except for personal data that pursuant to Law is deemed public;

V. The possibility to exercise access, correction, cancellation or opposition rights; and

VI. The name of the individual in charge of the personal data system and if any of any addressees.

When sing questionnaires or any other printed materials to obtain data, any warnings provided for herein shall be clearly and visibly contained.

In the event interested party's data of personal nature has not been collected, that party shall be expressly, accurately and unequivocally be informed by the person in charge of the personal data system, in a three-month period following the data registration time, except when that party has already been priorly notified about provisions in fractions I, IV y V herein.

Provision set forth herein shall be excluded when so expressly provided by any law.

Likewise, provisions set forth herein shall not apply when personal data has been obtained from any source available to the general public.

Article 10.- No person shall be obliged to provide any personal data deemed as sensitive, such as data on ethnic or racial origin, morality or emotional features, political ideology or opinions, believes, religious and philosophical principles, sexual preference, among other. It is expressly banned to establish personal data systems aimed at exclusively storing personal data set forth in priorly immediate paragraph. Those systems may only be handled if related with purposes of a general nature, if provided by law, if expressly consented by the interested party or if for statistical or historic purposes,

provided a dissociation proceedings has been priorly executed. The dissociation proceeding shall not be required when related with scientific or public health studies.

Article 11.- Any files or systems established for administrative purposes by agencies, institutions o public health entities, and containing data of a personal nature, shall be subject to the general protection system provided for in this Law. Data of a personal nature obtained for police purposes, may be collected without consent by the individuals related therewith, however it shall be limited to any presumptions and data categories required to prevent a real danger to public security or to prevent or prosecute a crime, and that data shall be stored in particular systems established therefor, that shall be classified based on categories and in accordance with the degree of reliability thereof. Obtaining and handling of data referred to herein may be exclusively performed when it is definitely required for purposes of a specific investigation, without prejudice to legality control of administrative performance of the obligation to decide on accusations filed by the interested parties before jurisdictional entities. Personal data collected for police purposes shall be cancelled if and when it is not required any more for the investigations causing data to be kept. For this purpose, the interested party age shall be specially taken into consideration, as well as the nature of stored data, the need to keep the data until any investigation or specific proceeding has concluded, the final judgments, specifically, acquittal, commutation, rehabilitation and liability extinguishment.

Article 12.- The individuals in charge of the personal data systems for police purpose, to prevent crime behavior or regarding tax matters, may deny access, correction,, opposition and cancellation of personal data based on dangers that may arise in the defense of government or the public security, protection of rights and of third party's rights or the requirements of investigations being performed, and also when those rights obstruct the performance of the authority meeting their duties.

CHAPTER III

SECURITY MEASURES

Article 13.- Public entities shall establish technical and organizational security measures to guarantee confidentiality and entirety of each personal data system in their possession, thus preserving full exercise of rights provided herein, against any alteration, loss, transmission and unauthorized access, in accordance with the data type contained in those systems. Those measures shall be adopted regarding any lower or higher degree of protection required by the personal data. Those measures shall be in writing

and notified to the Institute for registry purposes. Security measures established therefor shall detail name and position of the public servant, or if applicable, any individual or legal entity taking part in handling personal data in the capacity of individual in charge of the personal data system or user, as applicable. Regarding users, the information on the legal act whereby the public entity authorized handling of the personal data system shall be included. in the event of data updated, the applicable amendment shall be notified to the Institute, in a 30-business day term following the date when change was performed.

Article 14.- Public entity in charge of the custody and handling of the personal data system shall take security measures, based on the following:

A. Type of security:

I. Physical.- It refers to any measure aimed at protecting premises, equipment, support or data software to prevent risks arising out of acts of God or force majeure events;

II. Logical.- it is related with protection measures allowing identification and authentication of persons or users authorized to handle personal data based on their duty;

III. Development and applications.- It is related with authorizations required to create or process personal data systems, based on their relevance, to guarantee data is properly developed and used, providing for user participation, environment separation, methodology to be applied, life and management cycles, as well as specific considerations regarding applications and tests;

IV. Encryption.- it is related with implementation of algorithms, codes, passwords, and specific protection devices guaranteeing information confidentiality and completeness; and

V. Communications and networks.- it relates to preventive restrictions and/or risks that shall be fulfilled by data or personal data system users to access dominions or to install authorized software, as well as to manage telecommunications.

B. Security Levels:

I. Basic.- it shall be deemed as such, the level regarding general security measures which application is mandatory for all personal data systems. Those measures are related with the following:

a) Security document;

b) duties and obligations of staff taking part in handling personal data systems;

c) Registry of events;

d)Identification and authentication;

e) Access control;

f) Support management, and

g) Backup and recovery copies.

II. Medium.- it refers to taking security measures which application is related to those data systems in regard to committing administrative or criminal violations, public treasury, financial services, property data, as well as systems containing data of a personal nature that may allow obtaining an assessment of an individual's personality. That security level, in addition to measures qualified as basic, takes into account the following:

a) Individual in charge of security;

b) Auditing;

c) Physical access control; and

d) Tests using real data.

III. High.- It refers to security measures applicable to data systems related to ideology, religion, believes, political affiliation, racial or ethnic origin, health condition, biometrics, genetic or sexual life, and also those systems containing data collected for police, security, prevention, investigation and crime prosecution purposes. Data systems that should be assigned a high security level, in addition to incorporating the basic and medium security levels, shall complete the below detailed measures:

a) Support distribution;

b) Access registry; and

c) Telecommunications.

Various security levels shall be established taking into account the features applicable to information.

Article 15.- Security measures set forth in prior Article are the lowest required measures, therefore, the public entity shall take any additional measures deemed advisable to offer better guaranties for protecting and safeguarding the personal data systems. Due to information nature, any security measures taken shall be deemed as confidential and shall only be transmitted to the Institute for registration purposes.

CHAPTER IV

PERSONAL DATA HANDLING

Article 16.- Handling of personal data shall require the express, unequivocal consent in writing by the interested party, except in the following exclusions:

I. When collected to exercise legal features conferred to public entities;

II. In the event of a court order;

III. When related to parties to a business, labor or administrative relation agreement, and it is required to keep or fulfill them;

IV. If the interested party is not able to consent due to health problems and handling of information thereof is required for prevention or medical diagnosis purposes, to provide or administer health care or medical treatment, provided that information handling is performed by a person who is subject to a professional secrecy obligation or any other equivalent duty;

V. When transmission is expressly provided by law;

VI. When transmission is made among government agencies and aimed at further handling data for historic, statistical or scientific purposes;

VII. When made public by third parties to provide a service regarding personal data handling by freely and legitimately agreeing on a legal relationship which development, fulfillment and control involves that data communication shall be legal as soon as the purpose justifying thereof is restricted;

VIII. When related to personal data regarding health matters, and when required for public health and emergency reasons or to carry out any epidemiological research; and

IX. When data is contained in sources easily accessible to the general public and handling thereof is needed, provided the interested party's essential rights and liberties are not violated.

Consent set forth in this Article may be revoked when a justifiable cause therefore exists, and no retroactive consequences are assigned thereto.

A public entity may not disseminate or assign personal data contained in data systems developed in executing their duties, except when expressly consented in writing or through an equivalent authentication mean by the individuals the information is related with. To that effect, the office of public information shall make available the required forms to obtain that consent.

Assignee shall be subject to legal and regulatory obligations similar to the assignor, and shall jointly be liable for violations thereof.

Article 17.- In the event data of personal nature is used or assigned thus seriously preventing or putting in jeopardy in a similar manner the exercise of individuals rights, the Institute may demand from the individuals in charge of the personal data systems to stop using or assigning data. If demand is ignored, through a resolution duly founded and originated, the Institute may block those systems, in accordance with any procedures established therefor. Any violation to the immobilization ordered by the Institute shall be sanctioned by the competent authority pursuant to the Federal Civil Service Liability Law.

Article 18.- Handling of personal data systems regarding health matters, is governed by provisions in the General Health Law, The Health Law for the Federal District, and all other rules deriving out thereof. Handling and assignment of that data obliges to preserve personal identification data of patients, apart from clinical-handling nature data; so that confidentiality thereof is preserved, except when the own patient has consented not to have them split. Excluded are events of scientific research, public health or court purposes where it is deemed essential to unify data identified with clinical-welfare data. Access to data and documents related with individuals' health condition shall be strictly limited to the specific purposes for each case.

Article 19.- Personal data systems which have been the purpose of handling, shall be deleted once the preservation terms thereof have elapsed or when they are not needed any more for the purpose they were collected for. If handling of systems has been performed by an individual other than the public entity, any legal instrument giving rise thereto shall set forth the term to be preserved by user, and once it has elapsed, all data shall be returned to the public entity that shall guarantee its custody or handling, if any, or disposal.

Article 20.- In the event addressees of data are institutions located in different states, public entities shall make sure that those institutions shall guarantee they have protection levels similar or above to those set forth herein, and in the relative regulations of the applicable public entity. In the event that the data addressees are persons or institutions located in other countries, the individual in charge of the personal data system shall assign thereof, pursuant to provisions in any applicable federal law, provided the security and protection levels set forth herein are duly guaranteed.

CHAPTER V

OBLIGATIONS BY PUBLIC ENTITIES

Article 21.- The Head of the public entity shall appoint the individual in charge of the personal data systems, who shall:

I. Meet the policies and guidelines as well as the standards issued on personal data management, handling, security and protection;

II. Take any required security measures to protect personal data and to report them to the Institute for registration thereof, pursuant to provisions herein;

III. Prepare and submit to the Institute a report on obligations provided herein, no later than the last business day of January of each year. Failure regarding that report shall incur liabilities;

IV. nform the interested party when collecting personal data, about existence and purpose of the personal data systems as well as the mandatory or optional possibility to provide it and consequences thereof;

V. Adopt proper proceedings to process requests for personal data access, correction, cancellation and opposition, and if applicable, for assigning thereof. Public servants in charge of processing and following up those requests shall be duly trained;

VI. Use personal data only when it is related with the purposes it was collected for;

VII. Allow at all times the interested party to exercise the right to access personal data thereof, to request any correction or cancellation, and to oppose the handling thereof pursuant to provisions hereof;

VIII. Update personal data whenever deemed proper. Information being inaccurate or incomplete shall be corrected or completed so it matches the interested party's current information, provided a document supporting updating of that data is available. The above-mentioned shall be without prejudice to the right of the interested party to request that the personal data pertaining thereto is corrected or cancelled;

IX. Establish specific criteria on handling, maintenance, security and protection of personal data system;

X. Prepare a training program on personal data security matters;

XI. Decide on exercising rights for access, correction, cancellation and opposition of individuals' data;

XII. Establish specific criteria for management, maintenance, security and protection of personal data systems;

XIII. To carry out, if applicable, coordinate material execution of various operations and

procedures applicable to handling data and data of personal nature systems under his custody are;

XIV. Coordinate and supervise security measures to be taken and under which personal data systems are subject to in accordance with the regulations currently in force;

XV. To report in a founded and motivated manner to competent authorities the exceptions applied to general system provided for access, correction, cancellation or opposition of personal data; and

XVI. Any other arising out of this Law or any other applicable legal ordinances.

Article 22.- The Head of a public entity shall be responsible for making decisions on the purpose, content and use of personal data system handling. That head may delegate his authority at the administrative unit where the material competence is located, and for which exercise the data system serves instrumentally and to which unit the person in charge thereof is assigned to.

TITLE THREE

AUTHORITY IN CHARGE OF CONTROLLING AND MONITORING

SOLE CHAPTER

THE INSTITUTE AND AUTHORITY THEREOF

Article 23.- The Institute for Access to Public information of the Federal District is the autonomous institution in charge of coordinating and monitoring fulfillment hereof, as well as of any regulations arising thereof. The authority in charge of guaranteeing protection and proper handling of personal data shall be responsible thereof.

Article 24.- The Institute shall have the following authority:

I. To establish, in the field of its competence, policies and guidelines of general observance and mandatory for management, handling, security and protection of personal data in possession of public entities; as well as to prepare those standards required for fulfillment hereof;

II. To develop and approve the personal data access, correction, cancellation and

opposition request forms;

III. To establish electronic system to receive and process personal data access, correction, cancelation and opposition requests;

IV. To prepare a registry of personal data systems in possession of public entities;

V. To prepare and update a security measure registry of personal data systems in possession of public entities, pursuant to provisions in this Law;

VI. To issue opinions on topics related herewith, as well as to prepare notes and recommendations for public entities, arising out of violations to principles governing this Law;

VII. To inform the internal control body at the applicable public entity about resolutions issued in regard to potential breach to provisions subject matter hereof;

VIII. To guide and advise the persons requiring so, in regard to the contents and scope of this Law;

IX. To prepare and publish studies and research for this Law to be widely known;

X. To request and evaluate the reports submitted by public entities regarding exercise of rights provided in this Law. That evaluation shall be included in the report that pursuant to Article 74 of the Transparency and Access to Public Information Law shall be submitted by the Institute to Legislative Assembly of the Federal District and shall include at least:

a) The number of personal data access, correction, cancellation and opposition requests submitted before each Public Entity, as well as any outcome thereof;

b). The time to reply the request;

c). Status of claims filed before internal control bodies and difficulties determined in fulfilling this Law;

d). Use of public funds for that purpose;

e). Any actions carried out;

f). Management indicators; and

g). Impact of performance.

XI. To organize seminars, courses, workshops and any other activities thus promoting that this Law is widely known, as well as the persons' rights regarding their personal data;

XII. To establish training programs in the filed of personal data protection, and to promote actions making easier for public entities and their staff to take part in those activities, thus guaranteeing proper fulfillment of principles governing this Law;

XIII. To promote in education institutions, both public and private, that they include in their academic activities, both curricular and extra-curricular, topics praising the relevance of the right to protect personal data;

XIV. To promote preparation of guide books explaining the proceedings and processes subject matter of this Law;

XV. To investigate, support and solve the petition for revision pursuant to provisions in this Law, and in the Transparency and Access to Public Information Law for the Federal District;

XVI. To evaluate performance of Public Entities, by periodically and officially making inspection visits, and to check that principles set forth in this Law are fulfilled. Those visits may not related at all to data with restricted access pursuant to the applicable law;

XVII. To undertake reconciling of interest of interested parties with those of public entities, whenever they are in conflict by executing this Law; and

XVIII. Any other provisions set forth by this Law, and any other applicable ordinances.

Article 25.- In order to promote the habit to protect personal data, events promoting professionalization of public servants in the Federal District should be organized, and security measures required for custody of personal data at each public entity should be promoted.

TITLE FOUR

RIGHTS AND PROCEDURE FOR EXERCISING THEM

CHAPTER I

RIGHTS ON PERSONAL DATA MATTERS

Article 26.- All persons, being priorly identified by an official document shall have access, correction, cancellation and opposition rights regarding their personal data in possession of public entities, and those rights shall be independent. Consequently it is not possible to understand that exercise of any of them shall be prior requirement of that it shall prevent exercise of another. Reply to any rights provided in this Law shall be provided in a legible and readable manner, and it may be provided, at the election of the

interested party, in writing or through direct consultation.

Article 27.- Right of access shall be exercised to request and obtain information on data of personal nature submitted for handling purposes, on source of data, as well as on any assignments made or planned to be made, pursuant to provisions in this Law.

Article 28.- The interested party's data correction right shall proceed, only when that data is inaccurate or not complete, not proper or excessive, provided however that is not impossible or requiring disproportionate endeavors. However, when data is related with facts evidenced in an administrative proceeding or in a court proceeding, that data shall be deemed accurate provided it matches the facts.

Article 29.- The interested party shall have the right to request cancellation of own data when handling thereof shall not abide by provisions in the Law o by guidelines issued by the Institute, or if the opposition right has been exercised and that right has proceeded. Cancellation shall give rise to data being blocked, and shall be preserved only for public entities; to process potential responsibilities arising out of the handling, during the prescription term thereof. Once term has elapsed, they shall proceed to disposal thereof, pursuant to the applicable regulations. Disposal of data shall not proceed if that might give reside to damages to legal rights or third party's interests, or when a legal obligation to preserve that information exists.

Article 30.- The interested party shall have the right to oppose handling of data pertaining thereto, in the event the data was collected without consent thereof, and if there are founded reasons therefor, and no provision to the contrary is set forth in the law. In the event that presumption is updated, the individual in charge of the personal data system shall cancel the data related with the interested party.

Article 31.- If verified or cancelled data had been priorly transmitted, the individual in charge of handling shall notify any correction performed to data that was transmitted to, if the latter maintains handling, and that person shall also proceed to correct or cancel that data.

CHAPTER II

PROCEEDINGS

Article 32.- Receiving and handling personal data access, correction, reception and handling requests submitted before public entities shall be subject to the proceedings set forth herein.

Without prejudice of what is provided in other laws, the interested party or the legal representative thereof only, priorly evidencing his identity, may request the public entity, through the competent public information office, to allow access, correction, cancellation or that the opposition right thereof, regarding personal data related therewith, to be effective, and to be kept in a personal data system in possession of a public entity.

The public information office of the public entity shall notify the requester or electronic mean mentioned therefor, in a term not to exceed fifteen business days form the date the request is submitted, any resolution adopted regarding the request, so that, if proceeding, to be effective within ten business days following the date of the above-mentioned notice.

The fifteen day term referred to in prior paragraph may be increased only once, for a similar term, provided the applicable circumstances justify that.

if when request is submitted it is not accurate or fails to include all required information, at that time the Public Entity, if request is made verbally, shall aid the petitioner to solve any deficiencies. If details provided by petitioner are not enough to locate the personal data or if they are erroneous, the public information office at the public entity may prevent, only once, and within the five business days following submittal of the request, so that request is clarified or completed, and by warning the individual that if prevention is not followed up it shall be deemed that request was never submitted. That requirement stops the terms set forth in two prior paragraphs.

In the supposition that the personal data referred to in the request is created in the personal data systems of the public entity and that it is considered a request for access, correction, cancellation or opposition that may not proceed, a founded and motivated resolution must be issued on the matter. This response must be signed by the head of the public information office and by the person in charge of the personal data system of the public entity.

When the personal data with respect to which the access rights are exercised, correction, cancellation or opposition, are not found in the information systems of the public entity, the interested party will be informed through a detailed notice that indicates the personal data systems in which the search was carried out. This notice will have to be signed by the head of the public information office and the person in charge of the personal data system of the public entity.

Article 33 - The request for access or opposition to, or correction or cancellation of, personal data, must be submitted before the public information office of the public entity that the interested party believes is processing his/her personal data. The procedure for access or opposition to, or correction or cancellation of, personal data, will initiate with the submittal of the request in any of the following manners:

I. In writing, it will be personally submitted by the interested party, or his/her legal representative, in the public information office, or, through ordinary mail, certified mail or messenger service;

II. In verbal form, it will be carried out by the interested party, or his/her legal representative, directly in the public information office, orally and directly, which will have to be documented by the person in charge of the office in the respective format;

III. By e-mail, it will be carried out by the interested party, or his/her legal representative, through an e-mail address and sent to the assigned e-mail address of the public information office of the public entity;

IV. By the electronic system that the Institute establishes for such effect, and

V. By telephone, under the terms of the guidelines that are issued by the Institute.

Article 34 - The request for access or opposition to, or correction or cancellation of, personal data, will have to contain, at least, the following requirements:

I. Name of the public entity to which it is addressed;

II. Complete name of interested party, and in such case, his/her legal representative;

III. Clear description and explanation of the personal data with respect to that sought in the exercise of one of the above mentioned rights;

IV. Any other element that facilitates its location;

V. The address, one that must be found within the Federal District, or by electronic means in order to receive notifications, and

VI. Optionally, the preferred form in which the access to personal data is granted, which could be direct consultation, simple or certified copies.

In the case of applications for access to personal data, the interested party, or in such case, his/her legal representative will have to prove his/her identity and personality at the

time of the delivery of the information. Also, the identity will have to be proven before the public entity carries out the correction or cancellation.

In the case of a correction of personal data, the interested party must indicate the information that is erroneous and the correction that must be made, and attach any probatory documentation supporting the request, unless the consent of the interested party is solely required and that is acceptable.

In the event of applications to cancel personal data, the interested party will have to indicate the reasons based on which he/she considers that the handling of information does not meet the provision in the Law, or to prove, if applicable, the source for exercising his/her right of opposition.

The means by which the petitioner will be able to receive notifications and agreements of proceeding will be: e-mail, personal notice at his/her address or in the corresponding public information office. In case the petitioner does not indicate an address, or one of the means authorized by this law, to hear and receive notifications, the warning will be notified by list posted at the Public Information office of the corresponding Public Entity.

The sole means by which the interested party may receive the data with reference to personal data, will be through the public information office, and without greater formality than to prove his/her identity and to cover the costs in accordance with the present Law and the Financial Code of the Federal District.

The Institute and the public entities will have the infrastructure and technological means necessary to guarantee the effective access to the information for handicapped people.

Article 35 - With the request for access or opposition to, or correction or cancellation of, personal data submitted, the public information office of the public entity, will observe the following procedure:

I. It will proceed to the reception and registry of the request and will give submit a copy of the registered request to the interested party, which will serve as receipt of the request, on which the institutional seal, plus the hour and the date of the registry will have to appear;

II. With the request registered, it will verify if it meets the requirements established by the previous article, otherwise it will advise the interested party, as indicated in article 32 of the present Law. To meet the requirements it will be turned over to the corresponding administrative unit so that the location of the information requested will proceed, in order to issue the corresponding response;

III. The administrative unit will inform the public information office of the existence of the requested for information. In case of nonexistence, it will proceed in accordance with

that stipulated in article 32 so that the public information office carries out a new search in another area or administrative unit.

In the response, the public information office, will indicate the by item cost of the reproduction that the petitioner will have to pay under the terms of the Financial Code of the Federal District;

IV. At the address or through the means indicated for such effect, the public information office will notify the interested party or his/her legal representative of the existence of a response so that it may be collected at the public information office;

V. In every case, the delivery in printed form or the direct electronic access to the petitioner for the information will be carried out in a personal manner to the interested party or his/her legal representative; and

VI. Delivery of the requested information will be carried out after the exhibition of the original document with which the interested party or his/her legal representative proves their identity.

In case the public entity determines that the correction or cancellation of the personal data will proceed, it must notify interested party of the proceeding of the request, so that, within the 10 following working days, the interested party or the his/her legal representative may prove his/her identity before the public information office so the correction or cancellation of the personal data will be carried out.

Article 36 - In the case that the request may not proceed, the public information office must notify the petitioner in a founded and motivated manner, of the reasons for which its request did not proceed. The response must be signed by the head of the public information office and by the person in charge of the personal data system, with the possibility that these functions may come under the same. When the correction of personal data must be made in files based on jurisdictional procedures or those followed by judgment, no data will be suppressed, but that referred to as correct will be established, as long as the sentence or resolution has not caused the state.

Article 37 - The proceeding request for access or opposition to, or correction or cancellation of, personal character information is gratuitous. However, the interested party will have to cover the costs for the reproduction of information, under the terms of the Financial Code of the Federal District. The costs of reproduction of the requested information will be charged to the petitioner previous to his/her delivery and it will be calculated according to:

I. The cost of the materials used in the reproduction of the information;

II. The cost of shipping; and

III. The document certification when it proceeds.

The Public Entities will have to strive to reduce the costs of information delivery to the minimum. The interested party may not request the delivery of personal data with respect to a same system in a period of less than six months after the previous request, unless by effect, he/she proves a legitimate interest, in which case he/she will be able to be request it at any time.

CHAPTER III

PETITION FOR REVISION

Article 38 - The interested party may interpose a petition for revision before the Institute, that he/she considers to be offended by the resolution, final or proceeding, that falls upon his/her request for access or opposition, or correction or cancellation, or before the omission of the response. For this effect, the public information offices when responding to the applications, will advise the appellant on his/her right to interpose the petition for revision and the manner and period of time in which to do it. The above mentioned notwithstanding, the right that gives interested parties the ability to interpose complaint before the internal control agencies of the obliged entities.

Article 39 - The Institute will have access to the information contained in the personal data systems that are indispensable to solve the petition. Said information must maintain a confidential character and it will not be available in the records. The resolutions that the Institute issues will be final, unassailable and obligatory for the public entities and the individuals. The individual may interpose action for infringements of fundamental rights and freedoms against the resolutions of the Institute. The competent judicial authority will have access to the personal data systems when it is indispensable to resolve the matter and had been offered in judgment. Said information must be maintained with such character and he will not be available in the records.

Article 40 - The petition for revision will be processed in accordance within the terms, period and requirements indicated in the Transparency and Access to Public Information Law of the Federal District. Also, the appellant will be able to interpose the appeal of revocation, that will be substantiated under the terms that established by the

Transparency and Access to Public Information Law of the Federal District and the Internal Regulation of the Institute.

TITLE FIVE
LIABILITIES

SOLE CHAPTER
INFRACTIONS

Article 41 - Those which constitute infractions to the present Law:

I. The omission or irregularity in the attention of the request for access or opposition to, or correction or cancellation of, personal data;

II. To prevent, to block or to deny the exercise of rights to that referred to in the present Law;

III. To obtain information of a personal character without providing the information stipulated in the present Law;

IV. To create information system of personal character, without the previous publication in the Official Journal of the Federal District;

V. To collect information without the express consent of the interested party when it is required;

VI. To fail to fulfill the principles stipulated by the Law;

VII. To transgress the measures of protection and confidentiality of which are referred to in the present Law;

VIII. To totally or partially omit the recommendations made by the Institute, as well as to obstruct the its functions;

IX. To omit or to present the information in an untimely manner that which is referred to in the present Law;

X. To collect personal data in a deceptive or fraudulent manner;

XI. To transmit personal data, outside of the permitted cases, particularly when the transmission is intended to obtain an illegal profit;

XII. To prevent or to block the inspection ordained by the Institute or its instruction to block the personal data systems, and

XIII. To destroy, to alter, to yield personal data, files or personal data systems without

authorization;

XIV. To fail to fulfill with the immobilization of personal data systems ordained by the Institute, and

XV. To fail to fulfill any of the resolutions contained in this Law.

The infractions to referred to in this article or any other derived from the failure to fulfill the obligations established in this Law, will be sanctioned under the terms of the Federal Civil Service Liability Law, being independent of those of civil or penal order deemed fit, and the procedures for the compensation of the damage caused by the public entity.

Article 42 - The Institute will denounce, before the competent authorities, any conduct stipulated in the previous article and will present the evidence that it considers pertinent. The internal control and examining agencies of the public entities will submit a half yearly statistical report of the administrative procedures initiated for the failure to meet the present Law, and their results, to the Institute. This information will be incorporated to the annual report of the Institute. Said resolution will notify the Public Entity and the person in charge of the personal data system and, in such case, to the interested parties of the personal data that will be affected. The above mentioned notwithstanding, the criminal or civil responsibilities that could be derived.

TRANSITORY ARTICLES

ONE - The present decree will enter in force **the day after** its publication in the Official Gazette of the Federal District. It is to be published in the Journal of the Federation for its greatest dissemination.

TWO - It is to be published in the Official Gazette of the Federal District for its due observance and request.

THREE - The public entities must notify the Institute of the list of Personal data systems that they own for their records, thirty working days after the present Law comes into force.

FOUR - The document in which the security measures are established to that referred to in the article of chapter III of Title II of the present Law, must be issued by the public entities within sixty working days after the Law comes into force, and it must remitted to the Institute for its registry within the same period.

Office of the Legislative Assembly of the Federal District, on the twenty seventh day of the month of August of the year two thousand eight. BY THE BOARD OF

DIRECTORS.- DEP. AGUSTÍN CARLOS CASTILLA MARROQUÍN, PRESIDENT.- DEP. LETICIA QUEZADA CONTRERAS, SECRETARY.- DEP. ALFREDO VINALAY MORA, SECRETARY.- Signatures.

In fulfillment of that stipulated in article 122, Section C, Second Base, subsection II, parenthesis b), of the Political Constitution of the United Mexican States; 48, 49 and 67, subsection II of the Government Statutes of the Federal District, and for its due publication and observance issued the present Promulgatory Decree, in the Official Residence of the Head of Government of the Federal District, in the City of Mexico, on the eighteenth day of the month of September of two thousand eight.- **THE HEAD OF GOVERNMENT OF THE FEDERAL DISTRICT, MARCELO LUIS EBRARD CASAUBON.- SIGNATURE.- THE SECRETARY OF GOVERNMENT, JOSÉ ÁNGEL ÁVILA PÉREZ.- SIGNATURE.- THE SECRETARY OF URBAN DEVELOPMENT AND HOUSING, J. ARTURO AISPURO CORONEL, ARCH.- THE SECRETARY OF ECONOMIC DEVELOPMENT, LAURA VELÁZQUEZ ALZÚA.- SIGNATURE.- THE SECRETARY OF THE ENVIRONMENT, MARTHA DELGADO PERALTA.- SIGNATURE.- THE SECRETARY OF WORKS AND SERVICES, JORGE AFGANIS DÍAS LEAL.- SIGNATURE.- THE SECRETARY OF SOCIAL DEVELOPMENT, MARTÍ BATRES GUADARRAMA.- SIGNATURE.- THE SECRETARY OF HEALTH, ARMANDO AHUE ORTEGA.- SIGNATURE.- THE SECRETARY OF FINANCES.- MARIO DELGADO CARRILLO.- SIGNATURE.- THE SECRETARY OF TRANSPORTATION, ARMANDO QUINTERO MARTÍNEZ.- SIGNATURE.- THE SECRETARY OF PUBLIC SAFETY, MANUEL MONDRAGÓN Y KALB.- FIRMA.- THE SECRETARY OF TURISM.- ALEJANDRO ROJAS DÍAZ DURÁN.- FIRMA.- THE SECRETARY OF CULTURE, ELENA CEPEDA DE LEÓN.-. SIGNATURE.- THE SECRETARY OF CIVIL DEFENCE.- ELÍAS MIGUEL MORENO BRIZUELA.- SIGNATURE.- THE SECRETARY OF WORK AND PROMOTION OF EMPLOYMENT.- BENITO MIRÓN LINCE.- SIGNATURE.- THE SECRETARY OF EDUCATION.- AXEL DIDRIKSSON TAKAYANAGUI.- SIGNATURE.- THE SECRETARY OF RURAL DEVEOLPMENT AND EQUITY FOR THE COMMUNITIES.- MARÍA ROSA MÁRQUEZ CABRERA.-SIGNATURE.**