

ACT N° 25.326 and REGULATORY DECREE N° 1558/01

PERSONAL DATA PROTECTION

<u>ACT 25.326 (O.B. 11/02/2000)</u>	<u>REGULATORY DECREE 1558 (O.B. 12/03/2001)</u>
Personal data protection. General provisions. General principles concerning data protection. Rights of the owners of the data. Users and persons responsible of archives, registers and databases. Control. Sanctions. Action for the protection of personal data.	<u>REGULATION OF THE ACT N° 25.326</u> Regulation of the Act N° 25.326 is approved. General principles concerning data protection. Rights of the owners of the data. Users and persons responsible of archives, registers and databases. Control. Sanctions.
CHAPTER I - GENERAL PROVISIONS	CHAPTER I - GENERAL PROVISIONS
Purpose The purpose of this Act is the full protection of personal information recorded in data files, registers, banks or other technical means of data-treatment, either public or private for purposes of providing reports, in order to guarantee the honor and intimacy of persons, as well as the access to the information that may be recorded about such persons, in accordance with the provisions of Section 43, Third Paragraph of the National Constitution. The provisions contained in this Act shall also apply, to the relevant extent, to data relating to legal entities. In no case shall journalistic information sources or data bases be affected.	SECTION 1° For the purposes of this regulation, the concepts of archives, files, registers, databases and databanks intended to provide reports, include all those which are not intended exclusively for personal use, notwithstanding the circulation of the reports or information be for a charge or free of charge.
Definitions SECTION 2. - For purposes of this Act, the terms hereinafter mentioned shall have the following meanings: Personal data: Information of any kind referred to certain or ascertainable physical persons or legal entities. Sensitive data: Personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior. Data file, register, base or bank: These terms designate, interchangeably, any organized set of personal data which is subject to treatment or processing, either	SECTION 2° Non-regulated.

electronically or otherwise, whatever form its collection, storage, organization or access may take.

Data treatment : Systematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organization, storage, modification, relation, evaluation, blocking, destruction, and in general, the processing of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers.

Person responsible for a data file, register, bank or base: Physical person or legal entity, either public or private, owning a data file, register, bank or base.

Computerized data : Personal data subjected to electronic or automated treatment or processing.

Data owner: Any physical person or legal entity having a legal domicile or local offices or branches in the country, whose data are subject to the treatment referred to in this Act.

Data user : Any person, either public or private, performing in its, his or her discretion the treatment of data contained in files, registers or banks, owned by such persons or to which they may have access through a connection .

Data Dissociation: Treatment of personal data in such a way that the information obtained cannot be related to any certain or ascertainable person.

CHAPTER II
GENERAL PRINCIPLES GOVERNING THE PROTECTION OF DATA

CHAPTER II
GENERAL PRINCIPLES GOVERNING THE PROTECTION OF DATA

Data files - Lawfulness

The formation of data files is lawful when such data are duly registered, observing in the operation thereof the principles set by this Act, as well as the regulations arising therefrom.

Data files shall not have a purpose contrary to the laws or public order.

SECTION 3°

Non-regulated.

Quality of the Data

1.- The personal data collected for treatment purposes must be certain, appropriate, pertinent, and not excessive with reference to the scope within and purpose for which

SECTION 4°

In order to determine the loyalty and good faith when personal data is obtained, as well as the use it will have, it shall be analyzed the procedure carried out for its collection, and particularly the information that was given to the data owner according to section 6°

<p>such data were secured.</p> <p>2.- The collection of the data shall not be carried out using disloyal or fraudulent means, or in a manner contrary to the provisions of this Act.</p> <p>3.- The data subject to treatment shall not be used for any purpose or purposes which are different from or incompatible with those giving rise to their collection.</p> <p>4.- The data shall be accurate and updated, if necessary.</p> <p>5.- Any data totally or partially inaccurate, or incomplete, must be suppressed and replaced, or, as the case may be, completed, by the person responsible for the file or data base upon notification of the inaccuracy or incompleteness of the relevant information, without prejudice to the data owner's rights set forth in Section 16 of this Act.</p> <p>6.- The data must be stored in such a way that enables the data owner to exercise his or her right of access.</p> <p>7.- The data shall be destroyed once it has ceased to be necessary or relevant to the purposes for which it has been collected.</p>	<p>of the Act N° 25.326.</p> <p>When the collection of the information had been done by linking up or processing archives, registers, databases or databanks, the source of information and its intended use shall be analyzed. The out-of-date information shall be deleted by the user without being necessary any request on the part of the data owner.</p> <p>The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall monitor ex-officio the due compliance of this legal principle, and shall impose the corresponding penalties to the person responsible or user, when applicable.</p> <p>The NATIONAL BUREAU OF PERSONAL DATA PROTECTION, upon request or ex-officio in case of suspicion of illegality, shall check the due compliance with the legal and regulatory provisions concerning every stage of the use of personal data:</p> <ul style="list-style-type: none"> a) Legality of collection or personal information taking; b) Legality of exchange of data, and transfer to third parties, or in the interrelationship between them; c) Legality of cession itself; d) Legality of the mechanism used for internal and external control of the archive, register, database or databank.
<p>Consent</p> <p>1.- The treatment of personal data is unlawful when the data owner has not given his or her express consent, which must be given in writing, or through any other similar means, depending on the circumstances.</p> <p>The consent above, given with other statements, must appear in a prominent and express manner, together with the warnings set forth in Section 6 hereof.</p> <p>2.- The consent above shall not be deemed necessary when :</p> <ul style="list-style-type: none"> a. the data are secured from source of unrestricted public-access; b. are collected for the performance of the duties inherent in the powers of the State; c. consist of lists limited to name, national identity card number, taxing or 	<p>SECTION 5°</p> <p>The consent given by the data owner is that preceded by an explanation to him according to his social and cultural status, regarding the information referred to in section 6° of the Act N° 25.326.</p> <p>The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall establish the requirements for the consent to be given by means other than written notification, which should assure the authorship and integrity of the statement.</p> <p>The consent given for the treatment of personal data can be revoked at any time. Such revocation will not have retroactive effect.</p> <p>For the purposes of section 5°, sub-section 2 e) of the Act N° 25.326 the concept of financial entity comprises people affected by the Act N° 21.526 and credit card issuing companies, financial trustees, financial entities liquidated by the Central Bank of Argentina, and people who are specifically included by the enforcement authority</p>

<p>social security identification, occupation, date of birth and, domicile,</p> <p>d. arise from a contractual relationship, either scientific or professional of data owner, and are necessary for its development or fulfillment;</p> <p>e. refer to the transactions performed by financial entities, and arise from the information received from their customers in accordance with the provisions of Section 39 of Act Number 21.526.</p>	<p>indicated in the aforementioned Act.</p> <p>It is not necessary to get consent for the information described in sub-sections a), b), c) and d) of section 39 of the Act N° 21.526.</p> <p>Bank secrecy will never be affected, and the spreading of the information concerning passive transactions carried out between banks and their customers is forbidden, according to sections 39 and 40 of the Act N° 21.526.</p>
<p>Information</p> <p>Whenever personal data are requested, data owners shall be previously notified in an express and clear manner :</p> <p>a) The purpose for which the data shall be treated, and who their addressees or type of addressees may be;</p> <p>b) The existence of the relevant data file, register or bank, whether electronic or otherwise, and the identity and domicile of the person responsible therefor;</p> <p>c) The compulsory or discretionary character of the answers to the questionnaire the person is presented with, particularly, in relation to the data connected with in the following Section;</p> <p>d) The consequences of providing the data, of refusing to provide such data or of their inaccuracy;</p> <p>e) The possibility the party concerned has to exercise the right of data access, rectification and suppression.</p>	<p>SECTION 6°</p> <p>Non-regulated.</p>
<p>Types of data</p> <p>1.- No person can be compelled to provide sensitive data.</p> <p>2.- Sensitive data can be collected and subjected to treatment only in case there exist circumstances of general interest authorized by law, or with statistical or scientific purposes provided data owners cannot be identified.</p> <p>3.- It is prohibited to create files, banks or registers storing information that directly or indirectly reveals sensitive data. Without prejudice to the foregoing, the Catholic Church, religious associations, and political and labor organizations shall be entitled to</p>	<p>SECTION 7°</p> <p>Non-regulated.</p>

<p>keep a register of their members.</p> <p>4.- Data referring to criminal or other offense-commission records can be treated only by the competent public authorities, within the framework established by the corresponding laws and regulations.</p>	
<p>Health-related data</p> <p>Public or private health institutions, as well as medical science professionals are entitled to collect and treat such personal data as they relate to the physical or mental condition of patients who make use of their services or who are or may have been in their care, in pursuance of the principles of professional secret.</p>	<p>SECTION 8°</p> <p>Non-regulated.</p>
<p>Data security</p> <p>1. - The person responsible for or the user of data files must take such technical and organizational measures as are necessary to guarantee the security and confidentiality of personal data, in order to avoid their alteration, loss, unauthorized consultation or treatment, and which allow for the detection of any intentional or unintentional distortion of such information, whether the risks arise from human conduct or the technical means used.</p> <p>2. - It is prohibited to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security.</p>	<p>SECTION 9°</p> <p>The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall stimulate the cooperation among public and private sectors to create and implement measures, practices and procedures that arouse confidence in the information systems and the providing and handling methodologies.</p>
<p>Confidentiality duty</p> <p>1. - The responsible for and all persons taking part in any stage of the treatment of personal data have a professional secret duty in respect of the said data. Such duty shall subsist even after the relationship with the data file owner has expired.</p> <p>2. - The obligated party may be discharged from the confidentiality obligation by judicial resolution, and in case there exist substantiated reasons relating to public safety, national defense or public health.</p>	<p>SECTION 10°</p> <p>Non-regulated.</p>
<p>Communication of Data</p> <p>1.- The personal data subjected to treatment may be communicated only to meet the purposes directly related to the legitimate interests of the person responsible for data file and the recipient, and upon the consent previously given by the data owner, who must be informed about the purpose of such communication of data, and provided with an identification of the recipient or with the elements that enable him or her to identify such</p>	<p>SECTION 11°</p> <p>The provisions stated in section 5 of the Act N° 25.326 are applicable to the consent for the cession of data. In the particular case of public databases or archives of an official agency which according to its specific functions were intended to be released to the general public, the requirement concerning the legitimate interest of the grantee shall be</p>

<p>recipient.</p> <p>2.- The consent for the communication of data is revocable.</p> <p>3.- Consent is not required when:</p> <ul style="list-style-type: none"> a) A law so provides; b) There exist the circumstances set forth in Section 5, Paragraph 2; c) The communication of data takes place directly between governmental agencies, to the extent of their corresponding competencies; d) The communication of data made is of health-related personal data, and it is necessary for public health or emergency reasons, or for conducting epidemiological surveys; provided that the identity of the data owners is kept confidential by adequate dissociation means.; e) An information dissociation procedure had been applied, so that the persons to whom the information refers were unidentifiable. <p>4.- The recipient be subject to the same regulatory and legal obligations as the person responsible for data file, and the latter shall respond jointly and severally for the observance of such obligations before the controlling body and the relevant information owner.</p>	<p>considered implicit in the general interest that caused the unrestricted public access.</p> <p>The massive cession of personal data from public registers to private registers shall only be authorized by law or by the decision of an official responsible, if the information is accessible by the public and respect for the protection principles established in the Act N° 25.326 has been guaranteed. It shall be understood by personal data massive cession that which affects a collective group of people.</p> <p>The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall set the security standards applicable to the mechanisms of dissociation of data. The cessionary referred to in section 11, sub-section 4 of the Act N° 25.326 could be totally or partially exempt from all responsibility if he proves that the event causing the damage cannot be attributed to him.</p>
<p>International transfer</p> <p>1.- The transfer of any type of personal information to countries or international or supranational entities which do not provide adequate levels of protection, is prohibited.</p> <p>2.- The prohibition shall not apply in the following circumstances:</p> <ul style="list-style-type: none"> a) international judicial cooperation; b) exchange of medical information, when so required for the treatment of the party affected, or in case of an epidemiological survey, provided that it is conducted in pursuance of the terms of Paragraph e) of the foregoing Section; c) stock exchange or banking transfers, to the extent thereof, and in pursuance of the applicable laws; d) when the transfer is arranged within the framework of international treaties 	<p>SECTION 12°</p> <p>Banning to transfer personal data to countries or international or supranational entities which do not provide adequate levels of protection, is not in force when the data owner had not given express consent to the cession.</p> <p>Consent shall not be necessary in case of transfer of data from a public register which is legally constituted to provide the public with information and is open to consultation by the general public or any person that can prove legitimate interest, as long as the corresponding legal and regulatory conditions are satisfied.</p> <p>The NATIONAL BUREAU OF PERSONAL DATA PROTECTION is allowed to evaluate ex-officio or upon the request of the interested party, the level of protection provided by the rules of a State or international organization. If it concludes that a State or organization does not protect appropriately personal data, it shall submit to the NATIONAL EXECUTIVE POWER a decree project to issue such statement. The</p>

<p>which the Argentine Republic is a signatory to;</p> <p>e) when the transfer is made for international cooperation purposes between intelligence agencies in the fight against organized crime, terrorism and drug-trafficking.</p>	<p>project shall be endorsed by the Minister of Justice and Human Rights and the Minister of Foreign Affairs, International Commerce and Religion.</p> <p>The appropriate level of protection offered by a country or international organization shall be evaluated taking into account all the circumstances that concur in a data transfer; particularly it shall be considered the nature of the information, the aim and length of the treatment planned, their final destination, general and sectorial rules of law, in force in the corresponding country, as well as professional rules, codes of conduct and security measures in force in such places, or those applicable to the international and supranational organizations.</p> <p>It is understood that a State or international organization offers an adequate level of protection when it is directly derived from its legal system in force, or from self-regulation systems, or from the protection established by the contractual clauses that establish the personal data protection.</p>
<p>CHAPTER III RIGHTS OF DATA OWNERS</p>	<p>CHAPTER III RIGHTS OF DATA OWNERS</p>
<p>Right to Information</p> <p>Any person may request information from the competent controlling body regarding the existence of data files, registers, bases or banks containing personal data, their purposes and the identity of the persons responsible therefor. The register kept for such purpose can be publicly consulted, free of charge.</p>	<p>SECTION 13°</p> <p>Non-regulated.</p>
<p>Right of access</p> <p>1.- Data owners, once they have duly evidenced their identity, have the right to request and obtain information on their personal data included in public data registers or banks, or in private registers or banks intended for the provision of reports.</p> <p>2.- The person responsible or user shall provide the requested information within ten calendar days of being demanded of such request . Upon expiration of the said term without such request being answered, or if the report is deemed insufficient, the proceeding to protect personal data or habeas data herein provided for shall be started.</p> <p>3.- The right of access dealt with in this Section may only be exercised free of charge within intervals no shorter than six months, unless a legitimate interest to do otherwise is shown.</p>	<p>SECTION 14°</p> <p>The request referred to in section 14, sub-section 1 of the Act N° 25.326 does not require specific methods as long as it guarantees the identification of the owner. It can be made by the interested party directly to the person responsible or user of the archive, register, database or databank, or indirectly, by means of a written demand which leaves an acknowledgement of receipt. Other services of direct or semi-direct access can also be used, such as electronic means, telephone calls, on-line complaints or any other means valid for this purpose. In each case, preferred means to know the answer could be indicated.</p> <p>In the case of public databases or archives of an official agency which according to its specific function were intended to be released to the general public, the conditions to exercise the right to access could be proposed by the institution and approved by the NATIONAL BUREAU OF PERSONAL DATA PROTECTION, which shall assure that</p>

4.- In the event of death persons, their general heirs shall be entitled to exercise the right mentioned in this Section.

the procedures suggested do not either violate nor restrict in any way the warranties of that right.

The right to access shall permit:

- a) To know whether or not the data owner is in the archive, register, database, databank;
- b) To know all the information concerning his person included in the archive;
- c) To request information about the sources and means used to get his data;
- d) To ask about the purposes for which they were collected;
- e) To know their destination;
- f) To know if the archive is registered according to the requirements of the Act N° 25.326

Upon expiration of the term to answer stated in section 14, sub-section 2 of the Act N° 25.326, the interested party shall be able to carry out the protection of personal data and report the event before the NATIONAL BUREAU OF PERSONAL DATA PROTECTION.

In the event of dead persons, their general heirs shall prove their bonds by means of either the corresponding affidavit of heirship, or a written document that proves them as universal heirs of the interested party.

Information contents

- 1.- The information must be provided clearly, without any codes and, where applicable, enclosing an explanation of the terms used, in a language that is understood by a citizen with an average degree of education.
- 2.- The information must be extensive and deal with the full record corresponding to the owner, even in case the request submitted refers to only one item of personal data. In no case shall the report disclose information corresponding to third parties, even if such third parties are related to the requesting party.
- 3.- The information may, at the owner's option, be provided in writing, by electronic, telephonic, visual, or other adequate means for such purpose.

SECTION 15°

- 1.- The information must be provided clearly, without any codes and, where applicable, enclosing an explanation of the terms used, in a language that is understood by a citizen with an average degree of education.
- 2.- The information must be extensive and deal with the full record corresponding to the owner, even in case the request submitted refers to only one item of personal data. In no case shall the report disclose information corresponding to third parties, even if such third parties are related to the requesting party.
- 3.- The information may, at the owner's option, be provided in writing, by electronic, telephonic, visual, or other adequate means for such purpose.

Rectification, updating or suppression right

- 1.- Every person has the right to rectify, update, and when applicable, suppress or keep confidential his or her personal data included in a data bank.
- 2.- The person responsible for or the user of the data bank, must proceed to rectify, suppress or update the personal data belonging to the affected party, by performing the operations necessary for such purpose within the maximum term of five business days of the complaint being received or the mistake or false information being noticed.
- 3.- Noncompliance with such obligation within the term established in the preceding paragraph, will enable the interested party to bring, without any further proceedings, the action for the protection of personal data or habeas data contemplated in this Act.
- 4.- In the event of a data communication or transfer the person responsible for or the user of the data bank must notify the recipient of such rectification or suppression within five business days of the data treatment being effected.
- 5.- Such suppression must not be effected in the event it could cause harm to the rights or legitimate interests of third parties, or there existed a legal obligation to preserve such data.
- 6.- During the process for the verification and rectification of the relevant mistake or falsehood in the information, the person responsible for or the user of the data bank must either block the access to the file, or indicate, when providing the information relating thereto, the circumstance that such information is subject to revision.
- 7.- The personal data must be kept during the terms contemplated in the applicable provisions or, where appropriate, in the contractual relationships between the person responsible for or the user of the data bank and the data owner.

Exceptions

- 1.- The persons responsible for, or the users of public data banks, by means of a well grounded decision may deny the access to or the rectification or suppression of such data, based on national defense, public order, and safety grounds or the protection of rights and interests of third parties.
- 2.- The information about personal data may also be denied by the persons responsible for or users of public data banks when such information could hinder pending judicial or administrative proceedings relating to the compliance with tax or social security

SECTION 16°

In the provisions included in sections 16 up to 22 and 38 up to 43 of the Act N° 25.326 in which some of the rights to correction, updating, deletion and confidentiality are mentioned, it shall be understood that such rules refer to all of them.

In the case of public databases or archives created as a result of the cession of information provided by financial entities, pension funds management companies, insurance companies, and according to section 5, sub-section 2 of the Act N° 25.326, the rights to correction, updating, deletion and confidentiality shall be exercised before the grantor involved as a party in the legal relationship related to the contested data. If the complaint is sustained, the corresponding entity shall request the CENTRAL BANK OF ARGENTINA, the SUPERINTENDENCY OF PENSION FUNDS MANAGEMENT COMPANIES, or the NATIONAL SUPERINTENDENCY OF INSURANCE COMPANIES, whichever is applicable, to make the necessary changes in their databases. Every change shall be notified by the same means used to the spreading of the information.

The person responsible for or the user of the public databases or archives accessible to the public without restrictions can carry out the notification referred to in section 16, sub-section 4 of the Act N° 25.326 through the rectification of the data done by the same means used for its spreading.

SECTION 17°

Non-regulated.

<p>obligations, the performance of health and environment control functions, the investigation of crimes and the verification of administrative violations. The resolution so providing must be justified and notice thereof be given to the party concerned.</p> <p>3.- Notwithstanding the provisions of the foregoing paragraphs, access to the relevant records must be given at the time the affected party is to exercise his or her defense rights.</p>	
<p>Legislative Committees</p> <p>The National Defense Committee and the Bicameral Committee for the Control of Internal Security and Intelligence Agencies and Activities of the National Congress, and the Committee for Internal Security of the House of Representatives of the Nation, or any bodies that in the future may substitute them, shall have access to the data banks or files referred to in Section 23, Paragraph 2 for justified reasons and in respect of those areas as are the jurisdiction of such Committees.</p>	<p>SECTION 18°</p> <p>Non-regulated.</p>
<p>No charges applied</p> <p>The rectification, updating or suppression of inaccurate or incomplete personal data in public or private files shall be effected without any charge to the party concerned.</p>	<p>SECTION 19°</p> <p>Non-regulated.</p>
<p>Objection to personal assessments</p> <p>1.- Those judicial decisions or administrative acts involving an appreciation or assessment of human behavior shall not have as their only basis the result of the computerized treatment of personal data providing a definition of the profile or personality of the party concerned.</p> <p>2.- Any act contrary to the preceding provision shall be irremediably null.</p>	<p>SECTION 20°</p> <p>Non-regulated.</p>
<p>CHAPTER IV PERSONS RESPONSIBLE FOR OR USERS OF DATA BANKS, FILES, AND REGISTERS</p>	<p>CHAPTER IV PERSONS RESPONSIBLE FOR OR USERS OF DATA BANKS, FILES, AND REGISTERS</p>
<p>Registers of data files. Registration</p> <p>1.- Any private or public data file, register, base or bank intended to provide reports must be registered with the Registry to be established for such purpose by the controlling body.</p>	<p>SECTION 21°</p> <p>The registration of private archives, registers, databases and databanks intended to provide with information shall be enabled after this regulation is published in the Official Bulletin.</p> <p>Public and private archives, registers, databases and databanks referred to in section 1 of</p>

2.- The data file register shall include at least the following information:

- a) Name and domicile of the person in charge;
- b) Characteristics and purpose of the file;
- c) Nature of the personal data contained in each file;
- d) Form of collection and updating of data;
- e) Destination of the data and physical persons or legal entities to whom such data may be transmitted;
- f) Manner in which the registered information can be interrelated;
- g) Means used to guarantee the security of data, with the obligation to provide details of the category of persons with access to the information treatment process
- h) Data preservation term;
- i) Form and conditions under which persons may have access to data referring to them, and the procedures to be implemented for the rectification or updating of such data.

3.- No user of data shall be in possession of personal data of a nature that is different from the one stated in the register.

this regulation shall be registered.

For the purposes of registering the archives, registers, databases and databanks for the objective of publicity, the persons responsible shall proceed according to what is stated in section 27, fourth paragraph, of this regulation.

Public data banks, files or registers

1.- The regulations concerning the creation, modification or suppression of data banks, registers or files belonging to public bodies must be adopted by means of general provisions published in the National Official Gazette or in the official journal.

2.- The corresponding provisions shall set forth:

- a) Characteristics and purpose of the file;
- b) Persons in respect of whom data are requested, and the discretionary or compulsory character of the provision of such data by them;
- c) Procedures to obtain and update the data;

SECTION 22°

Non-regulated.

<p>d) Basic structure of the file, whether computerized or not, and a description of the nature of the personal data to be contained therein;</p> <p>e) the contemplated communications, transfers or interconnections;</p> <p>f) bodies responsible for the file, with an indication of the hierarchical instrumentality of such body;</p> <p>g) the offices to which claims may be submitted in connection with the exercise of access, rectification or suppression rights.</p> <p>3.- The provisions that shall be established for deleting computerized registers will indicate the destiny or the measures adopted for the destruction thereof.</p>	
<p>Special cases</p> <p>1.- Personal data, which on account of their having been stored for administrative purposes, must be subjected to permanent registration with the data banks belonging to the armed forces, security forces, police or intelligence agencies shall be subject to the provisions of this law, the same principle applying to such data on personal background as are provided by the said banks to the administrative or judicial authorities that may require them by virtue of legal provisions.</p> <p>2.- The treatment of personal data with national defense or public security purposes by the armed forces, security forces, police or intelligence agencies, without the consent of the parties concerned, is limited to those cases and categories of data as are necessary for the strict compliance with the duties legally assigned to such bodies for the national defense, public security or the punishment of crimes. In those cases, files must be specific, and established for the said purpose, and they shall be classified by categories, depending on their degree of reliability.</p> <p>3.- Personal data registered with police purposes shall be canceled when not deemed necessary for the inquiries which gave rise to their storage.</p>	<p>SECTION 23°</p> <p>Non-regulated.</p>
<p>Private data banks, registers or files</p> <p>Private persons forming data banks, registers or files which are not intended for an exclusively personal use must be registered in accordance with the provisions of Section 21.</p>	<p>SECTION 24°</p> <p>Non-regulated.</p>
<p>Provision of computerized services involving personal data</p>	<p>SECTION 25°</p>

1.- When personal data treatment services are provided for the account of third parties, such data cannot be applied or used with any purpose other than the one appearing on the corresponding contract for the provision of the service, nor can such data be communicated to other parties, even for storage purposes.

2.- Once the corresponding contractual obligations have been performed, the treated personal data must be destroyed, except in case there is an express authorization given by the person for account of whom such services are rendered, by reason of a possibility of the data being used for future services, in which case the data may be stored under due security conditions for a maximum term of up to two years.

Contracts for the provision of services involving the treatment of personal data must have the levels of security established in the Act N° 25.326, this regulation and the complementary rules dictated by the NATIONAL BUREAU OF PERSONAL DATA PROTECTION, as well as the tenant's obligations that arise concerning the confidentiality that should be kept about the information obtained.

The performance of data treatment services must be regulated by a contract that links the person in charge of the provision of the service and the person responsible or user of such service, as well as particularly states:

- a) That the person in charge of the data treatment service shall only act following the instructions of the person responsible of the treatment
- b) That the obligations stated in section 9 of the Act N° 25.326 are also incumbent on the person in charge of the data treatment service.

Provision of credit information services

1.- In the provision of credit information services only personal data of a pecuniary character relevant for the evaluation of the economic solvency and the credit of a person can be treated, such data to be obtained from sources accessible to the public or arising from reports provided by the party concerned or with his or her consent.

2.- The information may also be personal data relating to the performance or non-performance of pecuniary obligations, provided by the creditor or by a person acting for his or her account or in his or her interest.

3.- At the request of the data owner, the person responsible for or the user of the data bank, shall communicate the reports, evaluations, and appraisals provided about him or her over the last six months together with the name and domicile of the recipient, in the event such data were obtained by communication of data.

4.- Only personal data relevant to assess the economic and financial solvency of the parties concerned over the last five years can be filed, registered or communicated. Said term shall be reduced to two years when debtor pays off or settles the obligation in any other way, and this fact shall be included in the report.

5.- The provision of credit information services shall not require the prior consent of the data owner to the purposes of the communication of data, or the subsequent transmission thereof, when such data are related to the commercial or credit activities of the

SECTION 26°

For the purposes stated in section 26, sub-section 2, of the Act N° 25.326, personal data related to the performance or non-performance of pecuniary obligations, mutual agreements, current accounts, credit cards, trust agreements, leasing and loans in general, and any other obligation of patrimonial nature, as well as those that show the level of performance and the qualification in order to determine without any doubt the content of the information issued.

In the case of public databases or archives from an official entity intended to be released to the general public, the obligations stated in section 26, sub-section 3, of the Act N° 25.326 shall be considered fulfilled as long as the person responsible for the database notify the data owner of any information, assessment or appreciation that had been done upon those files and spread during the last SIX (6) months.

In order to evaluate somebody's economic and financial solvency, according to section 26, sub-section 4, of the Act N° 25.326, it shall be taken into account all the available information from the beginning up to the expiry date of every obligation. To count FIVE (5) years, they shall be considered from the date when the last adverse piece of information that indicates the debt was demandable was filed. If the debtor proves that the last available piece of information coincides with the expiration of the debt, the term shall be reduced to TWO (2) years. For data about performance of the obligations before their due date, there shall be no time to delete them.

<p>recipients.</p>	<p>In order to calculate the term of TWO (2) years for the maintenance of the data when the debtor had paid off or settled the obligation, the exact expiry date of the debt shall be taken into account.</p> <p>For the purposes of fulfilling what is stated in section 26, sub-section 5 of the Act N° 25.326, the CENTRAL BANK OF ARGENTINA shall restrict the access to their databases available on the Internet, except for those cases concerning information about natural persons, demanding the input of the ID number or CUIL (Workers Identification Number) of the data owner, which had been obtained by the cessionary through a previous commercial or contractual relationship.</p>
--------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Data files, registers or banks with advertising purposes</p> <p>1.- Data suitable to establish certain profiles with promotional, commercial or advertising purposes may be treated in the collection of domiciles, distribution of documents, advertising or direct sales and other similar activities. This shall also include data which permit to determine consumption habits, when such data appear on documents which are accessible to the public or have been provided by the owners themselves or have been obtained with their consent.</p> <p>2.- In the instances contemplated in this Section, the data owner may exercise the right of access free of any charge.</p> <p>3.- The owner may at any time request the withdrawal or blocking of his name from any of the data banks referred to in this Section.</p>	<p>SECTION 27°</p> <p>Data with advertising purposes could be collected, treated and transferred without the consent of the owner when it was intended to be used in the formation of specific profiles that categorize similar preferences and habits, as long as the data owners are only identified by their belonging to those generic groups, plus their personal information strictly necessary to make the offer to the recipient.</p> <p>Chambers, associations and professional organizations of the sector that have a Code of Conduct approved by the NATIONAL BUREAU OF PERSONAL DATA PROTECTION, to which their members adhere by bylaws, along with the enforcement authority, shall implement within NINETY (90) days following the issuing of this regulation, a method of blocking or deletion on the part of the owner of the piece of information that must be excluded from the databases with advertising purposes. The deletion could be total or partial to blocking, strictly upon the owner's request, the use of some of the means of communication, such as mail, telephone, e-mails or others.</p> <p>In every communication with advertising purposes done by mail, telephone, email, Internet or other means to be known, the data owner's possibility to ask for the total or partial deletion and blocking of his name from the database shall be expressly indicated and highlighted. Upon the request of the interested party, the name of the person responsible or user of the databank that provided the information shall be informed.</p> <p>For the purposes of guaranteeing the right to information in section 13 of the Act N° 25.326, only chambers, associations and professional organizations of the sector that have a Code of Conduct approved by the NATIONAL BUREAU OF PERSONAL DATA PROTECTION, to which their members adhere by bylaws, shall be registered. At the moment of their registration, the chambers, associations and professional</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>organizations shall provide a list of their members indicating their names, surnames and domiciles.</p> <p>The person responsible or user of the archives, registers, databases and databanks for advertising purposes who does not adhere to any Code of Conduct, shall register in the Registry mentioned in section 21 of the Act N° 25.326.</p> <p>The information related to the health condition could only be treated for purposes of making offers of goods and services, as long as they were obtained according to the Act N° 25.326, and they could not arouse discrimination, in a context of consumer–supplier of medical services/treatments or non-profit organization relationship. That information could not be transferred to third parties without previous express consent of the data owner. For that purpose, the data owner shall be clearly informed of the delicate nature of the information he is giving out and the fact that he is not forced to provide with them, as well as the content of sections 6 and 11, sub-section 1, of the Act N° 25.326 and the possibility he has of requesting the deletion or blocking in the database of his information.</p>
<p>Data files, registers or banks relating to opinion polls</p> <p>1.- The regulations contained in this Act shall not apply to opinion polls, surveys or statistics collected pursuant to Law No. 17,622, market research works, scientific or medical research, and other similar activities, to the extent that the data collected cannot be attributed to a certain or ascertainable person.</p> <p>2.- If in the data collection process it were not possible to keep the anonymity of the relevant person, a dissociation technique shall be used, so that no particular person may be identified.</p>	<p>SECTION 28°</p> <p>Archives, registers, databases and databanks mentioned in section 28 of the Act N° 25.326 are responsible and subject to the fines established in section 31 of the aforementioned Act when they infringe its regulations.</p>
<p>CHAPTER V CONTROL</p>	<p>CHAPTER V CONTROL</p>
<p>Controlling Body</p> <p>1.- The controlling body shall take all actions necessary to the compliance with the objectives and other provisions of this Act. To such purposes, it will have the following functions and powers:</p> <p>a) Give any requesting party assistance and advise on the scope of this Act and the legal means available for the defense of the rights guaranteed by the same;</p>	<p>SECTION 29°</p> <p>1) The NATIONAL BUREAU OF PERSONAL DATA PROTECTION, in the domain of the SECRETARY OF JUSTICE AND LEGISLATIVE AFFAIRS of the MINISTRY OF JUSTICE AND HUMAN RIGHTS is created as a controlling body for the Act N° 25.326.</p> <p>The Director shall be exclusively devoted to his functions, which he will</p>

- b) Pronounce the rules and regulations to be observed in the development of the activities covered by this Act;
- c) Do a census of data files, registers or banks covered by the Act and keep a permanent record thereof;
- d) Control compliance with the norms on data integrity and security by data files, registers or banks. To such purpose it shall be entitled to request the corresponding judicial authorization to access data treatment premises, equipment or software in order to verify violations of this Act;
- e) Request information from public and private entities, which shall furnish the background, documents, software or other elements relating to personal data that such entities may be required. In these cases, the authorities shall guarantee the security and confidentiality of the information and elements supplied;
- f) Enforce the administrative sanctions that may apply for the violation of the norms set forth in this Act and the regulations passed as a consequence thereof;
- g) Assume the role of accuser in criminal actions brought for violations of this Act.
- h) Control fulfillment of requirements and guarantees to be met by private files or banks which provide reports to obtain the corresponding registration with the Register created by this Act.

The Director shall exclusively devote to his or her functions, shall be subject to the incompatibility provisions set forth by law for public officers and may be removed from office by the Executive Branch on account of wrong fulfillment of his or her duties.

exercise in full autonomy, and shall not be subject to any instruction.

- 2) The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall be formed by a National Director, Level "A" with Executive Function I, designated by the NATIONAL EXECUTIVE POWER, for a term of FOUR (4) years, and shall be elected among other people with experience in this field by the Minister of Justice and Human Rights or his deputy, as an exception to the Annex I of the Decree N° 993/91 and its amendments.

The Bureau will count on the personnel designated by the Ministry of Justice and Human Rights resorting to human resources existent in the NATIONAL PUBLIC ADMINISTRATION. The personnel shall keep secrecy regarding the personal data that handle during their work.

Within THIRTY (30) business days from the day he assumed the post, the National Director shall submit a project concerning the organizational structure and internal regulation to the NATIONAL EXECUTIVE POWER for him to approve it and broadcasting it in the Official Bulletin.

- 3) The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall be financed with:
 - a) The funds collected as fees for the services provided;
 - b) The funds derived from the fines established in section 31 of the Act N° 25.326;
 - c) The budgetary allocation included in the Budget of the National Administration Law from the year 2002.

Transitorily, since the effective date of this regulation until December 31, 2001, the cost of the structure shall be afforded with the budgetary credit corresponding to the MINISTRY OF JUSTICE AND HUMAN RIGHTS for the year 2001, without prejudice to what is stated in points a) and b) of the previous paragraph.

- 4) The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall have an Advisory Council that will work pro-bono and shall be in charge of advising the National Director in significant issues, and will be constituted by:

- A representative of the MINISTRY OF JUSTICE AND HUMAN RIGHTS;
- A magistrate of the PUBLIC FISCAL MINISTRY;
- A representative of the public archives which purpose is to provide with information, designated by the Chamber that groups the national credit information entities;
- A representative of the ARGENTINE FEDERATION OF COMMERCIAL DATA BUSINESS ORGANIZATIONS;
- A representative of the CENTRAL BANK OF ARGENTINA;
- A representative of the business organizations which purpose is stated in section 27 of the Act N° 25.326, designated by common consent of the respective Chambers;
- A representative of the FEDERAL CONSUMER ADVISORY COUNCIL;
- A representative of the IRAM, the Argentine Institute of Normalization, specialized in Information technology Security;
- A representative of the NATIONAL SUPERINTENDENCY OF INSURANCE COMPANIES;
- A representative of the Bicameral Committee for the Control of Internal Security and Intelligence Agencies and Activities of the NATIONAL CONGRESS

The entities mentioned above are invited to designate the representatives that shall integrate into the Advisory Council.

- 5) The following are the functions of the NATIONAL BUREAU OF PERSONAL DATA PROTECTION apart from those established in the Act N° 25.326:
 - a) To make the administrative and procedural rules related to registration proceedings and other functions of the bureau, and technical rules and procedures related to the treatment and security conditions of public and private archives, registers, databases and databanks:
 - b) To deal with complaints related to the treatment of personal data according to

	<p>the Act N^a 25.326.</p> <ul style="list-style-type: none"> c) To collect the fees established for the services of registration and others it offers; d) To organize and provide with it be necessary for the adequate operation of the Registry of public and private archives, registers, databases and databanks established in section 21 of the Act N^a 25.326; e) To elaborate the necessary tools suitable for the best citizens data protection and the best fulfilment of the applicable legislation; f) To approve the codes of conduct that are submitted according to section 30 of the Act N^a 25.326, after report of the Advisory Council, taking into account their adaptation to the regulatory principles for the personal data treatment, the representation exercised by the association and organization that elaborates the code, and its executive efficacy related to the operators of the sector through the provision of penalties or appropriate mechanisms.
<p>Codes of conduct</p> <p>1.- The associations or entities representing persons responsible for or users of privately-owned data banks may create professional practice codes of conduct, establishing the rules for the treatment of personal data tending to assure and improve the operational conditions of information systems on the basis of the principles established by this Act.</p> <p>2.- Such codes shall be registered with the register kept by the controlling body, who may deny registration whenever it considers that the said codes do not conform with the legal and regulatory provisions governing the matter.</p>	<p>SECTION 30°</p> <p>The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall encourage the creation of codes of conduct for the purpose of contribution to, depending on the characteristics of each sector, the proper application of the national rules stated in the Act N^a 25.326 and this regulation.</p> <p>The professional associations and other organizations that represent other categories of person responsible or users of public or private archives, registers, databases or databanks, which had developed projects of Ethics codes, or had the intention to modify or extend the validity of the existent national codes, could submit those projects to the NATIONAL BUREAU OF PERSONAL DATA PROTECTION for it to consider them. The bureau shall approve it or suggest the changes that it consider necessary for its approval.</p>
<p>CHAPTER VI SANCTIONS</p>	<p>CHAPTER VI SANCTIONS</p>
<p>Administrative sanctions</p> <p>1.- Without prejudice to the administrative responsibilities that may apply in the case of public data users or persons responsible therefor; in any case, in addition to the liability</p>	<p>SECTION 31°</p> <p>1. The administrative sanctions established in section 31 of the Act N^o 25.326 shall be applied to persons responsible or users of archives, files, registers, data</p>

for damages arising from the non-observance of this Act, and the applicable criminal penalties, the controlling body may apply sanctions consisting in a warning, suspension, or a fine ranging between one thousand pesos (\$1,000.-) and one hundred thousand pesos (\$100,000.-), closure or cancellation of the file, register or data base.

2.- The applicable regulations shall determine the conditions and procedures for the application of the above mentioned sanctions, which shall be graded in proportion to the seriousness and extent of the violation and the damages arising from such violations, guaranteeing the due process of law principle.

bases and data banks intended to provide reports, which would have registered or not in the corresponding registry. The amount of the sanctions shall be adjusted according to the nature of the personal rights affected, the quantity of treatments done, the benefits gained, the degree of intent, the recidivism, the damages caused to interested persons and third parties, and any other circumstance that be relevant to determine the degree of illegality and guilt present in the specific offense. It shall be considered as a recidivist someone who, having been sanctioned for an infringement of the Act N° 25.326 or its regulations, commits another infringement of similar characteristics within THREE (3) years from the application of the sanction.

2. The funds collected with the fines referred in section 31 of the Act N° 25.326 shall be applied for the financing of the NATIONAL BUREAU OF PERSONAL DATA PROTECTION.
3. The procedure shall respect the following provisions:
 - a) The NATIONAL BUREAU OF PERSONAL DATA PROTECTION shall start administrative actions in case of alleged infringement to the provisions of Act N° 25.326 and its regulations, ex-officio upon a denounce submitted by someone that cite a particular interest, by the Ombudsman, or by consumers associations.
 - b) A report shall be written in which it shall be expressly stated the event reported or checked and the provision allegedly infringed. In the same report, the documentation submitted shall be added and the alleged offender shall be summoned so that, within FIVE (5) business days, he submit his defense and evidence to prove his right. If it were an inspection record that requires a subsequent technical verification in order to determine the alleged infraction and it results positive, the alleged offender of such infraction shall be notified and summoned to submit his written defense within FIVE (5) business days. In his first submission, the alleged offender shall establish domicile and certify his legal status. The proof of the report written according to the provisions of this section, as well as the technical verifications provided, shall be sufficient evidence of the proven event, except when it turn out distorted by other evidence.
 - c) Evidence shall be accepted only when controversial events exist and as long as they do not turn out overtly irrelevant. Against the resolution that

	<p>denies means of evidence it shall only be granted an appeal of reconsideration. The proof shall occur within a period of TEN (10) business days, extendable only because of justified causes, and those which do not occur within the aforementioned period due to a cause attributable to the offender shall be withdrawn.</p> <p>When the investigative proceedings conclude, the final decision shall be issued within TWENTY (29) business days.</p>
<p>Criminal penalties</p> <p>1.- The following provision shall be included in the Argentine Criminal Code as Section 117 bis:</p> <ol style="list-style-type: none"> 1.- A penalty of imprisonment for the term of one month to two years shall correspond to anyone who knowingly inserts or has false information inserted in a personal data file. 2.- The penalty shall be of six months to three years to anyone who knowingly provides a third party with false information contained in a personal data file. 3.- The punishment scale shall be increased in one half of the minimum and the maximum penalties when a person is harmed as the result of the above mentioned action. 4.- When the offender or the person responsible for the offense is a public official in exercise of his duties, an accessory penalty consisting in the disqualification to occupy public offices for a term which shall double the one of the criminal penalty shall be applied. <p>2.- The following provision shall be included in the Argentine Criminal Code as Section 157 bis:</p> <p>A penalty of six months to three years of imprisonment shall be applied to anyone who:</p> <ol style="list-style-type: none"> 1. Knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into a personal data bank; 2. Discloses to third parties information registered in a personal data bank which should be kept secret by provision of law. <p>When the offender is a public officer, an accessory penalty consisting in a special</p>	<p>SECTION 32°</p> <p>Non-regulated.</p>

<p>disqualification for a term from one to four years shall be applied.</p>	
<p>CHAPTER VII ACTION FOR THE PROTECTION OF PERSONAL DATA</p>	<p>CHAPTER VII ACTION FOR THE PROTECTION OF PERSONAL DATA</p>
<p>Legal Basis of a Complaint</p> <p>The action for the protection of personal data or of habeas data shall be applicable:</p> <ul style="list-style-type: none"> a. to acquire knowledge of personal data stored in public or private data files, registers or banks intended for the provision of reports, as well as purposes thereof; b. to those cases in which the falsehood, inaccuracy or outdating of the relevant information is presumed, and the treatment of such data whose registration is prohibited by this Act, in order to demand their suppression, rectification, confidentiality or updating. 	<p>SECTION 33°</p> <p>Non-regulated.</p>
<p>Persons entitled to bring the action</p> <p>The action for the protection of personal data or of habeas data may be brought by the affected party, guardian or curator thereof, and the successors of physical persons, whether they are direct or collateral descendants of such persons up to the second degree, be it by him or herself or through an attorney.</p> <p>When the action is brought by legal entities, it must be brought by the legal representatives or agents appointed by them to such purpose.</p> <p>The Ombudsman may join the party concerned in the process.</p>	<p>SECTION 34°</p> <p>Non-regulated.</p>
<p>Parties against whom the action may be brought</p> <p>The action shall apply in respect of public or private data banks users and persons responsible therefore. In the case of private ones, it shall apply in the event such users and persons responsible have the purpose of providing reports.</p>	<p>SECTION 35°</p> <p>Non-regulated.</p>
<p>Jurisdiction</p> <p>This action may be brought before the court corresponding to the domicile of the plaintiff; the court corresponding to the domicile of the defendant; or the place in which the fact or event giving rise to the action materializes or may have effect, at the</p>	<p>SECTION 36°</p> <p>Non-regulated.</p>

<p>plaintiff's option.</p> <p>The federal jurisdiction shall apply:</p> <ul style="list-style-type: none">a. when the action is brought against public data files of national bodies, andb. when data files are interconnected in interjurisdictional, national or international networks.	
<p>Applicable procedure</p> <p>The habeas data action shall proceed in accordance with the provisions of this Act and the procedure corresponding to the ordinary action for the protection of constitutional rights (Amparo), and subsidiarily in accordance with the provisions of the National Code of Civil and Commercial Procedure as regards specially expedited summary proceedings.</p>	<p>SECTION 37°</p> <p>Non-regulated.</p>
<p>Requirements of the complaint</p> <p>1.- The complaint shall be filed in writing, identifying as accurately as possible the name and domicile or the data file, register or bank, as well as the name of the user or person responsible therefor.</p> <p>In the case of public files, registers or banks, an attempt shall be made to identify the governmental body in charge of them.</p> <p>2.- The plaintiff shall state the reasons why he understands that the identified data file, register or bank contains information about him or her; the reasons why he or she considers that such information about him or her is discriminatory, false or inaccurate, and evidence of compliance with the corresponding provisions so that the rights protected by this Act could be protected.</p> <p>3.- The affected party may request that, while the proceeding is taking place, the data register or bank records that the information concerned is being subject to legal proceeding.</p> <p>4.- The competent judge shall be entitled to order the provisional blocking of the file, with respect to the personal data giving rise to the legal action, when it is evident that the relevant information is discriminatory, false or inaccurate.</p> <p>5.- To the purposes of requesting information from the file, register or bank involved, the judicial criterion for the assessment of the circumstances contemplated in Paragraphs 1.-</p>	<p>SECTION 38°</p> <p>Non-regulated.</p>

and 2. shall be broad.	
<p>Procedures</p> <p>1.- Upon the action being admitted, the Court shall require the data file, register or bank to submit all the information concerning the plaintiff. The Court shall also be entitled to request information on the technical support of the data, basic documentation referring to the collection of data, and any other aspect deemed relevant to the solution of the case.</p> <p>2.- The term to answer the information request shall not be longer than five business days, which may be reasonably extended by the Court.</p>	<p>SECTION 39°</p> <p>Non-regulated.</p>
<p>Confidentiality of the information</p> <p>1.- The private data registers, files or banks may not allege confidentiality of the information required of them, except in case press information sources are affected.</p> <p>2.- When public data files, registers, or banks object to the submission of the requested report by raising the exceptions to the right of access, rectification or suppression authorized by this Act or in any specific Act, they shall furnish evidence as to the circumstances rendering the said legal exceptions applicable. In such cases, the judge shall be entitled to have personal and direct knowledge of the requested data securing confidentiality thereof.</p>	<p>SECTION 40°</p> <p>Non-regulated.</p>
<p>Answer to information requests</p> <p>In answering the information request, the data file, register or bank shall state the reasons why it included the questioned information, and the reasons why it did not meet the requirement of the party concerned, in pursuance of Sections 13 and 15 of this Act.</p>	<p>SECTION 41°</p> <p>Non-regulated.</p>
<p>Amended complaint</p> <p>Once the report has been answered, plaintiff may, within a three day term, extend the subject matter of the complaint by requesting the deletion, correction, confidentiality or updating of the personal data, in the events which are subject to the application of this Act. The same writing shall include the pertaining evidence thereof and shall be forwarded to defendant for a three day term.</p>	<p>SECTION 42°</p> <p>Non-regulated.</p>
<p>Judgment</p> <p>1.- Upon expiration of the term to answer the information request or upon answering such information request, and in the case provided for in Section 42, after the amended</p>	<p>SECTION 43°</p> <p>Non-regulated.</p>

<p>complaint has been answered, and after proof has been produced, if applicable, the Court shall render judgment.</p> <p>2.- In case the action is deemed legally based, an indication shall be given as to whether the information must be suppressed, rectified, updated or declared confidential, establishing a term for compliance with the court decision.</p> <p>3.- The rejection of the action shall not imply a presumption as to the liability the plaintiff may have incurred.</p> <p>4.- In any case, the judgment shall be communicated to the controlling body, which shall keep a record to such purpose.</p>	
<p>Venue</p> <p>The provisions of this Act set forth in Chapters I, II, III, and IV, and Section 32 shall be of public order and be applicable, to the relevant extent, all over the national territory.</p> <p>Provinces are hereby encouraged to adhere to those provisions of this Act as may be of an exclusively national jurisdiction.</p> <p>The federal jurisdiction shall apply in respect of data registers, files, or banks interconnected via national or international interjurisdictional networks.</p>	<p>SECTION 44°</p> <p>Non-regulated.</p>
<p>SECTION 45°</p> <p>The National Executive Power shall adopt the regulations for the implementation of this Act and establish the controlling bodies within one hundred and eighty days of its promulgation.</p>	<p>SECTION 45°</p> <p>Non-regulated.</p>
<p>Transitory provision</p> <p>The data files, registers, bases or banks intended to provide reports, existing at the moment when this Act is enacted, shall be recorded with the registry to be established in pursuance of Section 21, and conform to the provisions of the current legal regulations within the term established for such purpose by the regulations.</p>	<p>SECTION 46°</p> <p>Non-regulated.</p>
<p>SECTION 48.- Notify the Executive Power of This Act.</p>	