



[www.limeres.com](http://www.limeres.com) :: Limeres, Attorneys :: Tel. Arg.: +54 (9-11) 4162-0021 :: Tel. USA:  
+1 (650) 690-7050 / +1 (650) 395-7313 :: Skype: slimeres :: Limeres.com

## **ARGENTINA PERSONAL DATA PROTECTION ACT NUMBER 25326**

### ACT 25.326.

Enactment: October 4th, 2000

Partial Promulgation: October 30th, 2000

The Senate and the House of Representatives of Argentina met in Congress, etc. and enacted the following Act:

#### Chapter I

#### General Provisions

#### SECTION 1.- Purpose

The purpose of this Act is the comprehensive protection of personal information recorded in files, records, databases, databanks or other technical means of data treatment, either public or private for purposes of providing reports, in order to guarantee the right of individuals to their honor and privacy, as well as the access to information recorded thereupon, 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 2. - Definitions

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, database or databank: These terms designate, interchangeably, any organized set of personal data which is subject to treatment or processing, either 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 data files, registers, databases or databanks, 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

#### SECTION 3. - 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 there from.

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

#### SECTION 4. - 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 such data were secured.

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.

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.

4.- The data shall be accurate and updated, if necessary.

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.

6.- The data must be stored in such a way that enables the data owner to exercise his or her right of access.

7.- The data shall be destroyed once it has ceased to be necessary or relevant to the purposes for which it has been collected.

#### SECTION 5. - Consent

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.

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.

2.- The consent above shall not be deemed necessary when :

- 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 social security identification, occupation, date of birth, domicile and telephone number;
- d) arise from a contractual relationship, either scientific or professional of data owner, and are necessary for its development or fulfillment. 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.

#### SECTION 6. - Information

Whenever personal data are requested, data owners shall be previously notified in an express and clear manner:

- a) The purpose for which the data shall be treated, and who their addressees or type of addressees may be;
- b) The existence of the relevant data file, register or bank, whether electronic or otherwise, and the identity and domicile of the person responsible therefore;
- 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;
- d) The consequences of providing the data, of refusing to provide such data or of their inaccuracy;
- e) The possibility the party concerned has to exercise the right of data access, rectification and suppression.

#### SECTION 7. - Types of data

- 1.- No person can be compelled to provide sensitive data.
- 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.
- 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 keep a register of their members.
- 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.

#### SECTION 8.- Health-related data

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.

#### SECTION 9.- Data security

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.
2. - It is prohibited to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security.

#### SECTION 10. - Confidentiality duty

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.

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.

#### SECTION 11.- Communication of Data

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 recipient.

2.- The consent for the communication of data is revocable.

3.- Consent is not required when:

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.

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 Agency and the relevant information owner.

#### SECTION 12.- International transfer

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.

2.- The prohibition shall not apply in the following circumstances:

- 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 which the Argentine Republic is a signatory to;
- e) when the transfer is made for international cooperation purposes between intelligence agencies in the fight against organized crime, terrorism and drug-trafficking.

### Chapter III

#### Rights of Data Owners

##### SECTION 13. - Right to Information

Any person may request information from the competent controlling Agency 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.

##### SECTION 14. - Right of access

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.

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.

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.

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

#### SECTION 15. - 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 16. - 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.

#### SECTION 17. - 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 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.

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.

#### SECTION 18. - Legislative Committees

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.

#### SECTION 19. - No charges applied

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.

## SECTION 20. - Objection to personal assessments

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.

2.- Any act contrary to the preceding provision shall be irretrievably null.

## Chapter IV

Persons responsible for or users of data banks, files, and registers

## SECTION 21.- Registers of data files. Registration

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 Agency.

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.

## SECTION 22. - 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;

d) Basic structure of the file, whether computerized or not, and a description of the nature of the personal data to be contained therein;

e) the contemplated communications, transfers or interconnections;

f) bodies responsible for the file, with an indication of the hierarchical instrumentality of such body;

g) the offices to which claims may be submitted in connection with the exercise of access, rectification or suppression rights.

3.- The provisions that shall be established for deleting computerized registers will indicate the destiny or the measures adopted for the destruction thereof.

## SECTION 23. - Special cases

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.

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.

3.- Personal data registered with police purposes shall be canceled when not deemed necessary for the inquiries which gave rise to their storage.

#### SECTION 24. - Private data files, registers, databases or databanks

Private persons forming data files, registers, databases or databanks which are not intended for an exclusively personal use must be registered in accordance with the provisions of Section 21.

#### SECTION 25. - Provision of computerized services involving personal data

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.

#### SECTION 26. - 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 recipients.

#### SECTION 27. - Data files, registers or banks with advertising purposes

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.

2.- In the instances contemplated in this Section, the data owner may exercise the right of access free of any charge.

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.

#### SECTION 28. - Data files, registers, databases or databanks relating to opinion polls

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.

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.

## Chapter V

### Control

#### SECTION 29. - Controlling Agency

1.- The controlling Agency 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:

- 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;
- 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 datafiles, registers, databases or databanks. 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.

#### SECTION 30. - Codes of conduct

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.

2.- Such codes shall be registered with the register kept by the controlling Agency, who may deny registration whenever it considers that the said codes do not conform with the legal and regulatory provisions governing the matter.

## Chapter VI

### Sanctions

#### SECTION 31. - Administrative sanctions

1.- Without prejudice to the administrative responsibilities that may apply in the case of public data users or persons responsible therefore; in any case, in addition to the liability for damages arising from the non-observance of this Act, and the applicable criminal penalties, the controlling Agency 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.

#### SECTION 32. - Criminal penalties

1.- The following provision shall be included in the Argentine Criminal Code as Section 117 bis:

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.

2.- The following provision shall be included in the Argentine Criminal Code as Section 157 bis:

A penalty of six months to three years of imprisonment shall be applied to anyone who:

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.

When the offender is a public officer, an accessory penalty consisting in a special disqualification for a term from one to four years shall be applied.

## Chapter VII

### Action for the protection of personal data

#### SECTION 33. - Legal Basis of a Complaint

1) The action for the protection of personal data or of habeas data shall be applicable:

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.

#### SECTION 34. - Persons entitled to bring the action

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.

When the action is brought by legal entities, it must be brought by the legal representatives or agents appointed by them to such purpose.

The Ombudsman may join the party concerned in the process.

#### SECTION 35. - Parties against whom the action may be brought

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.

#### SECTION 36. - Jurisdiction

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 plaintiff's option.

The federal jurisdiction shall apply:

- a) when the action is brought against public data files of national bodies, and
- b) when data files are interconnected in inter-jurisdictional, national or international networks.

#### SECTION 37. - Applicable procedure

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, and in subsidy in accordance with the provisions of the National Code of Civil and Commercial Procedure as regards specially expedited summary proceedings.

#### SECTION 38. - Requirements of the complaint

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 therefore.

In the case of public files, registers or banks, an attempt shall be made to identify the governmental Agency in charge of them.

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.

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.

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.

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.- and 2. shall be broad.

#### SECTION 39. - Procedures.

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.

2.- The term to answer the information request shall not be longer than five business days, which may be reasonably extended by the Court.

#### SECTION 40. - Confidentiality of the information

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.

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.

#### SECTION 41. - Answer to information requests

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.

#### SECTION 42.- Amended complaint.

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.

#### SECTION 43. - Judgment

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 complaint has been answered, and after proof has been produced, if applicable, the Court shall render judgment.

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.

3.- The rejection of the action shall not imply a presumption as to the liability the plaintiff may have incurred.

4.- In any case, the judgment shall be communicated to the controlling Agency, which shall keep a record to such purpose.

#### SECTION 44. - Venue

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.

Provinces are hereby encouraged to adhere to those provisions of this Act as may be of an exclusively national jurisdiction.

The federal jurisdiction shall apply in respect of data registers, files, or banks interconnected via national or international inter jurisdictional networks.

SECTION 45. - 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.

SECTION 46. - Transitory provision

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.

Notify the Executive Branch of this Act.