Personal Data Protection
Law 25.326

General Provisions. General principles related to the protection of data. Rights of data owners. Users and individuals in charge of files, records, and databases. Oversight. Sanctions. Action to protect personal data.

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

Chapter I
General Provisions

Article 1 — (Purpose).

The purpose of this Act is the comprehensive protection of personal data included in files, records, databases or other data processing technical means -whether public or private- used for reporting purposes, in order to guarantee the right of individuals to their honor and privacy, as well as access to information recorded thereupon, in accordance with the third paragraph of Article 43 of the National Constitution.

The provisions of this Act shall also apply, if appropriate, to such data related to legal persons.

Under no circumstances shall databases or media information sources be affected hereby.

Article 2 — (Definitions).

The following terms shall have the following meanings to the effects of this Act:

— Personal data: Information of any kind referring to defined or definable individuals or corporations.

— Private data: Personal data revealing racial and ethnic origin, political views, religious, philosophic, or moral beliefs, union membership, and information referring to health or sexual life of individuals.

— File, record, databank or database: Indistinctly, they designate the organized group of personal data subject to processing, whether electronic or other means, whichever way they have been created, stored, organized or accessed by.

— Data processing: Systematic operations and procedures, whether electronic or otherwise, enabling collection, integrity, sorting, storage, change, relation, assessment, blocking, destruction and, in general, personal data processing, as well as sending of such data to third parties through communications, inquiries, interconnection or transfers.

— Person in charge of file, record, databank or database: Public or private individual or corporation, holder of a file, record, databank or database.

— Computer data: Personal data subject to electronic or automated processing or handling.

— Data owner: Any individual or corporation domiciled in the country, or having offices or branches in the country, whose data are subject to this Act.

— Data user: Any person --public or private-- carrying out, at its sole discretion, data processing, whether contained in files, records, or databases of its own, or through connection therewith.

— Data disaggregation: Any handling of personal data in such a way that information obtained cannot be associated to a person, determined or that may be determined.

Chapter II
General principles related to data protection

Article 3 — (Data file – Lawfulness).

Data file creation shall be lawful provided that it is duly registered in compliance with the principles set forth herein and rules and regulations passed as a consequence thereof.

Data files shall not have any purpose contrary to laws or public morals.

Article 4 — (Quality of data).

1. Personal data collected for processing thereof shall be true, appropriate, relevant, and not excessive in relation to the scope and purpose for which they have been obtained.
2. Data collection shall not be carried out by anti-trust or fraudulent means, or by means contrary to the provisions of this Act.
3. Data subject to processing shall not be used for purposes other than, or incompatible with, those purposes that led to their collection.
4. Data shall be accurate and updated if necessary.
5. If any data is known to be inaccurate or incomplete, such totally or partially inaccurate data or incomplete data shall be deleted and replaced or, if applicable, supplemented, by the person in charge of the file or database, notwithstanding holder's rights set forth in Article 16 hereof.
6. Data shall be stored in such a way that they allow the holder thereof to exercise the right of access thereto.
7. Data shall be destroyed whenever it is no longer necessary or relevant for the purposes for which it has been gathered.

Article 5 — (Consent).

1. Processing of personal data shall be unlawful if the holder has not given free, express and informed consent thereupon, in writing or evidenced by any other similar means, according to the relevant circumstances.

   The above referred consent, given with other representations, shall be expressly stated and highlighted, with the prior notice to the person from which data is required, which notice shall include information described in Article 6 hereof.

2. Consent shall not be necessary if:

   a) Data is obtained from unrestricted public-access sources;

   b) Data is gathered to comply with State powers or by virtue of a legal obligation;

   c) Data is included in reports whose data is limited to name, identity document, taxpayer or pension identification number, occupation, date of birth and domicile;

   d) Data is derived from a contractual, scientific or professional relationship of the data owner, and it is necessary for its development or compliance;

   e) Data is related to operations carried out by financial entities and information received from their customers in accordance with Article 39 of Act Number 21526.

Article 6 — (Information).

When gathering personal data, holders thereof shall be previously notified, expressly and clearly, about the following:

a) The purpose thereof and those who may be the addressees or class of addressees;

b) Existence of the relevant file, record, database --electronic or of any other kind-- and the identity and domicile of the person in charge thereof;

c) The fact that filling out the proposed questionnaire is mandatory or optional, specially regarding data referred to in the following Article;

d) The consequences to be derived from furnishing data, the reluctance to furnish data or from inaccuracy thereof;

e) The possibility for the interested party to exercise data access, change and deletion rights.

Article 7 — (Category of data).

1. No person shall be bound to provide private data.

2. Private data shall only be gathered and subject to processing provided that there are reasons of general public interest authorized by law. Private data may also be processed for statistical or scientific purposes when holders thereof cannot be identified.

3. The creation of files, databases or records storing information which directly or indirectly discloses private data is hereby forbidden. Notwithstanding, the Catholic Church, religious associations, and political organizations and unions may maintain records of their members.

4. Data related to criminal or misdemeanor records may only be subject to processing by competent public authorities, within the framework of the respective acts and rules and regulations.

Article 8 — (Health-date data). Public or private health care centers and practitioners working on health science-related fields may gather and handle personal data related to the physical or mental health of patients attending such centers, or who are or have been under treatment, respecting the professional secret principle.

Article 9 — (Safety of data).

1. The person in charge of the data file or the user thereof shall adopt all technical and organizational measures necessary to ensure the security and confidentiality of personal data, so as to prevent such data from being forged, lost, inquired, or processed without authorization, and allowing to detect any information deviation, whether intentional or not, whether risks arise from a human act or from the technical means in use.

2. It is hereby forbidden to record personal data in files, registers, or databases not compliant with technical integrity and security conditions.

Article 10. — (Confidentiality).

1. The person in charge and those involved in any phase of personal data processing shall be bound to keep the professional secret with respect thereto. Such obligation shall outlive the relationship with the data file holder.

2. The person bound to keep the professional secret may be released from such obligation by court decision, and provided that there are reasons of public security, national defense or public health.

Article 11. — (Assignment).

1. Personal data subject to processing may only be assigned to comply with purposes directly related to the lawful interest of both assignor and assignee, with prior consent of the data owner, who shall be informed about the purpose of the assignment. Identity of the assignor and elements allowing such assignor to assign such data shall be specified.

2. Assignment consent shall be revocable.

3. Consent shall not be necessary in the following cases:

   a) If provided for by law;

   b) In cases provided for in Article 5, subArticle 2;

   c) Assignment is carried out directly between governmental agencies, to the extent of compliance with their respective competencies;

   d) If personal data is related to health, and provide that assignment thereof is necessary for public health reasons, or for emergency reasons or to conduct epidemiological tests, as long as the identity of data owners is preserved by adequate disaggregation mechanisms;

   e) An information disaggregation procedure has been applied, in such a way that data owners cannot be identified.

4. The assignee shall be subject to the same legal and regulatory obligations of the assignor, and the assignor shall be jointly and severely liable for compliance thereof to the competent authority and the relevant data owner.

Article 12. — (International transfer).

1. Transfer of personal data of any kind to any country or international or supranational organization is hereby forbidden if adequate protection is not provided.

2. This shall not apply in the following events:

   a) International judicial cooperation;

   b) Exchange of medical data, if required by the patient's treatment, or by an epidemiological research, provided that it is carried out under the terms of subArticle e) of the previous Article;

   c) Bank or stock exchange transfers, relating to the respective transactions and in accordance with applicable laws;

   d) Whenever transfer has been agreed upon within the framework of international treaties signed by Argentina;

   e) Whenever the purpose of the transfer is international cooperation among intelligence organizations to fight against organized crime, terrorism and drug-trafficking.

Chapter III
Rights of Data Owners

Article 13. — (Information right).

Any person may request information from the appropriate authority in relation to personal data files, records, or databases, the purposes thereof and the identity of the persons in charge. The record maintained to such effect shall be available to public inquiry free of charge.

Article 14. — (Right of access).

1. The data owner, with the prior identity proof, shall be entitled to request and obtain information about his/her personal data included in public or private databases intended for reporting purposes.

2. The person in charge or the user of such databases shall provide the requested information within ten calendar days as of notice thereupon. If such ten-day period has elapsed and the request has not been met, or if the report furnished is insufficient, an action for protection of personal data or *habeas data* action may be commenced as provided for in this Act.

3. The right of access referred to in this Article may only be exercised free of charge once every six months, save a lawful interest is evidenced to such effect.

4. Exercise of the right referred to in this Article in the case of personal data or deceased individuals shall correspond to general heirs.

Article 15. — (Information contents).

1. Information shall be provided in a clear way, free from any coding and, if applicable, accompanied by an explanation of terms used, in a language understood by the general public.

2. Information shall be comprehensive and related to the entire holder's record, even when the requirement is only related to one aspect of personal data. In no event shall the report disclose any third-party data, even though they may be related to the interested party.

3. Information, at the holder's option, may be furnished in writing, by electronic means, telephone, images, or by any other means competent to such end.

Article 16. — (Right for data editing, updating, or deletion).

1. Any person shall be entitled to have his/her personal data, included in a database, edited, updated and, if applicable, deleted or subjected to confidentiality rules,.

2. The person in charge or the user of such database shall proceed to edit, delete or update personal data of the party involved, carrying out the necessary actions to such end within a maximum of five business days following receipt of the data owner's claim, or information on the error or untruthfulness.

3. Non-compliance with this obligation within the term agreed upon in the above subArticle, shall authorize the party involved to file an action for protection of personal data or habeas data action provided for herein.

4. In the case of assignment or transfer of data, the person in charge or the user of the database shall serve notice of the change or deletion upon the assignee within five business days following the data editing or deletion.
5.
6. Deletion shall not proceed in the event that it may damage third party lawful rights or interests, of if there is a legal obligation to preserve the integrity of such data.
7. During the relevant process of data verification and rectifying of the error or untruthfulness, the person in charge or the user of the database shall block the file, or state --at the time of providing information related thereto-- the fact that that such information is subject to revision.

8. Personal data shall be kept intact during the terms provided for in the applicable provisions or, if applicable, in contractual provisions agreed upon between the person in charge or the user of the database and the data owner.

Article 17. — (Defenses).

1. Persons in charge or users of public databases may, for reason, deny access, editing or deletion of data to protect the Nation's defense, public order and security, or to protect third party rights or interests.

2. Information about personal data may also be denied by persons in charge, or users, of public databases if it hinders pending judicial or administrative actions related to the investigation of compliance with tax or pension duties, the discharge of health and environmental oversight functions, investigation of crimes and identification of administrative violations. The resolution in force to establish such denial must state the reasons thereof, and notice thereupon shall be served on the party involved.

3. Notwithstanding the provisions of the above subArticles, if the party involved has to exercise the right of defense in a legal proceeding, access to records shall not be forbidden.

Article 18. — (Parliamentary Committees).

The National Defense Committee and the National Congress Bicameral Committee on Oversight of Domestic Security and Intelligence Agencies and Activities, and the House Domestic Security Committee, or any committees that may replace them, shall have access to files or databases referred to in Article 23, subArticle 2, for reason, and with regard to those aspects constituting the subject matter of such Committees competence.

Article 19. — (Gratuitousness).

Editing, updating or deletion of inaccurate or incomplete personal data included in public or private records shall be carried out free of charge.

Article 20. — (Challenge of personal assessments).

1. Court decisions or administrative acts implying an assessment of human conduct shall not be based solely on the results of computer processed personal data that may give a definition of the involved party profile or personality.

2. Any acts contrary to the precedent provision shall be null and void.

Chapter IV
Persons in charge of files, records, and databases and users thereof

Article 21. — (Data file record. Registration).

1. Any public or private file, record, or database intended for reporting purposes shall be recorded with the Registry authorized by the competent authority to such effect.

2. Registration of databases shall comprise, at least, the following information:

a) Name and domicile of the person in charge;
b) File characteristics and purpose;
c) Nature of personal data contained in each file;
d) Data gathering and updating modalities;

e) Purpose of data and individuals or corporations to which such data may be transferred;
f) Way of interrelating recorded information;
g) Means used to guarantee data security, detailing the category of people having access to information processing;
h) Data useful life;
i) Manner and conditions in which persons may access data referring thereto and proceedings to be carried out for data edit or update.

3. No data user may have personal data of any nature different from the nature of data stated in the record.

Non-compliance with these requirements shall imply administrative sanctions provided for in chapter VI hereof.

Article 22. — (Public files, records, or databases).

1. Rules governing the creation, editing or deletion of files, records or databases belonging to public agencies shall be passed by general provisions published in the National Official Gazette or in an authorized newspaper.

2. The respective provisions shall state the following:

1. Characteristics and purpose of the file;
2. Persons with respect to whom data is to be obtained and the mandatory or optional nature of data to be provided by such persons;
3. Procedure for data collection and updating;
4. Basic file structure, whether it be a computer file or not, and description of the nature of personal data contained therein;
5. Planned assignments, transfers or interconnections;
6. Agencies in charge of the file, stating their reporting line of command, if applicable;
7. Agencies where claims may be filed in order to exercise rights of access, editing or deletion of information.

3. The provisions passed for deletion of computer records, the destination thereof or such measures taken to destroy them shall be expressly stated.

Article 23. — (Special Events).

1. Personal data that, having been stored for administrative purposes, must be included as permanent record in databases belonging to the armed forces, security forces, police departments or intelligence agencies shall be subject to the provisions hereof; as well as data relating to personal records furnished by such databases to administrative or court authorities that may require them by virtue of standing legal provisions.

2. Processing of personal data for the purposes of national defense or public security by the armed forces, security forces, police departments or intelligence agencies, without the consent of the parties involved, shall be limited to those events and data categories necessary for strict compliance with the missions legally assigned to them for national defense or public security purposes, or to fight against crime. In such cases, files shall be specified and identified to such effect, and they shall be classified in categories, according to their degree of reliability.

3. Personal data registered for police purposes shall be deleted whenever they become no longer necessary for the investigation that gave rise to their storage.

Article 24. — (Private files, records, or databases).

Private persons creating files, records, or databases not intended exclusively for personal use shall register as provided for in Article 21.

Article 25. — (Delivery of personal data computer services).

1. Whenever personal data processing services are delivered on behalf of third parties, such data shall not be applied or used for a purpose other than that stated in the service provision agreement, and they shall not be assigned to third parties, not even for maintenance thereof.

2. Upon compliance with the contractual covenant, processed personal data shall be destroyed, except when there is express authorization thereupon on behalf of the person to whom such services are delivered, if the possibility of future service requests is reasonably presumed, in which case they may be stored under proper safety conditions for a maximum two-year period.

Article 26. — (Delivery of credit information services).

1. When delivering credit information service, only property-related personal data relevant to the individual's financial economic solvency and to the credit may be handled, provided that they have been obtained from sources available to the public, or from information furnished by the party involved or with the consent thereof.

2. Also personal data related to compliance or non-compliance with property obligations may be handled, if they have been furnished by the creditor or a person acting on his/her behalf.

3. At the request of the data owner, the person in charge, or the user, of the database shall communicate to such holder any information, assessment and opinions thereupon furnished during the last six month-period, and the name and domicile of the relevant assignee in the event that data was obtained by way of assignment.

4. Only personal data relevant to assess the economic and financial solvency of the parties involved during the last five years may be kept on file, recorded or assigned. Such term shall be reduced to two years if the debtor pays the debt or complies with the obligation, furnishing evidence of such payment or compliance.

5. Delivery of credit information services shall not require the prior consent of, or notice upon, the data owner for assignment thereof, if such services are related to the assignees´ business or credit activities.

Article 27. — (Files, records, or databases for advertising purposes).

1. In cases of domicile data gathering, documents distribution, advertising or direct selling and other similar business activities, data required to establish certain profiles for promotion, business or advertising purposes, or that may allow to establish consumer habits may be gathered; provided that such data be included in documents available to the public or be made available by data owners or obtained with their consent.

2. In the events provided for in this Article, the data owner may exercise the right of access free of charge.

3. At any time, the data owner may request deletion or blocking of its name from databases to which this Article refers.

Article 28. — (Files, records, or databases related to Surveys).

1. Provisions hereof shall not apply to opinion polls, measurements and statistics made in accordance with Act Number 17622, market prospecting, scientific or medical research and similar activities, if data gathered can not be attributed to a specified person or to a person whose identity may be determined.

2. If, during the data gathering process, it is not possible to maintain anonymity, the disaggregation technique shall be implemented, so that no person may be identified.

Chapter V
Oversight

Article 29. — (Oversight Authority).

1. The oversight authority shall take any steps necessary for compliance with purposes and other provisions hereof. To such effects, the oversight authority shall have the following duties and powers:

a) Assist and advise people, upon request, on the scope hereof and the legal means available for protection of rights guaranteed hereby;

b) Approve rules and regulations to be complied with in the performance of activities regulated by this Act;

c) Conduct a survey on files, records or databases comprised herein and keep a permanent record thereof;

d) Oversee the compliance by files, records or databases with data integrity and security rules. To such effect, the oversight authority may request judicial authorization to have access to data processing sites, equipment or programs in order to identify violations to this Act;

e) Request information from public and private entities, which shall furnish background information, documents, programs or other elements related to personal data processing as required. In such events, the oversight authority shall guarantee safety and confidentiality of furnished information and elements;

f) Impose administrative sanctions applicable, in each case, for violation against rules hereof and of rules and regulations passed hereunder;

g) Act as the accuser in criminal proceedings filed by reason of violations to this Act;

h) Oversee compliance with requirements and guaranties applicable to private files or databases intended to provide reports, in order to be registered in the appropriate Registry created by this Act.

2. (vetoed)

3. (vetoed)

The Director shall be a full-time official, and job incompatibilities set forth herein for public officers shall apply thereto, and the Executive may remove him/her from office on the grounds of bad performance.

Article 30. — (Codes of professional conduct).

1. Associations or entities representing those in charge, or users, of privately-held databases may enact codes of professional conduct, which shall set forth rules for processing of personal data, tending to secure and improve information systems´ operating conditions in accordance with the principles set forth herein.

2. Such codes shall be registered in the appropriate registry under the responsibility of the oversight authority to such effect, and such competent authority may deny registry whenever it may consider that they do not comply with standing legal and regulatory provisions.

Chapter VI
Sanctions

Article 31. — (Administrative sanctions).

1. Without prejudice to administrative liabilities applicable in the case of people in charge, or users, of public databases, the liability for damages derived from non-compliance with this Act, and applicable criminal sanctions, the competent authority may apply warning sanctions, suspension, and a one thousand pesos ($1,000) to one hundred thousand pesos ($100,000.) penalty, or instruct the closure or elimination of the file, record or database.

2. Rules and regulations shall determine the conditions and proceedings for enforcement of the applicable sanctions, which shall be determined in relation to the seriousness and time of the violation involved, and of the damages derived from such violation, by ensuring the due process of law.

Article 32. — (Criminal sanctions).

1. The following Article shall be included as Article 117 bis of the Criminal Code:

1st. Any person knowingly introducing or having introduced any false data in a personal data record shall be liable to a one-month to two-year imprisonment.

2nd. The sentence shall be a six-month to three-year imprisonment in the case of any person knowingly furnishing to a third party false information contained in a given personal data record.

3rd. The criminal scale shall be increased to half the minimum sentence and half the maximum sentence if any person sustains any damage by reason of such event.

4th. When the author or person in charge of the crime is an incumbent public officer, the following accessory sentence shall apply: disqualification to serve as public officer for twice the time of the sentence."

2. The following Article shall be included as Article 157 bis of the Criminal Code:

"One-month to two-year imprisonment shall apply to any person who:

1st. Knowingly or unlawfully, or in violation of confidentiality and data security systems, has access, in any way, to a personal database;

2nd. Reveals to a third party information recorded in a personal database whose secrecy should be preserved as provided by law. In the event that the author is a public officer, an additional sentence of one to four years special disqualification shall apply."

Chapter VII
Action for personal data protection

Article 33. — (Applicability).

1. The action for personal data protection or *hábeas data* shall apply:

a) to learn about personal data stored in public or private files, records or databases intended to provide reports, and learn about the purpose thereof;

b) whenever it is presumed that relevant information is false, inaccurate or outdated, or in case of processing of data whose registration is forbidden in this Act, to demand the change, deletion, confidentiality processing or updating thereof.

Article 34. — (Active entitlement)

The action for personal data protection or *habeas data* may be exercised by the party involved, his/her guardians and successors or assigns of individuals, whether direct or indirect heirs up to the second degree of congeniality, per se or by an attorney.

When the action is exercised by corporations, such action shall be inchoated by their legal representatives or attorneys appointed to such effect.

The Ombudsman may intervene in the proceedings for legal assistance purposes.

Article 35. — (Passive entitlement).

The action shall proceed against people in charge, and users, of public databases, and of private databases intended for reporting.

Article 36. — (Venue).

The judge with jurisdiction in the domicile of the author, or the domicile of the defendant, or the place where the event or act took place or where the event or act could have effects, at the author's election, shall have venue over these matters.

Federal courts shall have venue over these matters:

a) whenever the action is brought against public data files of national entities, and

b) whenever data files are interconnected through interjurisdictional, national or international, networks.

Article 37. — (Applicable proceedings).

The *habeas data* action shall be conducted in accordance with the provisions hereof and under the proceedings corresponding to the common summary proceeding to guarantee constitutional rights (*acción de amparo*) and, as a supplement, under the rules set forth in the Code of Civil and Commercial Proceedings, governing extraordinary summary proceeding (*juicio sumarísimo*).

Article 38. — (Complaint requirements).

1. The complaint shall be filed in writing, detailing as precisely as possible the file, record or database name and domicile and, if applicable, the name of the person in charge or user thereof.

In the case of public files, records or databases, the federal agency responsible for them shall be determined.

2. The complainant may allege reasons for which he/she understands that the identified file, record or database includes information related to him/herself, the reasons why he/she considers that the information related to him/herself is discriminatory, false or inaccurate, and he/she may also furnish evidence of compliance with requirements applicable to exercise of rights granted thereto by this Act.

3. The party involved may request that, while proceedings are pending, a notice be included in the record or database to the effects that the challenged information is subject to judicial proceedings.

4. The Court may instruct the provisional file blocking as it refers to the personal datum from which the trial arose, provided that the discriminatory, false or inaccurate nature of the relevant information is patent.

5. In order to require information from the file, record or database involved, the Court shall apply a broad criterion to the relevant circumstances of subArticles 1 and 2.

Article 39. — (Proceedings).

i. Upon admission of the action, the Court shall require from the file, record or database to send information related to the complainant. Likewise, the Court may request reports about data technical support, basic documents relating to data collection and any other aspect conducive to a case solution, as it may deem convenient.

ii. There shall be a maximum of five business days available to answer the report, which term may be prudently extended by the Court.

Article 40. — (Confidentiality of information).

i. Private records, files or databases shall not allege confidentiality of information required therefrom, save where journalistic information sources are affected.

ii. When a public file, record or database denies to send the requested report raising defenses of right of access, editing or deletion authorized by this Act or by a specific Act, such file, record or database shall furnish evidence of the facts that make such defense applicable. In such events, the Court may personally and directly get in contact with the requested data, thus assuring confidentiality thereupon.

Article 41. — (Answer to the report).

When answering the report, the file, record or database shall state the reasons why it included such challenged information and why it did not meet the request made by the interested party, in accordance with Articles 13 to 15 hereof.

Article 42. — (Amended complaint).

Upon answer to the report, the complainant may, within a three-day period amend the complaint requesting deletion, editing, confidentiality or updating of his/her personal data, if applicable hereunder, furnishing evidence thereof in the same act. Notice of this amended complaint shall be served upon the defendant within a three-day term.

Article 43. — (Judgement).

a) Upon maturity of the term to answer the report or upon filing of an answer thereto, and in the event provided for in Article 42, after answer to the amended complaint has been filed, and after the evidence been furnished thereon, the Court shall render judgment.

b) In case the action is deemed to proceed, the Court shall specify whether the information shall be deleted, edited, updated or declared confidential, establishing a term for compliance thereof.

c) If the action is rejected, the defendant shall not be presumed liable.

d) In any event, judgment shall be notified to the oversight authority, which shall keep a record to such effect.

Article 44. — (Scope of application).

The rules hereof contained in Chapters I, II, III, and IV, and in Article 32 are public and apply in the entire national territory.

Provinces are invited to endorse to regulations of this Act that may exclusively apply to the federal jurisdiction.

The federal jurisdiction shall govern with regard to records, files, or databases interconnected by interjurisdictional, national or international, networks.

Article 45. — The Executive shall pass the regulations governing this Act and shall create a competent authority within a one hundred and eighty day term following enactment hereof.

Article 46. — (Temporary provisions).

Files, records or databases intended to furnish information, existing at the time of the enactment of this Act, shall be registered in the registry created in accordance with Article 21, and shall be adapted to the provisions hereof within the term set forth by pertinent regulations.

Article 47. — (vetoed)

Article 48. — Be notified to the Executive.

Decree 995/2000

CONSIDERING file Number 020-003060/2000 of the Registry of the MINISTRY OF ECONOMY and the Bill registered under number 25326, enacted by the NATIONAL CONGRESS on October 4, 2000, and

WHEREAS:

The above mentioned Bill provides for integral protection of personal data, in accordance with the provisions of Article 43, third paragraph of the NATIONAL CONSTITUTION.

Article 29 of the Bill sets forth the creation of an Oversight Authority to take any and all necessary steps for compliance with purposes and provisions included in such Bill.

SubArticle 2 of such Article sets forth that the Oversight Authority shall serve independently and shall act as decentralized agency within the scope of the MINISTRY OF JUSTICE AND HUMAN RIGHTS.

SubArticle 3 of Article 29 of the Bill governs the conduct and management of such Oversight Authority.

The creation of the Oversight Authority as a decentralized agency shall imply, as any creation of a organization structure of its kind, an increase of expenditure for the NATIONAL STATE.

That this Act does not provide for financing of the Oversight Authority and Act Number 25237: National Government Budget for fiscal year 2000 and National Budget Act for fiscal year 2001 do not contain any credit allocations therefor.

That laws in force regulating Public Financial Management provide that any spending increase shall provide for its respective financing.

That, notwithstanding the above, the creation of an oversight authority is deemed relevant, but such competent authority shall comply with organizational characteristics set forth by the EXECUTIVE BRANCH as authorized by Article 45 of this Bill.

That Article 47 of the Bill sets forth that databases delivering credit information services shall delete or, if applicable, not include, any data referring to non-compliance or default in payment of an obligation, if such obligation has been settled on the effective date of this Act.

That this decision would imply the loss of historical information related to credit compliance of many system debtors, which could produce a cost increase in bank credit operations originated in the higher risk caused by uncertainty.

That, according to the reasons above, we must observe Article 29, subArticles 2 and 3 and Article 47 of the Bill registered under the Number 25,326.

That the proposed measure does not alter the spirit or consistency of the Bill enacted by the NATIONAL CONGRESS.

That the GENERAL OFFICE OF LEGAL AFFAIRS of the MINISTRY OF ECONOMY has been involved as applicable.

That the EXECUTIVE BRANCH is empowered to enact this Bill by virtue of the provisions of Article 80 of the NATIONAL CONSTITUTION.

Therefore,

THE PRESIDENT OF THE ARGENTINE REPUBLIC
IN AGREEMENT WITH HIS CABINET OF MINISTERS

DOES HEREBY DECREE AS FOLLOWS:

Article 1: Article 29, subArticles 2 and 3 of the Bill registered under the Number 25326 be observed

Article 2: Article 47 of Bill registered under the Number 25326 be observed.

Article 3: With the exceptions set forth in the precedent Articles, Bill registered under the Number 25326 be complied with and enacted as National Act.

Article 4: The NATIONAL CONGRESS be notified.

Article 5: The National Official of Official Registry be notified. This Bill be published and filed.