PERSONAL DATA PROTECTION LAW DRAFT BILL

Provides for the processing of personal data¹ aiming at protecting the personality and dignity of the natural person.

The PRESIDENT OF THE REPUBLIC. To be known that the National Congress decrees and I sanction the following Law.

CHAPTER I – PRELIMINARY PROVISIONS

Art. 1 – The present law provides for the processing of personal data, aiming at protecting the fundamental rights of freedom, intimacy and privacy of the natural person.

Art. 2 – The present law applies to any operation of processing undertaken totally or partially through automated means, by a natural person or a private or public legal person, regardless of the country where its headquarters are located and of the country where the database is located, as long as:

I – the processing operation² occurs in national territory; or

II – the personal data relating to the processing operation have been collected in national territory.

§ 1st – personal data will be deemed to have been collected in national territory if the data subject located therein at the moment of the collection.

§ 2nd – The present law does not apply to data processing:

I – undertaken by a natural person strictly for personal purposes; or

II – undertaken strictly for news reporting purposes.

1 TN.: “Personally Identifiable Information” in the US. The draft bill is inspired in and employs concepts of European Data Protection Law. We have chosen to use terms associated to data protection as they have been coined in English in the European context.

2 TN.: The original version employs the expression “operação de tratamento” (which could be literally translated as “treatment operation”). We have preferred to refer to the act of “processing” or the “processing operation” following the European Directive.
§ 3rd – Public bodies or entities are prohibited from transferring personal data stored in databases under their management, or to which such entities may have access by reason of their jurisdiction, to private entities, except in those cases in which processing is outsourced to private entities or else, and solely for a defined and specific purpose, by reason of concession or authorization for the provision of public services which demand such a transfer.

Art. 3 – State-owned companies and quasi-public corporations which operate in a free competition environment, subject to the provisions of art. 173 of the Federal Constitution, will be bound by the same rules as those enjoyed by private entities, pursuant to the present Law.

Sole Paragraph – State-owned companies and quasi-public corporations, when implementing public policies and, thus, not operating in a free competition environment, will be bound by the same rules as those enjoyed by public bodies or entities, pursuant to the present Law.

Art. 4 – Processing of personal data for the exclusive purposes of public security, defense, State security, investigation and law enforcement activities, will be regulated by a specific law, pursuant to general principles of protection and the data subjects rights provided by the present Law.

Sole Paragraph – The processing by private entities of data mentioned in the head of this article is prohibited, except in procedures conducted by a public legal person which must be specifically notified to the competent public body.

Art. 5 – For the purposes of the present Law:

I – personal data: shall mean the data pertaining to an identified or identifiable natural person, including by reference to an identification number, location data or online identifiers;

II – processing: shall mean the set of operations relating to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, transport, processing, filing, storage, discarding, evaluation or control of the information, modification, blockage or provision to third parties of personal data, by means of data disclosure interconnection, conveyance, diffusion or extraction;

III – sensitive data: shall mean personal data which reveal ethnic or racial origins, religious, philosophical or moral convictions, political opinions, membership in unions or organizations of religious, philosophical or political nature, data relating to one’s health or sexual life, as well as genetic data;

3 TN.: The original version refers to a “órgão competente”. The creation of a supervisory authority was not expressly contemplated by the draft bill. A generic reference to a competent (one can only assume, on data protection) public body (not defined or described in the wording of the draft) seems to have been directed at giving leeway for the administration decide on the matter further on in the legislative process.
IV – anonymous data: shall mean data pertaining to a data subject which cannot be identified, neither by data controller, nor by anyone else, taking into consideration those means reasonable prone to be used in identifying said data subject;

V – database: shall mean a structured set of personal data, located in one or many sites and stored in physical or electronic format;

VI – data subject: shall mean the natural person to whom pertains de personal data subject to processing;

VII – consent: shall mean the free, express, specific and informed statement through which the data subject agrees with the processing of his personal data for a defined purpose;

VIII – data controller: shall mean a natural or legal person, in private or public law, with whom lies the decisions relating to the processing of personal data;

IX – data processor: shall mean a natural or legal person, in private or public law, who processes personal data on behalf of the data controller;

X – data disclosure: shall mean the communication of personal data to one or more identified persons which not the data subject, regardless of the means of communication;

XI – interconnection: shall mean the transfer of personal data from one database to another, owned or not by the same person, for similar or different purposes;

XII – dissemination: shall mean the communication of personal data to one or more unidentified persons which not the data subject, regardless of the means of communication;

XIII – international data transfer: shall mean the transfer of personal data to a foreign country;

XIV – de-identification: shall mean the act of modifying personal data in such a manner that it cannot be linked, directly or indirectly, to an identified or identifiable individual;

XV – blockage: shall mean the storage of personal data or of a database with a temporary suspension of any processing operation;

XVI – erasure: shall mean the erasure of data or of a set of data stored in a database, regardless of the method employed;

4 TN.: In the original version the term employed in Portuguese is “responsável”. It is used in the sense of accountability.

5 TN.: In the original version the term employed in Portuguese is “operador”. It is used in the sense of that who executes an operation or task.
XVII – shared use of data: shall mean the disclosure, dissemination, international transfer, interconnection or shared processing of a database by public bodies or entities, when in fulfillment of their obligations, or among public bodies or entities and private entities, with specific authorization, for one or more classes of processing assigned by such public entities; and

XVIII – officer: a natural person, appointed by the data controller, to act as a communication channel before the data subjects and the competent public body.

Art. 6 – The processing of personal data must comply with the following general principles:

I – purpose principle, under which processing must be carried out for legitimate, specified, explicit purposes, which must also be known by the data subject;

II – adequacy principle, under which processing must be compatible with the purposes aimed by such processing and with the legitimate expectations of the data subject, taken into account the context of the processing;

III – necessity principle, under which processing must be limited to a minimum necessary to accomplish the aimed purposes, contemplating pertinent, proportional and not excessive data;

IV – free access principle, under which data subject must be granted eased and gratuitous access to information as to the classes of processing and on the whole of his personal data;

V – data quality principle, under which the data must accurate, clear and up-to-dated, the frequency required to accomplish the purpose of the processing taken into account;

VI – transparency principle, under which clear and adequate information relating to the processing operation must guaranteed to the data subject;

VII – prevention principle, under which constantly updated technical and administrative measures, which must also be proportional to the nature of the processed information and adequate to protect personal data from unauthorized access and from accidental and unlawful situations of destruction, loss, modification, disclosure or dissemination, must be employed.

VIII – prevention principle, under which measures capable of preventing the occurrence of damages as a consequence of the processing of personal data, must be adopted; and

IX – non-discrimination principle, under which processing must not be used for discriminatory purposes.

6 TN.: In the original version the term employed in Portuguese is “cancelamento” (which may be literally translated as “cancellation”). “Erasure” provides a clearer sense of the procedure.
§ 1st – Public bodies will make their processing of data operations public, by means of clear, precise and updated information provided through easy to access channels, preferably their websites, pursuant to the transparency principles established in item VI.

§ 2nd – The shared use of personal data must be consistent with specific ends associated to the execution of public policies and duties by public bodies and entities, pursuant to the purpose, adequacy and necessity principles, established by items I, II and III.

CHAPTER II – CONDITIONS FOR THE PROCESSING OF PERSONAL DATA

Section I – Consent

Art. 7 – Exception made to the provision of art. 11, processing of personal data will be lawful only upon free, express, specific and informed consent by the data subject.

§ 1st – Consent to the processing of personal data shall not constitute a condition for the provision of products or services or for the exercise of rights, except in those instances where data is essential for the completion of a transaction or exercise of a right.

§ 2nd – It is prohibited to process of personal data in those instances where consent has been obtained, in error, by cause of willful misconduct, flagrant necessity or coercion.

§ 3rd – Consent must be given in writing or by other means capable of certifying it.

§ 4th – Consent must be given separately from other contractual provisions.

§ 5th – Consent must relate to defined purposes, being reputed as void generic authorizations for the processing of personal data.

§ 6th – Consent can be revoked at any given time with no consequence to data subject.

§ 7th – Provisions that impose inequitable or abusive obligations to data subject, that put him in a situation of substantial handicap, or that are incompatible with good-faith or equity are void.

§ 8th – The burden of proof that consent has been obtained in compliance with the provisions of this Law, lies upon the data controller.

Art. 8 – A data subject ranging between 12 (twelve) and 18 (eighteen) years of age can give consent for the processing of data, such processing taking into account his peculiar state of person under development, granted the possibility of revocation of such consent, in his best interest, by his parents, guardians or tutors.
Art. 9 – In the case of a data subject below 12 (twelve) years of age, consent will be given by his parents, guardians or tutors and processing must take into account his peculiar state of person under development.

Art. 10 – At the moment in which consent is given, the data subject will be informed in a clear, adequate and prominent fashion about the following elements:

I – specific purpose for the processing;

II – manner and duration of the processing;

III – identification of the data controller;

IV – contact information of the data controller;

V – persons or category of persons to which data may be disclosed, as well as the scope of dissemination;

VI – obligations of the agents that will process data; and

VII – rights of the data subject, with specific mention to:

a) – the choice of not giving consent, with an explanation of the consequences of refusal, pursuant to § 1st of art. 6th;

b) – the possibility of accessing or rectifying data and to revoke consent, by means of a gratuitous and eased procedure; and

c) – the possibility of denouncing to the competent public body any non-compliance to the provisions of this Law.

§ 1st – Consent will be deemed void if the information provided to data subject is misleading or is not presented, clearly, adequately or prominently.

§ 2nd – In the event of modification of the information mentioned in items I, II, III or V to the head of this article, the data controller shall obtain a new consent from the data subject, after specifically highlighting the content of the modifications.

§ 3rd – In the event of modification of the information mentioned in item IV to the head of this article, the data controller must communicate to data subject the updated contact information.

§ 4th – For those activities involving a continued collection of personal data, the data subject must be informed in a regular basis of such a continued collection, in those terms defined by the competent public body.
Art. 11 – Consent will not be necessary when the data is of unrestricted public access or when processing is essential for:

I – fulfillment of a legal obligation by the data controller;

II – processing and shared use of data relating to the exercise of rights or fulfillment of duties defined by law or regulated by the public administration;

III – execution of pre-contractual procedures or obligations relating to an agreement in which the data subject is a party, pursuant to § 1st of art. 6th;

IV – performance of historical, scientific and statistical research, guaranteed, whenever possible, the de-identification of personal data;

V – regular exercise of rights in judicial and administrative procedures;

VI – protection of life or physical safety of the data subject or a third party;

VII – protection of health, with procedure performed by health care professional or public health authorities.

§ 1st – In those instances where consent is not necessary, data must be processed solely for the established purposes and for the least time possible, pursuant to the general principles established in this Law and guaranteed the rights of the data subject.

§ 2nd – Whenever items I and II are applicable, publicity shall be given to such cases pursuant to § 1st of art. 6th.

§ 3rd – In case of breach of the provisions of § 2nd, the data processor or the data controller responsible for processing the data may be held liable.

Section II – Sensitive Personal Data

Art. 12 – The processing of sensitive personal data is prohibited, except:

I – if data subject gives especial consent;

a) by means of specific statement, distinct from his statement of consent relating to other personal data; and

b) with prior and specific information regarding the sensitive nature of the data to be processed, with a warning regarding the risks involved in the processing of data of such nature; or
II – without the data subject giving consent, when the data is of unrestricted public access or in those cases in which it is essential for:

a) fulfillment of a legal obligation by the data controller;

b) processing and shared use of data relating to the exercise of rights or fulfillment of duties defined by law or regulated by the public administration;

c) performance of historical, scientific and statistical research, guaranteed, whenever possible, the de-identification of personal data;

d) regular exercise of rights in judicial and administrative procedures;

e) protection of life or physical safety of the data subject or a third party;

f) protection of health, with procedure performed by health care professional or public health authorities.

§ 1st – The provisions herein apply to any processing capable of revealing sensitive personal data.

§ 2nd – The processing of sensitive personal data shall not be performed in detriment of the data subject, except as provided in the specific legislation.

§ 3rd – In cases where items ‘a’ and ‘b’ are invoked by public bodies and entities, publicity shall be given to the waiver of consent pursuant to §1st of art. 6th.

Art. 13 – Competent public body may define additional safety and protective measures in regard to sensitive personal data, which shall be adopted by the data controller or other processing agents.

§ 1st – The performance of certain classes of sensitive personal data processing may be subject to prior authorization of competent public body, pursuant to regulation.

§ 2nd – The processing of personal biometric data shall be disciplined by a competent public body, which shall provide for the cases in which biometric data shall be deemed sensitive personal data.

**Section III – Termination of Processing**

Art. 14 – The termination of the processing of personal data shall occur in the following cases:

I – verification that the purpose has been achieved or that the data is no longer necessary or relevant for achieving the specific desired purpose;

II – end of the processing period;
III – communication by the data subject; or

IV – order by competent public body in the event of breach of a legal provision or regulation.

**Sole Paragraph** – The competent public body will establish maximum periods for the processing of personal data, except as provided in specific law.

**Art. 15** – Personal data shall be erased after the termination of processing, preservation being authorized for the following purposes:

I – fulfillment of a legal obligation by the data controller;

II – performance of historical, scientific and statistical research, guaranteed, whenever possible, the de-identification of personal data; or

III – assignment to third parties, pursuant to this Law.

**Sole Paragraph** – Except as provided in specific legislation and guaranteed the rights of the data subject, the competent public body may establish specific cases in which personal data may be preserved.

**CHAPTER III – DATA SUBJECT RIGHTS**

**Art. 16** – The ownership of one’s personal data is ensured to every natural person, guaranteed their fundamental rights of freedom, intimacy and privacy, pursuant to this Law.

**Art. 17** – The data subject has the right to obtain:

I – confirmation of the existence of the processing of his data;

II – access to his data;

III – correction of incomplete, inaccurate and outdated data; and

IV – de-identification, blockage or erasure of unnecessary or excessive data, or of data processed in breach of the provisions of this Law.

§ 1st – The data subject may oppose to processing based on a waiver of consent by arguing a breach of the provisions of this Law.
§ 2nd – The rights provided herein will be exercised upon request from the data subject directed to one of the processing agents, who shall give prompt attention to such request.

§ 3rd – If it is not possible to promptly respond to the data subject’s request, pursuant to § 2nd, the data controller shall send the data subject, within seven days of the receipt of the request, a response in which it may:

I – inform that it is not a data processing agent; or

II – indicate the factual and legal reasons that prevent the prompt resolution of data subject’s request.

§ 4th – Response to the request made pursuant § 2nd shall be performed without any charge to the data subject.

§ 5th – In the event of correction, erasure, de-identification or blockage of any previously disclosed data, the data controller shall notify those third parties to whom data has been disclosed, in order to them replicate such operations.

Art. 18 – Confirmation of the existence or access to personal data will be provided at data subject’s discretion:

I – immediately, in a simplified format; or

II – through a clear and complete statement indicating the data’s origin and registration date, the criteria used and the purpose of the processing, to be provided within seven days from the data subject’s request.

§ 1st - Personal data will be stored in a format that allows the exercise of the right to access.

§ 2nd - The information and data may be provided at data subject’s discretion:

I – in electronic format, which is safe and suitable for such purpose; or

II – in physical format, in which case the amount necessary exclusively for the reimbursement of costs associated to the provision of services and materials used may be charged.

§ 3rd - Whenever the database is in electronic format, data subject may request a complete electronic copy of his personal data in a format that allows its subsequent use, including in other data processing operations.
§ 4\textsuperscript{th} - The competent public body may define the formats in which the information and data will be provided to the data subject.

**Art. 19** - The data subject has the right to seek a review of decisions that affect his interests and which have been taken solely on the basis of automated personal data processing, including decisions with the purpose of setting data subject’s profile or assessing aspects of data subject’s personality.

§ 1\textsuperscript{st} - The data controller shall provide, whenever requested, adequate information regarding the criteria and procedures used to take the automated decision.

§ 2\textsuperscript{nd} - Exception is made for the processing of personal data necessary to fulfill a legal obligation.

**Art. 20** - Personal data relating to the regular exercise of rights by the data subject cannot be used to his detriment.

**Art. 21** - The defense of data subject’s interests and rights may be exercised individually or collectively in court, as provided by Law No 9507 of November 12, 1997, by articles 81 and 82 of Law No 8078 of September 11, 1990, by Law No 7347 of July 24, 1985, and in other methods of individual and collective legal protection.

**CHAPTER IV – DATA DISCLOSURE AND INTERCONNECTION**

**Art. 22** - In the event of disclosure or interconnection of personal data, the assignee shall be subject to the same legal and regulatory obligations of the assignor, with whom he will be jointly and severally liable for any damage caused.

**Sole Paragraph** - Joint and several liability will not apply to those cases of data disclosure or interconnection performed in the exercise of the duties established by Law No 12527 of November 18, 2011, regarding the guarantee of access to public information.

**Art. 23** - Data disclosure or interconnection of personal data between private legal persons, will depend on data subject’s free, express, specific and informed consent, except for those cases of waiver of consent provided by the present Law.

**Art. 24** - Data disclosure or interconnection of personal data between public legal persons and private legal persons will depend on data subject’s free, express, specific and informed consent, except:

I – in those cases of waiver of consent as provided by the present Law;
II – in the case of shared use data provided by item XVII of art. 5th, which must be made public in accordance to § 1st of art. 6th; or

III – in the event of prior authorization by the competent public body, which will assess if the waiver of consent is in the public interest, adequate and necessary.

**Sole Paragraph** - The authorization provided on item III of the head of this article may be conditioned:

I – to the communication, to the data subject, of the interconnection, pursuant to §1st of art. 6th;

II – to the offering, to data subjects, of the option to have their data erased; or

III – to the fulfillment of additional obligations, as defined by the competent public body.

**Art. 25** - Data disclosures or interconnection between public bodies and entities will be made public, pursuant to §1st of art. 6th, and will follow the general rules defined in this Chapter.

**Art. 26** - The competent public body may request, at any given time, to public bodies and entities that perform data interconnection and shared use of personal data, to provide a specific report about the scope and nature of processed data, as well as further details of the data processing operation, and may issue additional recommendations to ensure compliance with the present Law.

**Art. 27** - The competent public body may establish additional rules concerning the activities of data disclosure and interconnection of personal data.

**CHAPTER V – INTERNATIONAL TRANSFER OF DATA**

**Art. 28** - The international transfer of personal data will only be allowed to countries that afford a level of personal data protection equivalent to that of the present Law, subject to the following exceptions:

I – when the international transfer of data is necessary for international judicial cooperation between public intelligence and investigation agencies, pursuant to international rules and laws;

II – when the international transfer of data is necessary for the protection of life or the physical safety of the data subject or of a third party;

III – when the competent public body authorizes the transfer, pursuant to the regulation;
IV – when the international transfer of data is a result of obligations undertaken in international cooperation agreement;

V – when the international transfer of data is necessary for the implementation of public policies or duties of public service, being made public pursuant to § 1st of art. 6th.

**Sole Paragraph** - The level of data protection of the country will be assessed by the competent public body, which will take into account:

I – general and sectorial rules provided by the laws in force at the country of destination;

II – nature of data;

III – observance of the general principles of personal data protection established by the present Law;

IV – adoption of the security measures provided in the regulation; and

V – other specific circumstances regarding the transfer.

**Art. 29** - In the case of countries that do not afford an equivalent level of data protection to that of the present Law, the consent referred to in art. 7th will be special and will be provided:

I – by means of a specific statement, distinct from the consent regarding other data processing operations; and

II – with prior and specific information regarding the international character of the operation, which shall warn about the risks involved, considering the vulnerability circumstances of the country of destination.

**Art. 30** - The authorization referred to in item III of the main section of art. 28 will be granted when the data controller offers sufficient guarantees of compliance with the general principles of protection and with the rights of the data subjects, presented on contractual clauses approved for a specific transfer, in standard contractual clauses or in global corporate rules, pursuant with the regulation.

§ 1st - The competent public body may compose standard contractual clauses, which must be in accordance to the general principles of protection and with the rights of the data subjects, guaranteed the joint and several liability, regardless of negligence, of assignor and assignee.

§ 2nd - Data controllers which are part of the same group of companies or multinational conglomerate may submit global corporate rules for approval by the competent public body, which
shall be mandatory for all companies of the group or conglomerate, with the purpose of being authorized to conduct international transfer of data within the group or conglomerate without the need of specific authorizations, pursuant to the general principles of protection and the rights of the data subjects.

§ 3rd - During the assessment of the contractual clauses or of global corporate rules by the competent public body, additional information or the conduction of audits regarding the processing operations may be required.

Art. 31 - Assignor and assignee are jointly and severally liable for data processing conducted overseas or in nation territory, in any event, regardless of negligence.

Art. 32 – In the cases of international transfer of data from a foreign country to Brazil, data processing in national territory will be only allowed when, in the operations undertaken in that foreign country, the rules regarding the grant of consent have been complied with.

Art. 33 – The competent public body may establish additional rules to allow the categorization of a processing operation as an international transfer of personal data.

CHAPTER VII – AGENTS LIABILITY

Section I – Processing Agents and Indemnification

Art. 34 - The data controller and the data processor are the personal data processing agents.

Art. 35 - Whoever, through the processing of personal data, causes, individual or collective, material or moral damage to another, is obliged to indemnify.

§ 1st - The Judge, in civil lawsuits, can reverse the burden of proof in favor of the data subject when, in his opinion, the data subject’s allegation is plausible or when the production of proof by the data subject may be excessively burdensome;

§ 2nd – The data controller or the data processor can avoid liability if they prove that the event which caused damages is not imputable to them.

____________________________

7 TN.: In the original version the expression used in Portuguese is “ressarcimento de danos”. We understand that, in the context it is being used, it has the sense of “indemnification”.

Page 14 of 19
Art. 36 - Any waiver of requirement for consent does not relieve the processing agents from other obligations established by the present Law, especially, to abide by the general principles and the guarantee of rights of the data subjects.

Art. 37 - The appropriate sanctions under the present Law shall be personally imputable to data processors and data controllers of public bodies which do not comply with the present Law, as provided in Law No 8112, of December 11, 1990 and Law No 8429 of June 2nd, 1992.

Art. 38 - The competences and responsibilities relating to the management of databases within public bodies and entities, as well as the responsibility for the performance of official acts relating to personal data, shall be defined in the regulations that deal with the definition of its competences.

Section II – Data Controller and Data Processor

Art. 39 - The data processor shall perform the processing according to the instructions provided by the data controller, who will monitor compliance with such instructions and with the rules relating to the matter.

§ 1st - The data controller is jointly and several liable regarding to all processing operations performed by the data processor.

§ 2nd – The competent public body may order the data controller to draft a privacy impact report relating to its data processing operations, pursuant to regulation.

Art. 40 - The data controller and the data processor shall keep a record of the personal data processing operations performed by them, pursuant to the provisions of art. 15.

Sole Paragraph – The competent public body may rule on the format, structure and term of record keeping.

Section III – Personal Data Processing Officer

Art. 41 – The data controller shall appoint an officer who will be in charge of the personal data processing.

§ 1st - The officer’s identity and contact information shall be publicly disclosed in a clear and objective manner, preferably on the data controller’s website.

§ 2nd – the officer’s activities shall consist of:

I – receiving complaints and communications from data subjects, provide clarifications and undertake appropriate measures;
II – receive communications from the competent public body and undertake appropriate measures;

III – instruct the entities’ staff regarding the practices to be observed for the protection of personal data; and

IV – other duties established by additional rules or determined by the data controller.

§ 3rd – The competent public body will establish additional rules regarding the appointment and duties of the officer, including the possibility of exemption of the obligation to appoint an officer, considering criteria of nature or size of the entity, as well as the volume of data processing operations.

Section IV – Data Security and Confidentiality

Art. 42 – The data processor shall implement constantly updated technical and administrative security measures, proportionate to the nature of the processed information and able to protect personal data from unauthorized access and accidental or illegal destruction, loss, modification, disclosure, dissemination, or any form of inappropriate or illegal data processing.

Sole Paragraph – Security measures must be compatible with the current state of technology, with the nature of the data and with the specific characteristics of the processing, particularly regarding sensitive data.

Art. 43 – The processing agents or any other person involved in any phase of the data processing abides by a duty of secrecy regarding the personal data, even after its termination.

Art. 44 – The data controller shall immediately notify the competent public body in the event of any security incident that may cause damages to data subjects.

Sole Paragraph – The notification shall mention, at least:

I – a description of the nature of the relevant personal data;

II – information on the data subjects;

III – description of the security measures employed for data protection, including data encryption procedures;

IV – risks relating to the incident; and

V – measures that have been or will be taken to revert or mitigate the consequences of the damage.
Art. 45 – The competent public body may order the adoption of measures regarding security incidents related to personal data, considering its severity, such as:

I – prompt notification to data subjects;

II - a broad disclosure of the fact in the media; or

III - measures to revert or mitigate the consequences of the damage.

§ 1st – While judging the severity of the incident, any evidence that the appropriate technical measures were adopted to make the relevant personal data unintelligible to unauthorized third parties will be accessed.

§ 2nd – In those cases in which it is possible to establish that the incident endangers the personal safety of the data subjects or that it can cause them damages, a prompt notification to data subjects affected by the security incident will be obligatory, regardless of an order by the competent public body.

Art. 46 - The systems used for the processing of personal data must be structured in order to meet the security requirements, the general principles established by the present Law and by other regulations.

Art. 47 - The competent public body may establish additional rules regarding criteria and minimum security standards, including based on technological developments.

Section V – Best Practices

Art. 48 - The data controllers, individually or through associations, may formulate best practices standards which establish structuring conditions, operational regimes, procedures, security policies, technical standards, specific obligations for all those involved in the processing, educational initiatives or internal supervisory arrangements, pursuant to the provisions of the present Law and additional rules on data protection.

Sole Paragraph – Updated and publicly available best practice standards may be recognized and published by the competent public body.

Art. 49 - The competent public body will stimulate the adoption of technical standards for software and Internet applications that may ease the disposal by data subjects of their personal data, including the right to not being tracked.
CHAPTER VIII – ADMINISTRATIVE SANCTIONS

Art. 50 - The violations to the provisions of the present Law by private legal persons, will be subject to the following administrative sanctions, to be imposed by the competent public body:

I – simple or daily fine;

II – publication of the violation;

III – personal data de-identification;

IV – blockage of personal data;

V – suspension of personal data processing operations, for a period not exceeding two years;

VI – erasure of personal data;

VII – prohibition of sensitive data processing, for a period not exceeding ten years; and

VIII – prohibition of operating databases, for a period not exceeding ten years.

§ 1st - Sanctions may be applied cumulatively.

§ 2nd - The procedures and criteria for the imposition of sanctions will be appropriate to the gravity and extent of the violation, to the nature of the affected individual rights, the existence of recurrence, the economic situation of the offender and to the damages caused, pursuant to the regulation.

§ 3rd - The prohibition periods provided for in sections VII and VIII of the head of this article, may be extended by the competent public body, provided that it detects a failure to comply with its orders, recurrence in offenses or the lack of full compensation for damages caused by the violation.

§ 4th - The foregoing shall not preclude the application of administrative, civil or criminal sanctions defined in specific legislation.

§ 5th - The provisions of sections III thru VII may be applied to public bodies or entities, subject to the provisions of Law No 8112 of December 11, 1990 and Law No 8429 of June 2, 1992.
CHAPTER IX – FINAL PROVISIONS

Art. 51 - The competent public body will establish rules regarding the progressive compliance of databases created up to the date of entry into force of the present Law, taken into account the complexity of the processing operations, the nature of data and the data controller’s size.

Art. 52 – The present Law shall come into force within one hundred and twenty (120) days from the date of its publication.