VELLA PUGLIESE BUOSI GUIDONI

DRAFT BILL

Provides for the processing of personal data[1]
to guarantee the free development of the natural person's personality and of its dignity.

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 by a natural person or by a private or public legal person, aiming at protecting the fundamental rights of freedom and privacy and the free development of the natural person's personality.

Art. 2 –Personal data protection in Brazil is founded on the respect to privacy, as well as to:

I - informational self-determination;

II - freedom of expression, communication and opinion;

III - the preservation of intimacy, private life, honor and image;

IV - economic and technological development; and

V - free enterprise, free competition and consumer protection.

Art. 3 - The present law applies to any processing operation[2] undertaken by a natural person or a private or public legal person, regardless of the country where its headquarters are located or of the country where the data is located, as long as:

I – the processing operation occurs in national territory;

II - the processing operation has the purpose of offering or delivering goods or services or the processing of data of individuals located in national territory; or

---

[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.

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

Sole Paragraph - personal data will be deemed to have been collected in national territory if the data subject is located therein at the moment of the collection.

Art. 4 - 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, artistic, literary or academic purposes; or

III – undertaken for the exclusive purposes of public security, national defense, State security, investigation and law enforcement activities.

§ 1st – The data processing provided in item III above will be regulated by a specific law, pursuant to general principles of data protection and to the data subjects rights as provided by the present Law.

§ 2nd - The processing by private entities of data mentioned item III above is prohibited, except in procedures conducted by a public legal person which must be specifically notified to the competent public body.

§ 3rd - The competent public body will issue technical opinions and recommendations relating to the exceptions provided for in items II and III, as well as may request to the data controller privacy impact reports.

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 electronic identifiers when those are related to a person;

II – processing: shall mean all operations carried out with personal data, such as those relating to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, discarding, assessment or control of the information, modification, dissemination, transfer, disclosure or extraction;

III – sensitive data: shall mean personal data related to ethnic or racial origins, religious 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 and biometric data;

IV – anonymized data: shall mean data pertaining to a data subject which cannot be identified;

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 personal data being processed;

VII – consent: shall mean the free and unequivocal 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 who lays 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 – officer: a natural person, appointed by the data controller, to act as a communication channel before the data subjects and the competent public body;

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

XII – anonymization: any procedure by which a given data no longer can be linked, directly or indirectly, to an individual;

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

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

XV – 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.

Art. 6 – The processing of personal data must comply with the duty of good-faith and the following principles:

I – purpose: under which processing must be carried out for legitimate, specified and explicit purposes, which must also be informed to data subject;

II – adequacy: under which, context considered, processing must be compatible with the purposes of such processing and with the legitimate expectations of the data subject;

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

IV – free access: 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: under which the data must accurate, clear, relevant and up-to-dated, the frequency required to accomplish the purpose of the processing taken into account;

VI – transparency: under which clear, adequate and easily accessible information relating to the processing operation and the respective processing agents, must guaranteed to the data subject;

VII – security: 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: 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: under which processing must not be used for discriminatory purposes.

CHAPTER II – REQUIREMENTS FOR THE PROCESSING OF PERSONAL DATA

Section I – Requirements for the Processing

Art. 7 – Personal data may only processed in the following cases:

I – upon free and unequivocal consent by the data subject;

II – for the fulfillment of a legal obligation by the data controller;

III – where processing and shared use of data relating to the exercise of rights or fulfillment of duties defined by law or regulation, is necessary for the public administration;

IV – for the performance of historical, scientific and statistical research, guaranteed, whenever possible, the anonymization of personal data;

V – by request of the data subject, when necessary for the performance of a contract or preliminary procedures related to a contract, to which the data subject is a part of;

VI – for the regular exercise of rights in judicial and administrative procedures;

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

VIII – for the protection of health, in the context of a procedure performed by health care professionals or public health authorities;

IX - when necessary to meet the legitimate interests of the data controller, subject to the interests or fundamental rights and freedom of the data subject.

§ 1st – Whenever hypothesis provided for by items II and III are applicable, the data subject shall be informed of the processing of his personal data.

§ 2nd – In the case of breach of the provisions of §1st, the data processor or the data controller responsible for processing the data may be held liable.

§ 3rd - The processing of personal data to which access is public, should be carried out according to this law, taking into account the purpose, good faith and public interest which justified their availability.

Art. 8 - The data subject shall have facilitated access to information concerning the processing of its data, which must be made available in clear, adequate and prominent fashion in regard to the following elements, among others:

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 the disclosure;

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

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

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

b) – the possibility of denouncing to the competent public body any breach to the provisions of this Law; and

c) – the choice of not giving consent, in circumstances where consent is required with an explanation of the consequences of refusal.

§ 1st – In the event that consent is required, it 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 item IV to the head of this article, the data controller must communicate to data subject the updated contact information.

§ 3rd – 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, as defined by the competent public body.

§ 4th - When the consent to the processing of personal data is a condition for the supply of product or service or to the exercise of a right, the data subject shall be informed prominently of such fact as well as to the means by which data subject can exercise control over the processing of his data.

§ 5th – The competent public body may define the means mentioned in the preceding paragraph.

Art. 9 – The consent referred to in art. 7, I shall be free and unequivocal and provided in writing or by other means capable of certifying it.

§ 1st – If consent is to be given in writing, it must be provided separately from other contractual provisions.

§ 2nd - The burden of proof that consent has been obtained in compliance with the provisions of this Law, lies upon the data controller.

§ 3rd - 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.

§ 4th - Consent must relate to specified purposes, generic authorizations for the processing of personal data being reputed as void.

§ 5th - Consent can be revoked at any given time, by express manifestation of the data subject.

§ 6th – In the event of modification of the information mentioned in items I, II, III or V of art. 8, the data controller shall obtain a new consent from the data subject, specifically highlighting the content of the modifications.

§ 7th - The competent public body may adjust the requirements for consent, considering the context in which it is provided and the nature of the personal data provided.

Art. 10 - The legitimate interest of the data controller may only justify a single data processing which must be necessary and based on a concrete situation, guaranteed the fundamental rights and freedoms of the data subject.

§ 1st - The legitimate interest should address the legitimate expectations of the data subject regarding the processing of his personal data, pursuant to the provisions of art. 6, II.

§ 2nd - The data controller must take measures to ensure the transparency of data processing based on its legitimate interest and provide effective mechanisms to allow the data subjects express their opposition to the processing of their personal data.

§ 3rd - When the data processing is based on the legitimate interest of the data controller, only the personal data absolutely necessary for the intended purpose can be processed and should be anonymized whenever this measure is compatible with the purpose of the processing operation.

§ 4th - The competent public body may request to the data controller a privacy impact report relating to its data processing operations based on legitimate interest.

Art. 11 – The processing of sensitive personal data is prohibited, except:

I – if data subject gives unequivocal, express and specific 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 their data.

II – without the data subject giving consent, 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 anonymization of sensitive 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; or

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

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

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

§ 3rd – Provisions of letter "c" of item II only apply if the activities described are not related to commercial activities, public administration, criminal or intelligence investigation, ensuring wherever possible, anonymization of personal data.

§ 4th - In cases where letters 'a' and 'b' of item II, are invoked by public bodies and entities, publicity shall be given to the waiver of consent pursuant to art. 24.

Art. 12 – 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, or may request the data controller to present a privacy impact report.

Art. 13 - The anonymized data will be considered personal data for the purposes of this Law when the anonymization process to which it has been subject to is reversed or when, by means of reasonable efforts, it may be reversed.

§ 1st - For the purposes of this Law, all data used to put together the behavioral profile of a particular natural person, even if not identified, may also be considered as personal data.

§ 2nd - The competent public body may rule on standards and techniques used in anonymization processes and conduct assessments relating to their safety.

§ 3rd - The sharing and use of anonymized data must be subject to publicity and transparency, without prejudice of the competent public body requesting the data controller a privacy impact report relating any risks that the anonymization process may be reversed, as well as to other aspects of their data processing.

Art. 14 - The processing of personal data pertaining to children or and to legally incapable persons, as defined by law, may only occur with the consent of the legal guardian and in their best interest.

Sole Paragraph - The processing of personal data of teenagers and relatively incapable persons shall observe the following conditions:

I - authorization conditioned to supervision, assistance or confirmation by the legal guardian; and

II - respect for their personal status, without prejudice of legal guardians revoking consent to the processing of their personal data at any time.

Section II – Termination of Processing

Art. 15 – 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, which includes the exercise of its right to revoke consent as provided for in art. 9, § 5th; or

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

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

Art. 16 – 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 anonymization of personal data; or

III – transfer to third parties, provided the requirements for data processing established by this Law are respected.

Sole Paragraph – Except as provided in specific legislation and as long as 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. 17 – 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. 18 – The data subject has the right to obtain, regarding his data:

I – confirmation of the existence of the data processing;

II – access to his data;

III – correction of incomplete, inaccurate and outdated data;

IV – anonymization, blockage or erasure of unnecessary or excessive data, or of data processed in breach of the provisions of this Law;

V - portability, upon request, of his personal data to another service or product provider;

VI – erasure at any time, of personal data to which treatment the data subject has consented; and

VII – effectiveness of consumer protection laws, when applicable, to the protection of personal data.

§ 1st – The data subject may oppose to processing based on a waiver of consent, when in 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, specifying whenever possible, the actual 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, anonymization or blockage of any previously disclosed data, the data controller shall notify those third parties to whom data has been disclosed, in order that they replicate such operations.

Art. 19 – 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 date of data subject's request.

§ 1st - Personal data will be stored in a format that favors 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 data processing is originated from data subject`s consent or from contract, 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.

§ 4th - The competent public body may define the formats in which the information and data will be provided to the data subject.

§ 5th – The competent public body may rule differently, for specified sectors, regard time periods defined in items I and II to the main section of this article.

Art. 20 - 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.

Sole Paragraph - The data controller shall provide, whenever requested, clear and adequate information regarding the criteria and procedures used to take the automated decision, commercial and industrial secrets to be respected.

Art. 21 - Personal data relating to the regular exercise of rights by the data subject cannot be used to his detriment.

Art. 22 - The defense of data subject's interests and rights may be exercised individually or collectively in court, as provided by Law No 9,507 of November 12, 1997, by articles 81 and 82 of Law No 8,078 of September 11, 1990, by Law No 7,347 of July 24, 1985, and in other methods of individual and collective legal protection.

CHAPTER VI – PERSONAL DATA PROCESSING BY PUBLIC AUTHORITY

Art. 23 - The processing of personal data by legal entities of public law referred to in the sole paragraph of art. 1 of Law 12,527 of November 18, 2011, shall be conducted in regard to their public purpose, in the pursuit of public interest and for purposes of the fulfillment of their legal competence or of legal duties relating to public service.

Art. 24 – Public bodies will make their data processing activities public, by means of clear, accurate and updated information provided through easily accessible means, preferably their websites, pursuant to the transparency principles established in art. 5, item VI of this Law.

§ 1st – The public bodies which process data shall appoint an officer, as established in art. 40.

§ 2nd - The competent public body may define the means by which processing operations will be made public.

Art. 25 – State-owned entities and parastatal companies operating in private regimes pursuant to art. 173 of the Federal Constitution, shall receive, under this Law, the same treatment as that granted to private legal persons.

Sole Paragraph – State-owned entities and parastatal companies when implementing public policies and not acting in private regime, shall receive, under this Law, the same treatment as that granted public bodies and agencies, pursuant to this Chapter.

Art. 26 - The shared use of personal data by the public authority shall meet specific purposes relating to the implementation of public policies and legal authority by public bodies and agencies, pursuant to the principles of personal data protection established in art. 6 of this Law.

Sole Paragraph - The public authority is prohibited to transfer to private entities personal data contained in databases to which the public authority has access, except in cases of decentralized execution of public activities which require such transfer, and exclusively for this specific and determined purpose, and pursuant to provisions of Law No 12527 of November 18, 2011.

Art. 27 - Data disclosure or transfer of personal data by a public legal person to a private legal person must be informed to the competent public body and will rely on data subject's consent, except:

I – in those cases of waiver of consent as provided by this Law; or

II – in the case of shared use data, which must be made public in accordance to art. 24.

Art. 28 – The disclosure of personal data between public bodies and entities will be made public, pursuant to art. 24.

Art. 29 - The competent public body may request, at any given time, to public entities that process personal data to provide a specific report concerning the scope and nature of processed data, as well as further details of the data processing operation, and may issue supplementary technical opinion, to ensure compliance with the present Law.

Art. 30 - The competent public body may establish additional rules concerning the activities of disclosure of personal data.

Section II – Liability

Art. 31 – In the event the provisions of the present Law are breached by reason of treatment of personal data by public legal persons, the competent public body may send report indicating the appropriate measures to cease the violation.

Sole Paragraph - The penalties applicable to public agents under this Law shall apply personally to public officials as provided by Law No. 8.112, of December 11, 1990, and Law No. 8429 of June 2, 1992.

Art. 32 – The competent public body may request to agents to public authorities to issue privacy impact reports, as well as suggest adoption of standards and best practices to the processing of personal data by public authorities.

CHAPTER V – INTERNATIONAL TRANSFER OF DATA

Art. 33 - The international transfer of personal data will only be allowed in the following cases:

I - to countries that afford a level of personal data protection at least as equivalent to that of the present Law;

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

III – 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;

IV – when the competent public body authorizes the transfer;

V – when the international transfer of data is a result of obligations undertaken in international cooperation agreement;

VI – when the international transfer of data is necessary for the implementation of public policies or duties by public service, publicity required pursuant to art. 24;

VII – when the data subject has given consent to such transfer, with prior and specific information regarding the international character of the operation and warning regarding the risks involved.

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 sector specific rules provided by the laws in force at the country of destination;

II – nature of data;

III – adherence to 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. 34 - The authorization referred to in item IV of the main section of art. 33 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 by the competent public body for a specific transfer, in standard contractual clauses or in global corporate rules, pursuant to the regulation.

§ 1st - The competent public body may draft standard contractual clauses or approve statements contained in documents that support the international transfer of data, all of which must be in accordance to the general principles of data protection and with the rights of the data subjects, guaranteed the joint and several liability of assignor and assignee, regardless of negligence.

§ 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, documents or of global corporate rules by the competent public body, additional information or the conduction of audits regarding the processing operations may be required.

§ 4th – Sufficient guarantees of compliance with the general principles of data protection and the rights of data subjects mentioned in the main section of this article will also be analyzed in relation to the technical and organizational measures taken by the data processor pursuant to the provisions of Paragraph 1st and Paragraph 2nd of art. 45.

Art. 35 – Regardless of negligence, assignor and assignee are jointly and severally liable for data processing regardless of where they are located and of the specific situation.

CHAPTER VI – PERSONAL DATA PROCESSING AGENTS

Section I – Data Controller and Data Processor

Art. 36 - The data controller and the data processor are the personal data processing agents.

Art. 37 - The data controller and the data processor shall keep a record of the personal data processing operations performed by them.

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

Art. 38 - 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.

Art. 39 - 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 disclosure of personal data between data controllers and data processors as private legal persons depends on the data subject's consent, except for those cases of waiver of consent provided by the present Law.

Section II – 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 and contractors regarding the practices to be observed for the protection of personal data; and

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

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

Section III – Liability and Damage Compensation

Art. 42 – Whoever, through the processing of personal data, causes, individual or collective, material or moral damage to another, is obliged to indemnify.

Sole Paragraph - 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.

Art. 43 – 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. 44 – In the event of personal data processing, 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 processing performed in the exercise of the duties establishes by Law No 12,527 of November 18, 2011, regarding the guarantee of access to public information.

CHAPTER VII – DATA SECURITY AND BEST PRACTICES

Section I – Data Security and Confidentiality

Art. 45 –The data processor shall implement technical and administrative security measures, able to protect personal data from unauthorized access and accidental or illegal destruction, loss, modification, disclosure or any form of inappropriate or illegal data processing.

§1st - The competent public body may issue technical and administrative standards to guarantee effectiveness to the requirement made in the main section of this article, taking into account the nature of the data processed and the specific characteristics of the processing and the current state of technology, particularly regarding sensitive data.

§2nd – The security measures must be observed starting from the stage of design of the product or service until their execution.

Art. 46 - 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. 47 - The data controller shall notify the competent public body in the event of any security incident that may cause risk or relevant damages to data subjects.

Sole Paragraph – The notification shall be made within a reasonable timeframe and 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;

V – in the case that the notification has not been immediate, the reasons for the delay; and

VI - measures that have been or will be taken to revert or mitigate the consequences of the damage.

Art. 48 –The competent public body will verify the severity of the incident and may, if necessary to safeguard the rights of the data subject, order to the data controller to adopt other measures, such as:

I – prompt notification to data subjects;

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

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

§ 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. 49 - 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.

Section II – Best Practices

Art. 50 - 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, and other aspects related to the processing of personal.

§ 1st – In establishing best practices standards, the data controller and the data processor shall take into account the nature, scope and purpose of the data processing and of the data, as well as the probability and severity of risks of damage to individuals.

§ 2nd - Updated and publicly available best practice standards may be recognized and published by the competent public body.

Art. 51 - The competent public body will stimulate the adoption of technical standards that make the control by data subjects of their personal data easier.

CHAPTER VIII – CONTROL

Section I – Administrative Sanctions

Art. 52 - 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 – anonymization of personal data;

IV – blockage of personal data;

V – suspension of personal data processing operations;

VI – erasure of personal data;

VII –suspension of the operation of databases.

§ 1st – Sanctions will be accompanied by reasoned judgement, and may be established separately or cumulatively, taking into account the peculiarities of the case and the severity and nature of the violation, the nature of the individual rights impacted by the violation, the existence of recurrence, the economic situation of the offender and to the damages caused.

§ 2nd - The foregoing does not replace the application of administrative, civil or criminal sanctions defined in specific legislation.

§ 3rd - The provisions of sections III thru VII may be applied to public bodies or entities, subject to the provisions of Law No 8,112 of December 11, 1990 and Law No 8,429 of June 2, 1992.

Section II - Competent Public Body and the National Board of Data Protection and Privacy

Art. 53 - The competent public body appointed to oversee the implementation and enforcement of this Law shall have the following duties:

I - ensuring the protection of personal data, pursuant to the law;

II – definition guidelines for a National Policy for Personal Data Protection and Privacy;

III - to disseminate to the public the knowledge of the rules and public policy regarding personal data protection, as well as security measures;

IV - to promote research of national and international practices regarding personal data and privacy protection;

V - encourage the adoption of standards for products and services that facilitate the exercise by the data subject of the control over their personal data;

VI - to promote cooperation efforts with personal data protection authorities of other countries, being those international or transnational in nature;

VII - issue annual reports regarding its activities;

VIII - issue rules on personal data and privacy protection; and

IX - perform other acts within its jurisdiction, including those provided by this Law and in general legislation.

Art. 54 - The National Data Protection and Privacy Council will be composed of fifteen representatives and fifteen alternates appointed by the Minister of Justice, for a two-year term, renewable once for the same period, as follows:

I - seven representatives of the Federal Executive Branch, appointed by act of the Executive Branch;

II - one representative appointed by the House of Representatives;

III - one representative appointed by the Senate;

IV - one representative appointed by the National Judiciary Council;

V - one representative appointed by the National Council for Public Prosecutors;

VI - one representative appointed by the Internet Steering Committee in Brazil (CGI.br);

VII - one representative of the civil society;

VIII - one representative of the academy; and

IX - two representatives of the private sector.

§ 1st - Participation in the National Council will be considered an activity of relevant public interest and will be unpaid.

§ 2nd - The representatives referred to in items II to VI of the caption and their respective alternates shall be appointed by the heads of the respective bodies and entities.

§ 3rd - The representatives referred to in items VII to IX of caption and their respective alternates shall be appointed in accordance with the National Data Protection and Privacy Council internal regulation which shall be later approved.

Art. 55. The National Data Protection and Privacy Council shall:

I - provide information and advice for the development of the National Policy for Personal Data and Privacy Protection;

II - issue annual assessment reports regarding the implementation of actions required by the National Policy for Personal Data and Privacy Protection;

III - suggest actions to be implemented by the competent public body;

IV - carry out studies and debates on the protection of personal data and privacy; and

V - disseminate knowledge on personal data and privacy protection to the public.

CHAPTER IX – FINAL PROVISIONS

Art. 56 – The present Law shall come into force within one hundred and eighty (180) days from the date of its publication.

Sole Paragraph - The competent public body will establish rules regarding the progressive compliance of databases created until the date of entry into force of the present Law, taken into account the complexity of the processing operations and the nature of the data.