Provides for the protection of personal data and changes Law No. 12,965, of April 23, 2014 (the "Brazilian Internet Law").

The NATIONAL CONGRESS decrees:

CHAPTER I
PRELIMINARY PROVISIONS

Art. 1 This Law provides for the processing of personal data, including by digital means, by a natural person or a legal entity of public or private law, with the purpose of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

Art. 2 The discipline of personal data protection is grounded on the following:

I – respect for privacy;

II – informed self-determination;

III – freedom of expression, information, communication and opinion;

IV – inviolability of intimacy, honor and image;

V – economic and technological development and innovation;

VI – free enterprise, free competition and consumer defense;

VII – human rights, free development of personality, dignity and exercise of citizenship by natural persons.

Art. 3 This Law applies to any processing operation carried out by a natural person or a legal entity of public or private law, irrespective of the mean, the country in which its headquarter is located or the country where the data are located, provided that:

I – the processing operation is carried out in the national territory;

II – the purpose of the processing activity is to offer or provide goods or services or the processing of data of individuals located in the national territory; or

III – the personal data being processed were collected in the national territory.

§1 Data collected in the national territory are considered to be those whose data subject is in the national territory at the time of collection.

§2 Data processing as provided in Item IV of the lead sentence of Art. 4 of this Law is exempted from the provisions of Item I of this article.

Art. 4 This Law does not apply to the processing of personal data that:

I – is done by a natural person exclusively for private and non-economic purposes;

II – is done exclusively:

a) for journalistic and artistic purposes; or

b) academic purposes, with Arts. 7 and 11 of this Law being applicable in these cases;

III – is done exclusively for purposes of:

a) public safety;

b) national defense;

c) state security; or

d) activities of investigation and prosecution of criminal offenses; or

IV – have their origin outside the national territory and are not the object of communication, shared data use with Brazilian processing agents or the object of international transfer of data with another country that is not the country of origin, since the country of origin provides a level of personal data protection adequate to that established in this Law.

§1 Processing of personal data as provided in Item III shall be governed by specific legislation, which shall provide proportional and strictly necessary measures for fulfilling the public interest, subject to due legal process, the general principles of protection and the rights of the data subjects as provided in this Law.

§2 Processing of the data referred to in Item III of the lead sentence of this article is forbidden for legal entity of private law, except in procedures under the authority of legal entity of public law, of which the national authority shall be specifically informed

and which shall observe the limitation imposed in §4 of this article.

§3 The national authority shall issue technical opinions or recommendations regarding the exceptions provided in Item III of the lead sentence of this article, and shall request of the responsible parties impact reports on protection of personal data.

§4 Under no circumstances the entirety of the personal data in a database, as provided in Item III of the lead sentence of this article, may be processed by a legal entity of private law.

Art. 5 For purposes of this Law, the following definitions apply:

I – personal data: information regarding an identified or identifiable natural person;

II – sensitive personal data: personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person;

III – anonymized data: data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing;

IV – database: structured set of personal data, kept in one or several locations, in electronic or physical support;

V – data subject: a natural person to whom the personal data that are the object of processing refer to;

VI – controller: natural person or legal entity, of public or private law, that has competence to make the decisions regarding the processing of personal data;

VII – processor: natural person or legal entity, of public or private law, that processes personal data in the name of the controller;

VIII – officer: natural personal, appointed by the controller, who acts as a communication channel between the controller and the data subjects and the national authority;

IX – processing agents: the controller and the processor;

X – processing: any operation carried out with personal data, such as collection,

production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction;

XI – anonymization: use of reasonable and available technical means at the time of the processing, through which data loss the possibility of direct or indirect association with an individual;

XII – consent: free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose;

XIII – blocking: temporary suspension of any processing operation, by means of retention of the personal data or the database;

XIV – deletion: exclusion of data or a set of data stored in a database, irrespective of the procedure used;

XV – international data transfer: transfer of personal data to a foreign country or to an international entity of which the country is a member;

XVI – shared use of data: communication, dissemination, international transfer, interconnection of personal data or shared processing of banks of personal data by public agencies and entities, in compliance with their legal competences, or between these and private entities, reciprocally, with specific authorization, for one or more types of processing allowed by these public entities, or among private entities;

XVII –impact report on protection of personal data: documentation from the controller that contains the description of the proceedings of processing of the personal data that could generate risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate the risk;

XVIII – research body: body or entity of the direct or indirect public administration or a nonprofit legal entity of private law, legally organized under the Brazilian law, with headquarter and jurisdiction in Brazil, that includes in its institutional mission or in its corporate or statutory purposes basic or applied research of historic, scientific, technological or statistical nature;

XIX – national authority: body of the indirect public administration responsible for supervising, implementing and monitoring the compliance with this Law.

Art. 6 Activities of processing of personal data shall be done in good faith and be subject to the following principles:

I – purpose: processing done for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes;

II – suitability: compatibility of the processing with the purposes communicated to the data subject, in accordance with the context of the processing;

III - necessity: limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing;

IV – free access: guarantee to the data subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their personal data;

V – quality of the data: guarantee to the data subjects of the accuracy, clarity, relevancy and updating of the data, in accordance with the need and for achieving the purpose of the processing;

VI – transparency: guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy;

VII – security: use of technical and administrative measures which are able to protect personal data from unauthorized accesses and accidental or illegal situations of destruction, loss, alteration, communication or dissemination;

VIII – prevention: adoption of measures to prevent the occurrence of damages due to the processing of personal data;

IX – nondiscrimination: impossibility of carrying out the processing for illegal or abusive discriminatory purposes; and

X – accountability: demonstration by the agent of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures.

CHAPTER II

PROCESSING OF PERSONAL DATA

Section I

Requirements for the Processing of Personal Data

Art. 7 Processing of personal data shall only be carried out under the following circumstances:

I – with the consent of the data subject;

II – for compliance with a legal or regulatory obligation by the controller;

III – by the public administration, for the processing and shared use of data which are necessary for the execution of public policies provided in laws or regulations, or based on contracts, agreements or similar instruments, subject to the provisions of Chapter IV of this Law;

IV – for carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data;

V – when necessary for the execution of a contract or preliminary procedures related to a contract of which the data subject is a party, at the request of the data subject;

VI – for the regular exercise of rights in judicial, administrative or arbitration procedures, the last pursuant to Law No. 9,307, of September 23, 1996 (the "Brazilian Arbitration Law");

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

VIII – to protect health, in a procedure carried out by health professionals or by health entities;

IX – when necessary to fulfill the legitimate interests of the controller or a third party, except when the data subject's fundamental rights and liberties which require personal data protection prevail; or

X – for the protection of credit, including as provided in the pertinent legislation.

§1 When the provisions of Items II and III of the lead sentence of this article are

applicable, and except in the situations provided in Art. 4 of this Law, the data subject shall be informed of the situations in which processing of her/his data will be allowed.

§2 The way in which information is made available as provided in §1 and Item I of the lead sentence of Art. 23 of this Law may be specified by the national authority.

§3 The processing of publicly accessible personal data shall consider the purpose, the good faith and the public interest that justify its being made available.

§4 The consent requirement provided in the lead sentence of this article is waived for data manifestly made public by the data subject, safeguarding the rights of the data subject and the principles provided in this Law.

§5 The controller who has obtained the consent referred to in Item I of the lead sentence of this article that needs to communicate or share personal data with other controllers shall obtain specific consent from the data subject for this purpose, except when the need for such consent is waived as provided in this Law.

§6 Any eventual waiver of the consent requirement does not release processing agents from the other obligations provided in this Law, especially that of obeying the general principles and guarantees of the data subject's rights.

Art. 8 The consent provided in Item I of Art. 7 of this Law shall be given in writing or by another means that demonstrates the manifestation of the will of the data subject.

§1 If consent is given in writing, it must appear highlighted so as to stand out from the other contractual clauses.

§2 The burden of proof is on the controller to show that consent was obtained in compliance with the provisions of this Law.

§3 It is prohibited to process personal data if the consent is defective.

§4 Consent shall refer to particular purposes, and generic authorizations for processing personal data shall be void.

§5 Consent may be revoked at any time, by express manifestation of the data subject, through a facilitated and free of charge procedure, with processing carried out under previously given consent remaining valid as long as there is no request for deletion, pursuant to Item VI of the lead sentence of Art. 18 of this Law.

§6 If there is a change in the information as referred to in Items I, II, III or V of Art. 9 of this Law, the controller shall inform the data subject, with specific highlight of the content of the changes, in which case the data subject, in those cases where her/his consent is required, may revoke it if she/he disagrees with the change.

Art. 9 The data subject has the right to facilitated access to information concerning the processing of her/his data, which much be made available in a clear, adequate and ostensible manner, concerning, among other characteristics provided in regulation for complying with the principle of free access:

I – the specific purpose of the processing;

II – the type and duration of the processing, being observed commercial and industrial secrecy;

III – identification of the controller;

IV – the controller's contact information;

V – information regarding the shared use of data by the controller and the purpose;

VI – responsibilities of the agents that will carry out the processing; and

VII – the data subject's rights, with explicit mention of the rights provided in Art. 18 of this Law.

§1 In situations where consent is required, it shall be considered void if the information provided to the data subject contains misleading or abusive content or was not previously presented in a transparent, clear and unambiguous way.

§2 In the situation when consent is required, if there are changes in the purpose of the processing of personal data that are not compatible with the original consent, the controller shall previously inform the data subject of the changes of purpose, and the data subject may revoke her/his consent if she/he disagrees with the changes.

§3 When the processing of personal data is a condition for the provision of a product or service or for the exercise of a right, the data subject shall be informed with special highlight of this fact and of the means by which she/he may exercise her/his data subject's rights as listed in Art. 18 of this Law.

Art. 10. Controller's legitimate interest can only be grounds for processing personal data for legitimate purposes, based on particular situations, which include but

are not limited to:

I – support and promotion of the controller's activity; and

II – protection of data subject's regular exercise of her/his rights or provision of services that benefit her/him, subject to their legitimate expectations and fundamental rights and freedoms, in accordance with this Law.

§1 When processing is based on the controller's legitimate interest, only the personal data which are strictly necessary for the intended purpose may be processed.

§2 The controller shall adopt measures to ensure transparency of data processing based on her/his legitimate interests.

§3 The national authority may request of the controller an impact report on protection of personal data, when processing is based on her/his legitimate interest, being observed commercial and industrial secrecy.

Section II
Processing of Sensitive Personal Data

Art. 11. The processing of sensitive personal data shall only occur in the following situations:

I – when the data subject or her/his legal representative specifically and distinctly consents, for the specific purposes;

II – without consent from the data subject, in the situations when it is indispensable for:

a) controller's compliance with a legal or regulatory obligation;

b) shared data processing by the public administration of necessary data for the execution of public policies provided in laws or regulations;

c) studies carried out by a research entity, whenever possible ensuring the anonymization of sensitive personal data;

d) the regular exercise of rights, including in a contract and in a judicial, administrative and arbitration procedure, the last in accordance with the terms of Law No. 9,307, of September 23, 1996 (the "Brazilian Arbitration Law");

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

f) the protection of health, in a procedure carried out by health professionals or by health entities; or

g) ensuring the prevention of fraud and the safety of the data subject, in processes of identification and authentication of registration in electronic systems, respecting the rights mentioned in Art. 9 of this Law and except when fundamental rights and liberties of the data subject which require protection of personal data prevail.

§1 The provisions of this article apply to any processing of personal data that reveals sensitive personal data and that may cause harm to the data subject, subject to the provisions of specific legislation.

§2 When the provisions of lines a and b of Item II of the lead sentence of this article are applied by public agencies and entities, said waiver of consent shall be publicized, pursuant to Item I of the lead sentence of Art. 23 of this Law.

§3 Communication or shared use of sensitive personal data between controllers for the purpose of obtaining an economic advantage may be prohibited or regulated by the national authority, being heard the sectoral entities of the public authority, within their competences.

§4 Communication or shared use between controllers of sensitive personal data referring to health for the purpose of obtaining an economic advantage is prohibited, except in cases of portability of data when consented by the data subject.

Art. 12. Anonymized data shall not be considered personal data, for purposes of this Law, except when the process of anonymization to which the data were submitted has been reversed, using exclusively its own means, or when it can be reversed applying reasonable efforts.

§1 The determination of what is reasonable shall take objective factors into account, such as cost and time necessary to reverse the process of anonymization, depending on the available technology, and the exclusive use of its own means.

§2 Data can be considered personal, for purposes of this Law, when they are used to formulate behavioral profiles of a particular natural person, if that person is identified.

§3 The national authority may provide for standards and techniques to be used in

processes of anonymization, and carry out security checks, with opinions from the National Board for the Protection of Personal Data.

Art. 13. When carrying out public health studies, research entities may have access to personal databases, which shall be processed exclusively within the entity and strictly for the purpose of carrying out studies and research and shall be kept in a controlled and secure environment, in accordance with security practices provided in specific regulation and that include, whenever possible, anonymization or pseudonymization of the data, as well as taking into account the proper ethical standards related to studies and research.

§1 Disclosure of the results or of any portion of the study or the research, as mentioned in the lead sentence of this article, shall under no circumstances reveal personal data.

§2 The research entity shall be liable for the security of the information provided in the lead sentence of this article, and it is forbidden, under no circumstances, to transfer the data to a third party.

§3 Access to data as provided in this article shall be the object of regulation by the national authority and of the authorities in the area of health and sanitation, within the scope of their competences.

§4 For purposes of this article, pseudonymization is processing by means of which data can no longer be directly or indirectly associated with an individual, except by using additional information kept separately by the controller in a controlled and secure environment.

Section III
Processing of Children and Adolescents' Personal Data

Art. 14. The processing of personal data belonging to children and adolescents shall be done in their best interest, pursuant to this article and pertinent legislation.

§1 The processing of children's personal data shall be done with specific and highlighted consent given by at least one of the parents or the legal representative.

§2 When processing data as mentioned in §1 of this article, controllers shall make public the information about the types of data collected, the way it is used and the procedures for exercising the rights referred to in Art. 18 of this Law.

§3 Children's personal data may be collected without the consent mentioned in §1 of this article when collection is necessary to contact the parents or the legal representative, used one single time and not stored, or for their protection, and under no circumstances shall the data be passed on to third parties without consent as provided in §1 of this article.

§4 Controllers shall not condition the participation of data subjects, as referred to in §1 of this article, to games, internet applications or other activities for providing personal information beyond what is strictly necessary for the activity.

§5 The controller shall use all reasonable efforts to verify that the consent referred to in §1 of this article was given by the child's representative, considering available technologies.

§6 Information on the processing of data referred to in this article shall be provided in a simple, clear and accessible manner, taking into account the physical-motor, perceptive, sensorial, intellectual and mental characteristics of the user, using audiovisual resources when appropriate, in order to provide the necessary information to the parents or the legal representative and that is appropriate for the children's understanding.

Section IV
Termination of Data Processing

Art. 15. The processing of personal data shall be terminated under the following circumstances:

I – verification that the purpose has been achieved or that the data are no longer necessary or pertinent to achieve the specific purpose intended;

II – end of the processing period;

III – communication by the data subject, including when exercising her/his right to revoke consent, as provided in §5 of Art. 8 of this Law, subject to the public interest;

or

IV – determination by the national authority when there has been a violation of the provisions of this Law.

Art. 16. Personal data shall be deleted following the termination of their processing, within the scope and technical limits of the activities, being their storage authorized for the following purposes:

I – compliance with a legal or regulatory obligation by the controller;

II – study by a research entity, ensuring, whenever possible, the anonymization of the personal data;

III – transfer to third parties, provided that the requirements for data processing as provided in this Law are obeyed; or

IV – exclusive use of the controller, with access by third parties being prohibited, and provided the data has been anonymized.

CHAPTER III
DATA SUBJECTS' RIGHTS

Art. 17. All natural person is assured ownership of her/his personal data, with the fundamental rights of freedom, intimacy and privacy being guaranteed, under the terms of this Law.

Art. 18. The personal data subject has the right to obtain the following from the controller, regarding the data subject's data being processed by the controller, at any time and by means of request:

I – confirmation of the existence of the processing;

II – access to the data;

III – correction of incomplete, inaccurate or out-of-date data;

IV – anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law;

V – portability of the data to another service or product provider, by means of an express request and subject to commercial and industrial secrecy, pursuant to the

regulation of the controlling agency;

VI – deletion of personal data processed with the consent of the data subject, except in the situations provided in Art. 16 of this Law;

VII – information about public and private entities with which the controller has shared data;

VIII – information about the possibility of denying consent and the consequences of such denial;

IX – revocation of consent as provided in §5 of Art. 8 of this Law.

§1 The personal data subject has the right to petition, regarding her/his data, against the controller before the national authority.

§2 The data subject may oppose the processing carried out based on one of the situations of waiver of consent, if there is noncompliance with the provisions of this Law.

§3 The rights provided in this article shall be exercised by means of express request by the data subject or her/his legally constituted representative to the processing agent.

§4 If it is impossible to immediately adopt the measure mentioned in §3 of this article, the controller shall send a reply to the data subject in which she/he may:

I – communicate that she/he is not the data processing agent and indicate, whenever possible, who the agent is; or

II – indicate the reasons of fact or of law that prevent the immediate adoption of the measure.

§5 The request as mentioned in §3 of this article shall be fulfilled without costs to the data subject, within the time periods and under the terms as provided in regulation.

§6 The responsible shall immediately inform the processing agents with which she/he has carried out the shared use of data of the correction, deletion, anonymization or blocking of data, so that they can repeat an identical procedure.

§7 The portability of personal data referred to in Item V of the lead sentence of this article does not include data that have already been anonymized by the controller.

§8 The right referred to in §1 of this article may also be exercised before consumer-defense entities.

Art. 19. Confirmation of the existence of or access to personal data shall be provided by means of request by the data subject:

I – in a simplified format, immediately; or

II – by means of a clear and complete declaration that indicates the origin of the data, the nonexistence of record, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy, provided within a period of fifteen (15) days as from the date of the data subject's request.

§1 Personal data shall be stored in a format that facilitates the exercise of the right to access.

§2 Information and the data may be provided, at the data subject's discretion:

I – by an electronic mean that is safe and suitable to this purpose; or

II – in printed form.

§3 When processing originates from the consent of the data subject or from a contract, the data subject may request a complete electronic copy of her/his personal data, subject to commercial and industrial secrecy, in accordance with regulations of the national authority, in a format that allows its subsequent use, including for other processing operations.

§4 The national authority may provide differently regarding the time periods provided in Items I and II of the lead sentence of this article for specific sectors.

Art. 20. The data subject has the right to request review, by a natural person, of decisions taken solely on the bases of automated processing of personal data that affects her/his interests, including decisions intended to define her/his personal, professional, consumer or credit profile or aspects of her/his personality.

§1 Whenever requested to do so, the controller shall provide clear and adequate information regarding the criteria and procedures used for an automated decision, subject to commercial and industrial secrecy.

§2 If there is no offer of information as provided in §1 of this article, based on commercial and industrial secrecy, the national authority may carry out an audit to verify discriminatory aspects in automated processing of personal data.

Art. 21. Personal data concerning the regular exercise of rights by the data subject

cannot be used to her/his detriment.

Art. 22. The defense of the interests and rights of data subjects may be carried out in court, individually or collectively, as provided in pertinent legislation regarding the instruments of individual and collective protection.

CHAPTER IV
PROCESSING OF PERSONAL DATA BY PUBLIC AUTHORITIES

Section I
Rules

Art. 23. Processing of personal data by legal entities of public law referred to in sole paragraph of Art. 1 of Law No. 12,527, of November 18, 2011 (the "Brazilian Access to Information Law"), shall be done in fulfillment of its public purpose, in benefit of a public interest, for the purpose of performing legal competences or discharging legal attributions of the public service, provided that:

I – they communicate the situations in which, in the exercise of their competences, they carry out processing of personal data, supplying clear and up-to-date information about the legal base, purpose, procedures and practices used to carry out these activities in easily accessible media, preferably on their websites; and

II – an officer is appointed when carrying out personal data processing operations, in accordance with Art. 39 of this Law.

§1 The national authority may provide for the forms of publicity regarding processing operations.

§2 The provisions of this Law do not release the legal entities mentioned in the lead sentence of this article from establishing the authorities as provided in Law No. 12,527, of November 18, 2011 (the "Brazilian Access to Information Law").

§3 The time periods and procedures for exercising data subjects' rights before the public authorities shall obey the provisions of specific legislation, especially the provisions of Law No. 9,507, of November 12, 1997 (the "Brazilian Habeas Data Law"), of Law No. 9,784, of January 29, 1999 (the "Federal Administrative Procedure Law"),

and of Law No. 12,527, of November 18, 2011 (the "Brazilian Access to Information Law").

§4 Notarial and registry services, carried out under private law by delegation of public authorities, shall receive the same treatment given to legal entities as provided in the lead sentence of this article, in accordance with the terms of this Law.

§5º Notarial and registry bodies shall provide access to data by electronic means to the public administration, in view of the purposes mentioned in the lead sentence of this article.

Art. 24. Public companies and mixed-capital companies that operate in the competing market, subject to the provisions of Art. 173 of the Federal Constitution, shall receive the same treatment given to private legal entities of private law, under the terms of this Law.

Sole paragraph. Public and mixed-capital companies, when they are carrying out public policies and within the scope of their execution, shall receive the same treatment given to the bodies and entities of the public authorities, under the terms of this Chapter.

Art. 25. Data shall be kept in an interoperable format and structured for shared use intended for the execution of public policies, provision of public services, decentralization of public activity, dissemination and access to information by the general public.

Art. 26. The shared use of personal data by public authorities shall fulfill the specific purposes of execution of public policies and legal attributions by agencies and public entities, subject to the principles of personal data protection listed in Art. 6 of this Law.

§1 It is forbidden for public authorities to transfer to private entities personal data contained in databases to which they have access, except:

I – in cases of decentralized execution of public activity that requires transfer, exclusively for this specific and distinct purpose, subject to the provisions of Law No. 12,527, of November 18, 2011 (the "Brazilian Access to Information Law"); and

II – in cases in which the data are publicly accessible, subject to the provisions of this Law.

§2 Contracts and agreements as mentioned in §1 of this article shall be communicated to the national authority.

Art. 27. Communication or shared use of personal data from a legal entity of public law to a legal entity of private law shall be communicated to the national authority and shall rely on the consent of the data subject, except:

I – in situations in which consent is waived as provided in this Law;

II – when there is shared use of data, which will be publicized pursuant to Item I of the lead sentence of Art. 23 of this Law; or

III – in the exceptions contained in §1 of Art. 26 of this Law.

Art. 28. The national authority may request, at any time, that entities of the public authority carry out operations of processing of personal data, specific report about the scope and nature of the data and other details of the processing, and may issue complementary technical opinion to ensure compliance with this Law.

Art. 29. The national authority may establish complementary rules for communication or shared used of personal data activities.

Section II
Accountability

Art. 30. When there is an infringement of this Law as a result of personal data processing by public agencies, the national authority may send a report with applicable measures to stop the violation.

Art. 31. The national authority may request agents of the public authorities to publish impact reports on protection of personal data and may suggest the adoption of standards and good practices for processing personal data by the public authorities.

CHAPTER V
INTERNATIONAL TRANSFER OF DATA

Art. 32. International transfer of personal data is only allowed in the following

cases:

I – to countries or international organizations that provide a level of protection of personal data that is adequate to the provisions of this Law;

II – when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in this Law, in the form of:

a) specific contractual clauses for a given transfer;

b) standard contractual clauses;

c) global corporate norms;

d) regularly issued stamps, certificates and codes of conduct;

III – when the transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial agencies, in accordance with the instruments of international law;

IV – when the transfer is necessary to protect life or physical safety of the data subject or of third party;

V – when the national authority authorizes the transfer;

VI – when the transfer results in a commitment undertaken through international cooperation;

VII – when the transfer is necessary for the execution of a public policy or legal attribution of public service, which shall be publicized pursuant to Item I of the lead sentence of Art. 23 of this Law;

VIII – when the data subject has given her/his specific consent and distinct for the transfer, with prior information about the international nature of the operation, with this being clearly distinct from other purposes; or

IX – when it is necessary to satisfy the situations provided in Items II, V and VI of Art. 7 of this Law.

Sole paragraph. For purposes of Item I of this article, the legal entities of public law referred to in the sole paragraph of Art. 1 of Law No. 12,527, of November 18, 2011 (the “Brazilian Access to Information Law”), within their legal competences, and those parties accountable, within the scope of their activities, may request the national authority

to evaluate the level of protection of personal data provided by a country or international organization.

Art. 33. The level of data protection in the foreign country or international organization referred to in Item I of the lead sentence of Art. 32 of this Law shall be evaluated by the national authority, which shall take into consideration:

I – the general and sectorial rules of legislation in force in the receiving country or international organization;

II – the nature of the data;

III – compliance with the general principles of personal data protection and data subjects' rights as provided in this Law;

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

V – the existence of judicial and institutional guarantees for respecting the rights of personal data protection; and

VI – other specific circumstances relating to the transfer.

Art. 34. The definition of the content of standard contractual clauses, as well as the verification of specific contractual clauses for a particular transfer, global corporate rules or stamps, certificates and codes of conduct, referred to in Item II of the lead sentence of Art. 32 of this Law, will be done by the national authority.

§1 To verify the provision of the lead sentence of this article, requirements, conditions and minimum guarantees for the transfer that obey the rights, guarantees and principles of this Law must be considered.

§2 When analyzing contractual clauses, documents or global corporate rules submitted to the national authority for approval, supplementary information or due diligences performed for verification of the processing operations may be required, when necessary.

§3 The national authority may designate certification entities to carry out the provisions of the lead sentence of this article, which shall remain under their inspection subject to the terms defined in regulation.

§4 Acts carried out by certification entities may be reviewed by the national authority and, if they are not in compliance with this Law, submitted for revision or

voided.

§5 Guarantees sufficient for compliance with the general principles of protection and data subject's rights referred to in the lead sentence of this article shall also be analyzed in accordance with the technical and organizational measures adopted by the processor, according to the provisions of §§1 and 2 of Art. 45 of this Law.

Art. 35. Changes to guarantees presented as sufficient for compliance with the general principles of protection and of the data subject's rights referred to in Item II of Art. 32 of this Law shall be communicated to the national authority.

CHAPTER VI
PERSONAL DATA PROCESSING AGENTS
Section I
Controller and Processor

Art. 36. The controller and the processor shall keep records of personal data processing operations carried out by them, especially when based on legitimate interest.

Art. 37. The national authority may determine that the controller must prepare an impact report on protection of personal data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy.

Sole paragraph. Subject to the provisions of the lead sentence of this article, the report must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards and mechanisms of risk mitigation.

Art. 38. The processor shall carry out the processing according to the instructions provided by the controller, which shall verify the obedience of the own instructions and of the rules governing the subject.

Art. 39. The national authority may provide standards of interoperability for purposes of portability, free access to data and security, as well as regarding time records

must be kept, especially in view of the need and the transparency.

Section II
Data Protection Officer

Art. 40. The controller shall appoint an officer to be in charge of processing personal data.

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

§2 Officer's activities consist of:

I – accepting complaints and communications from data subjects, providing explanations and adopting measures;

II – receiving communications from the national authority and adopting measures;

III – orienting entity's employees and contractors regarding practices to be taken in relation to personal data protection; and

IV – carrying out other duties as determined by the controller or set forth in complementary rules.

§3 The national authority may establish complementary rules about the definition and the duties of the officer, including situations in which the appointment of such person may be waived, according to the nature and the size of the entity or the volume of data processing operations.

Section III
Liability and Loss Compensation

Art. 41. The controller or the processor that, as a result of carrying out their activity of processing personal data, cause material, moral, individual or collective damage to others, in violation of legislation for the protection of personal data, are obligated to redress it.

§1 In order to ensure the actual indemnification to the data subject:

I – the processor jointly answers for the damages caused by the processing when they do not comply with the obligations of data protection legislation or when she/he has not followed controller's lawful instructions, in which case the processor is deemed equivalent to the controller, except in cases of exclusion as provided in Art. 42 of this Law;

II – controllers who are directly involved in the processing from which damages resulted to the data subject shall jointly answer, except in cases of exclusion as provided in Art. 42 of this Law.

§2 The judge, in a civil lawsuit, may reverse the burden of proof in favor of the data subject when, at her/his discretion, the allegation appears to be true, there are no funds for the purpose of producing evidence or when production of evidence by the data subject would be overly burdensome.

§3 Lawsuits for compensation for collective damages, the objective of which is liability pursuant to the terms of the lead sentence of this article, may be filed collectively in court, subject to the provisions of pertinent legislation.

§4 Anyone who pays compensation for damage to the data subject has the right of recourse against other liable parties, to the extent of their participation in the damaging event.

Art. 42. Processing agents shall only not be held liable when they prove that:

I – they did not carry out the processing of personal data that is attributed to them;

II – although they did carry out the processing of personal data that is attributed to them, there was no violation of the data protection legislation; or

III – the damage arises from exclusive fault of the data subject or a third party.

Art. 43. Processing of personal data shall be irregular when it does not obey the legislation or when it does not provide the security that its data subject can expect of it, considering the relevant circumstances, among which are:

I – the way in which it was done;

II – the result and the risks that one can reasonably expect of it;

III – the techniques for processing personal data available at the time it was done.

Sole paragraph. The controller or the processor who neglect to adopt the security

measures provided in Art. 45 of this Law shall be held liable for the damages caused by the violation of the security of the data that caused the damage.

Art. 44. When there is violation of data subject's right in the scope of consumer relations, the rules of liability provided in pertinent legislation shall apply.

CHAPTER VII
SECURITY AND GOOD PRACTICES
Section I
Security and Secrecy of Data

Art. 45. Processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing.

§1 The national authority may provide minimum technical standards to make the provisions of the lead sentence of this article applicable, taking into account the nature of the processed information, the specific characteristics of the processing and the current state of technology, especially in the case of sensitive personal data, as well as the principles provided in the lead sentence of Art. 6 of this Law.

§2 The measures mentioned in the lead sentence of this article shall be complied with as from the conception phase of the product or service through to its execution.

Art. 46. Processing agents or any other person that intervenes in one of the processing phases undertake to ensure the security of the information as provided in this Law regarding personal data, even following conclusion thereof.

Art. 47. The controller must communicate to the national authority and to the data subject any occurrence of a security incident that may create risk or relevant damage to the data subjects.

§1 The communication shall be done in a reasonable time period, as defined by the national authority, and shall contain, as a minimum:

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

II – information on the data subjects involved;

III – an indication of the technical and security measures used to protect the data, subject to commercial and industrial secrecy;

IV – the risks related to the incident;

V – the reasons for delay, in cases in which communication was not immediate; and

VI – the measures that were or will be adopted to reverse or mitigate the effects of the damage.

§2 The national authority shall verify the seriousness of the incident and may, if necessary to safeguard the data subjects' rights, order the controller to adopt measures, such as:

I – broad disclosure of the event in communications media; and

II – measures to reverse or mitigate the effects of the incident.

§3 When judging the severity of the incident, eventual demonstration that adequate technical measures were adopted to render the affected personal data unintelligible will be analyzed, within the scope and the technical limits of the services, to third parties who were not authorized to access them.

Art. 48. The systems used for processing personal data shall be structured in order to meet the security requirements, standards of good practice and governance, general principles provided in this Law and other regulatory rules.

Section II
Good Practice and Governance

Art. 49. Controllers and processors, within the scope of their competence, concerning processing of personal data, individually or in associations, may formulate rules for good practice and governance that set forth conditions of organization, a regime of operation, procedures, including for complaints and petitions from data subjects, security norms, technical standards, specific obligations for the various parties involved in the processing, educational activities, internal mechanisms of supervision and risk

mitigation and other aspects related to the processing of personal data.

§1 When establishing rules of good practice, the controller and the processor shall take into consideration, regarding the processing and the data, the nature, scope, purpose and probability and seriousness of the risks and the benefits that will result from processing of data subjects' data.

§2 When applying the principles mentioned in Items VII and VIII of the lead sentence of Art. 6 of this Law, and subject to the structure, scale and volume of her/his operations, as well as the sensitivity of the processed data and the probability and seriousness of the damages to data subjects, the controller may:

I – implement governance program for privacy that, as a minimum:

a) demonstrate the controller's commitment to adopt internal processes and policies that ensure broad compliance with rules and good practices regarding the protection of personal data;

b) are applicable to the entire set of personal data under her/his control, irrespective of the means used to collect them;

c) are adapted to the structure, scale and volume of her/his operations, as well as to the sensitivity of the processed data;

d) establish adequate policies and safeguards based on a process of systematic evaluation of the impacts on and risks to privacy;

e) have the purpose of establishing a relationship of confidence with data subjects, by means of transparent operations, and that ensure mechanisms for the data subject to participate;

f) are integrated into its general governance structure and establish and apply internal and external mechanisms of supervision;

g) have plans for response to incidents and solution; and

h) are constantly updated based on information obtained from continuous monitoring and periodic evaluations;

II – demonstrate the effectiveness of her/his privacy governance program when appropriate and, especially, at the request of the national authority or other entity responsible for promoting compliance with good practices or codes of conduct, which,

independently, promote compliance with this Law.

§3 Rules of good practice and governance shall be published and updated periodically and may be recognized and disclosed by the national authority.

Art. 50. The national authority shall encourage the adoption of technical standards that facilitate data subjects' control of their personal data.

CHAPTER VIII
MONITORING
Section I
Administrative Sanctions

Art. 51. Data processing agents that commit infractions of the rules provided in this Law are subject to the following administrative sanctions, to be applied by the national authority:

I – warning, with an indication of the time period for adopting corrective measures;

II – simple fine of up to two percent (2%) of a private legal entity's, group or conglomerate revenues in Brazil, for the prior financial year, excluding taxes, up to a total maximum of fifty million reais (R$ 50,000,000.00) per infraction;

III – daily fine, subject to the total maximum referred to in Item II;

IV – publicizing of the infraction once it has been duly ascertained and its occurrence has been confirmed;

V – blocking the personal data to which the infraction refers to until its regularization;

VI – deletion of the personal data to which the infraction refers to;

§1 The sanctions shall be applied following an administrative procedure that will provide opportunity for a full defense, in a gradual, single or cumulative manner, in accordance with the peculiarities of the particular case and taking into consideration the following parameters and criteria:

I – the severity and the nature of the infractions and of the personal rights affected;

II – the good faith of the offender;

III - the advantage realized or intended by the offender;

IV – the economic condition of the offender;

V – recidivism;

VI – the level of damage;

VII – the cooperation of the offender;

VIII – repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing the damage, for secure and proper data processing, in accordance with the provisions of Item II of §2 of Art. 47 of this Law.

IX – adoption of a good practice and governance policy;

X – the prompt adoption of corrective measures; and

XI – the proportionality between the severity of the breach and the intensity of the sanction.

§2 The provisions of this article do not substitute the application of administrative, civil or criminal sanctions defined in specific legislation.

§3 The provisions of Items I, IV, V and VI of the lead sentence of this article may be applied to public entities and bodies, without prejudice to the provisions of Laws Nos. 8,112, of December 11, 1990 (the "Law of Legal Framework for Public Servants"), 8,429, of June 2, 1992 (the "Administrative Improbity Law"), and 12,527, of November 18, 2011 (the "Brazilian Access to Information Law").

§4 When calculating the amount of the fine provided in Item II of the lead sentence of this article, the national authority may consider total revenues of the company or group of companies, when it does not have the amount of revenues from the business activity in which the infraction occurred, defined by the national authority, or when the amount is presented in an incomplete form or is not demonstrated unequivocally and reputably.

Art. 52. The national authority shall define the methodologies that will be used for the calculation of the base value for fines, by means of its own regulations concerning administrative sanctions for violations of this Law, which must be the object of a public consultation.

§1 The methodologies referred to in the lead sentence of this article shall be previously published, for the information of the processing agents, and shall objectively present the forms and methods for calculating the base value of the fines, which shall contain detailed grounds for all its elements, demonstrating obedience to the criteria provided in this Law.

§2 The regulation of sanctions and corresponding methodologies shall establish the circumstances and conditions for adopting simple or daily fines.

Art. 53. The amount of daily fines applied to infractions of this Law shall be subject to the severity of the infraction and the extent of the damage or losses caused, and with grounded reasoning by the national authority.

Sole paragraph. The notice of imposition of a daily fine shall contain, as a minimum information, the description of the obligation being imposed, the reasonable timeframe stipulated by the body for compliance and the amount of the daily fine to be applied for non-compliance.

CHAPTER IX
FINAL AND TRANSITIONAL PROVISIONS

Art. 54. Law No. 12,965, of April 23, 2014 (the "Brazilian Internet Law"), shall henceforth contain the following alterations:

"Art. 7 …

X – permanent deletion of personal data that has been provided to an internet application, upon request, at the termination of the relationship between the parties, except in the situations in which storage of records is obligatory, as provided in this Law and in that which governs personal data protection;…"(Reviewer's Note)

"Art. 16…

II – from personal data that are excessive in relation to the purpose for which consent was given by the data subject, except in situations provided in the Law that governs personal data protection."(Reviewer's Note)

Art. 55. The foreign company shall be notified and summonsed of all procedural acts provided in this Law, irrespective of power of attorney or contractual or statutory

provisions, in the person of the agent or representative or person responsible for its subsidiary, agency, branch, establishment or office located in Brazil.

Art. 56. The national authority and the Anísio Teixeira National Institute for Educational Studies and Research (Inep), within the scope of their competences, shall enact specific regulations for accessing data processed by the Union for compliance with the provisions of §2 of Art. 9 of Law No. 9,394, of December 20, 1996 (the "Directive and Bases of National Education Act"), and those relating to the National Higher Education Evaluation System (Sinaes), as provided in Law No. 10,861, of April 14, 2004.

Art. 57. The national authority shall establish rules on the progressive suitability of databases established up to the date this Law comes into force, taking into account the complexity of the data processing operations and the nature of the data.

Art. 58. The rights and principles expressed in this Law do not exclude others provided in the Brazilian legal system related to the matter or in international treaties to which the Federative Republic of Brazil is a party.

Art. 59. This Law shall come into force eighteen (18) months following its official publication.