Law n. 13,709/2018 - Provides for the protection of personal data and changes Law n. 12,965/2014 (Brazilian Civil Rights Framework for the Internet)

THE NATIONAL CONGRESS decrees:

CHAPTER I

PRELIMINARY PROVISIONS

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

Article 2. The grounds of the regulation on personal data protection are the following:

I – respect for privacy;

II – informative self-determination;

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

IV – inviolability of intimacy, honor and reputation;

V – economic and technological development and innovation;

VI – free initiative, free competition and consumer protection; and

VII – human rights, free development of personality, dignity and exercise of citizenship by the individuals.

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

I – the processing operation be carried out in the Brazilian territory;

~~II – the purpose of the processing activity be the offer or supply of goods or services or the processing of data of individuals located in the Brazilian territory;~~

II – the processing activity has for an objective the offer or the supply of goods or services or the data processing of individuals located in the national territory; or

III – the processed personal data have been collected in the Brazilian territory.

Paragraph 1 Personal data collected in the Brazilian territory are understood as those personal data whose data subject is in the Brazilian territory at the time of the collection.

Paragraph 2 The provision of item I of this article shall not apply to the processing of data set forth in item IV of the head provision of article 4 of this Law.

Article 4. This Law shall not apply to the processing of personal data:

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

II – made exclusively for:

a) journalistic and artistic purposes; or

~~b) academic purposes, in which case articles 7 and 11 of this Law shall apply;~~

b) academic (purposes);

III - made exclusively for the following purposes:

a) public security;

b) national defense;

c) safety of the Country; or

d) crime investigation and punishment activities; or

IV – originating from outside the Brazilian territory and which are not subject to communication, shared use of data with Brazilian processing agents or subject to international transfer of data with other country than the country of origin, provided the country of origin provides a degree of personal data protection consistent with the provisions of this Law.

Paragraph 1 The processing of personal data set forth in item III shall be governed by a specific law, which shall contain proportional measures as strictly required to serve the public interest, subject to the due process of law, the general principles of protection and the rights of the data subjects set forth in this Law.

~~Paragraph 2 The processing of the data referred to in item III of the head provision of this article by a person governed by private law is prohibited, except in procedures carried out by a legal entity governed by public law, which shall be the subject matter of specific information to the supervisory authority and which shall observe the limitation imposed in paragraph 4 of this article.~~

Paragraph 2 The data processing referred by the III of the lead sentence of this article done by a private law entity shall only be admitted in proceedings under the guardianship of public law entity, in which case shall be respected the Paragraph3 limitation.

~~Paragraph 3 The supervisory authority shall issue technical opinions or recommendations relating to the exceptions set forth in item III of the head provision of this article, and it shall request the persons in charge to provide data protection impact assessments.~~

Paragraph 3 The personal data in the data basis constituted for the purposes of the III of the lead sentence of this article shall not be processed in its entirety by private law entity, not included the ones controlled by Public Authority.

Paragraph 4 In no event can all personal data of the database set forth in item III of the head provision of this article be processed by a person governed by private law.

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

I – personal data: information related to an identified or identifiable a natural person;

II – sensitive personal data: personal data on racial or ethnic origin, religious belief, public opinion, affiliation to union or religious, philosophical or political organization, data relating to the health or sex life, genetic or biometric data, whenever related to a natural person;

III – anonymized data: data relating to an data subject who cannot be identified, considering the use of reasonable technical means available at the time of the processed thereof;

IV - database: structured set of personal data, established in one or several sites, in electronic or physical support;

V - data subject: natural person to whom the personal data being processing refer;

VI – controller: natural person or legal entity, governed by public or private law, in charge of making decisions about the processing of personal data;

VII - processor: natural person or legal entity, governed by public or private law, which process personal data in the name of the controller;

~~VIII – data protection officer: natural person appointed by the controller, who acts as a channel of communication between the controller and the data subjects and the supervisory authority;~~

VIII – Data Protection Officer: person designated by the controller to function as a communication channel between the data subjects and the National Data Protection Authority;

IX – processing agents: the controller and the processor;

X - processing: any operation carried out with personal data, such as those that refer to the collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information evaluation or control, modification, communication, transfer, diffusion or extraction;

XI - anonymization: use of reasonable technical means available at the time of processing, by means of which the data loses the possibility of direct or indirect association to a natural person;

XII - consent: free, informed and unequivocal pronouncement by means of which the data subjects agree to the processing of their personal data for a specific purpose;

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

XIV - elimination: exclusion of data or of a group of data stored in a database, irrespective of the procedure used;

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

XVI – shared use of data: communication, diffusion, international transfer, interconnection of personal data or shared processing of personal databases by public bodies and entities in the performance of their statutory duties, or between them and private entities, reciprocally, with specific authorization, for one or more processing modalities permitted by these public entities, or between private entities;

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

~~XVIII – research body: body or entity of the direct or indirect public administration or not-for-profit legal entity governed by private law organized under the Brazilian laws, with its principal place of business and jurisdiction in Brazil, which includes in its institutional mission or in its corporate purpose or purpose established in the By-Laws basic or applied historic, scientific, technological or statistical research;~~

XVIII – research body: body or entity of direct or indirect public administration or non-profit private law entity legally constituted under Brazilian law, with headquarter and under the country jurisdiction, that included in its institutional mission or in its social or statutory purpose basic

or applied research of historical, scientific, technologic or statistic purposes; and

~~XIX - supervisory authority: body of the indirect public administration in charge of supervising, implementing and inspecting compliance with this Law.~~

XIX – National Authority: public administration body responsible to ensure, implement and inspect this law enforcement.

Article 6. The personal data processing activities shall observe the good faith and the following principles:

I - purpose: processing for legitimate, specific and explicit purposes informed to the data subject, without any possibility of subsequent processing inconsistently with these purposes;

II - adequacy: compatibility of the processing with the purposes informed to the data subject, in accordance with the context of the processing;

III - need: limitation of the processing to the minimum processing required for achievement of its purposes, encompassing pertinent, proportional and non-excessive data in relation to the purposes of the data processing;

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

V - quality of data: guarantee, to the data subjects, of accuracy, clarity, relevance and update of the data, according to the need and for compliance with the purpose of the processing thereof;

VI - transparency: guarantee, to the data subjects, of clear, accurate and easily accessible information on the processing and the respective processing agents, subject to business and industrial secrets;

VII - security: use of technical and administrative measures able to protect the personal data from unauthorized accesses and from accidental or unlawful situations of destructions, loss, alteration, communication or diffusion;

VIII - prevention: adoption of measures to prevent the occurrence of damage in view of the processing of personal data;

IX – non-discrimination: impossibility of processing data for discriminatory, unlawful or abusive purposes;

X – liability and accounting: proof, by the agent, of adoption of effective measures able to prove observance of and compliance with the personal data protection rules, and also with the effectiveness of these measures.

CHAPTER II

PROCESSING OF PERSONAL DATA

Section I

Requirements for the Processing of Personal Data

Article 7. The personal data can only be processed in the following events:

I – by means of the data subject's consent;

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

III - by the public administration, for the processing and shared use of data required for the performance of public policies set forth in laws or regulations or supported by contracts, agreements or similar instruments, subject to the provisions of Chapter IV of this Law;

IV – for the conduction of studies by research bodies, guaranteeing, whenever possible, the anonymization of personal data;

V – whenever necessary for the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject;

VI – for the regular exercise of rights in lawsuits, administrative or arbitration proceedings, the latter pursuant to the provisions of Law No. 9.307, of September 23, 1996 (Arbitration Law);

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

VIII – for protection of the health, in a procedure carried out by health professionals or by sanitary entities;

IX – whenever necessary to serve the legitimate interests of the controller or of third parties, except in the event of prevalence of fundamental rights and liberties of the data subject, which require protection of the personal data; or

X – for the protection of credit, including with respect to the provisions of the applicable law.

Paragraph 1 In the events of application of the provisions of items II and III of the head provision of this article and except for the events set forth in article 4 of this Law, the data subjects shall be informed of the events in which the processing of their data shall be permitted.

Paragraph 2 The form of provision of the information set forth in paragraph 1 and in item I of the head provision of article 23 of this Law may be specified by the supervisory authority.

Paragraph 3 The processing of personal data the access to which is public shall consider the purpose, the good faith and the public interest that would justify the availability thereof.

Paragraph 4 The requirement of the consent set forth in the head provision of this article for the data manifestly made public by the data subject is waived, provided the rights of the data subject and the principles set forth in this Law are observed.

Paragraph 5 The controller that has obtained the consent referred to in item I of the head provision of this article and who needs to communicate or share personal data with other controllers must obtain the specific consent of the data subject for such purpose, except for the events of waiver of consent set forth in this Law.

Paragraph 6 No waiver of the requirement of consent releases the processing agents from the other obligations set forth in this Law, especially observance of the general principles and of the guarantee of the rights of the data subject.

Article 8. The consent set forth in item I of article 7 of this Law must be provided in writing or by other means that proves the manifestation of will of the data subject.

Paragraph 1 In case the consent is provided in writing, it shall be included in a clause separated from the other contractual clauses.

Paragraph 2 The controller has the burden to prove that the consent has been obtained in accordance with the provisions of this Law.

Paragraph 3 The processing of personal data by means of defective consent is prohibited.

Paragraph 4 The consent shall refer to defined purposes, and generic authorizations for the processing of personal data shall be null.

Paragraph 5 The consent may be revoked at any time upon express pronouncement of the data subject, by a free and facilitated procedure, ratifying the processing carried out under a previous consent, as long as there is no request for elimination, pursuant to the provisions of item VI of the head provision of article 18 of this Law.

Paragraph 6 In the event of change in the information referred to in items I, II, III or V of article 9 of this Law, the controller shall inform the data subjects, specifically noting the contents of the change and, whenever the consent of the data subjects is required, it may be revoked by the data subjects if they disagree with the change.

Article 9. The data subjects are entitled to facilitated access to the information on the processing of their data, which shall be clearly, adequately and visibly provided, about the following, in addition to other characteristics set forth in the regulations, for compliance with the principle of free access:

I – specific purpose of the processing;

II – form and duration of the processing, observing the business and industrial secrets;

III – identification of the controller;

IV – contact information of the controller;

V - information about the shared use of data by the controller and the purpose;

VI – responsibilities of the agents who shall carry out the processing; and

VII - rights of the data subject, explicitly mentioning the rights contained in article 18 of this Law.

Paragraph 1 Whenever the consent is required, it shall be deemed null in case the information provided to the data subject has misleading or abusive contents or has not been previously presented in a transparent, clear and unequivocal form.

Paragraph 2 Whenever the consent is required, if there are changes in the purpose for processing of personal data that are not compatible with the original consent, the controller shall previously inform the data subjects of the changes of purpose, and the data subjects may revoke the consent in case they disagree with the changes.

Paragraph 3 Whenever the processing of personal data is a condition for the supply of a product or service or for the exercise of a right, the data subjects shall be emphatically informed of this fact and of the means by which they may exercise the data subjects' rights listed in article 18 of this Law.

Article 10. The legitimate interest of the controller may only be a reason for the processing of personal data for legitimate purposes, considered based on specific situations, which include, without limitation:

I – support and promotion of activities of the controller; and

II – protection, in relation to the data subjects, of the regular exercise of their rights or provision of services that benefit them, observing their legitimate expectations and the fundamental rights and liberties, pursuant to the provisions of this Law.

Paragraph 1 Whenever the processing is based on the legitimate interest of the controller, only the personal data strictly required for the desired purpose may be processed.

Paragraph 2 The controller shall adopt measures to guarantee the transparency of the processing of data based on his or her legitimate interest.

Paragraph 3 The supervisory authority may request to the controller a data protection impact assessment whenever the grounds of the processing are its legitimate interest, subject to the business and industrial secrets.

Section II

Processing of Sensitive Personal Data

Article 11. Sensitive personal data can only be processed in the following events:

I – whenever the data subjects or their legal representative specifically and emphatically consent to such processing, for specific purposes;

II – without the supply of the data subjects' consent, whenever they are essential for:

a) compliance with a statutory or regulatory obligation by the controller;

b) shared processing of data required for the enforcement, by the public administration, of public policies set forth in the laws or regulations;

c) the conduction of studies by a research bodies, guaranteeing, whenever possible, anonymization of the sensitive personal data;

d) regular exercise of rights, including in agreements and in lawsuits, administrative or arbitration proceedings, the latter pursuant to the provisions of Law No. 9.307, of September 23, 1996 (Arbitration Law);

e) protection of the life or of the physical safety of the data subjects or of third parties;

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

g) guarantee of the prevention of fraud and of the security of the data subjects, in the processes of identification and certification of record in electronic systems, observing the rights mentioned in article 9 of this Law and except in the event of prevalence of fundamental rights and liberties of the data subjects that require protection of the personal data.

Paragraph 1 The provisions of this article apply to any processing of personal data that discloses sensitive personal data and which may cause damage to the data subjects, except as otherwise provided in a specific law.

Paragraph 2 In the events of application of the provisions of letters "a" and "b" of item II of the head provision of this article by the bodies and public entities, said waiver of consent shall be made public, pursuant to the provisions of item I of the head provision of article 23 of this Law.

Paragraph 3 The communication or the shared use of sensitive personal data among controllers for the purpose of obtaining economic benefit may be prohibited or regulated by the supervisory authority, after consultation with the sectorial Government bodies, within the scope of their duties.

~~Paragraph 4 The communication or shared used among controllers of sensitive data relating to health for the purpose of obtaining economic benefit is prohibited, except in the events of portability of data, upon the data subjects' consent.~~

Paragraph 4 It is forbidden the communication or the shared use between personal data of special category of health controllers with the purpose of economic advantage, except in the case of:

I – data portability when consented by the subject;

II – need of communication to the proper provision of supplementary health care.

Article 12. Anonymized data shall not be deemed personal data for purposes of this Law, except when the anonymization process to which they have been submitted is reversed, using solely the appropriate means, or whenever it can be reversed with reasonable efforts.

Paragraph 1 The determination of what is reasonable shall take objective factors into consideration, such as the cost and time required to reverse the anonymization process, in accordance with the available technologies, and the exclusive use of appropriate means.

Paragraph 2 For purposes of this Law, the data used for formation of the behavioral profile of a given natural person, if identified, may also be deemed personal data.

Paragraph 3 The supervisory authority may provide on standards and techniques used in anonymization processes and make verifications about the security thereof, after consultation with the Brazilian Personal Data Protection Board.

Article 13. In the conduction of studies on public health, the research bodies may have access to personal databases, which shall be exclusively processed within those bodies and for the sole purpose of conduction of studies and researches, and they must always be kept in a controlled and safe environment, according to the security practices set forth in the specific regulations and which include, whenever possible, the anonymization or pseudonymization of the data, and which consider the due ethical standards relating to studies and researches.

Paragraph 1 The disclosure of the results or of any excerpt of the study or of the research set forth in the head provision of this article cannot in any way reveal personal data.

Paragraph 2 The research body shall be responsible for the security of the information set forth in the head provision of this article, and transfer of the data to third parties shall not be in any way permitted.

Paragraph 3 The access to the data set forth in this article shall be regulated by the supervisory authority and by the health and sanitary authorities, within the scope of their duties.

Paragraph 4 For the effects of this article, the pseudonymization is the processing by means of which a data loses the possibility of direct or indirect

association to a natural person, except for the use of additional information separately kept by the controller in a controlled and safe environment.

Section III

Processing of Personal Data of Children and Adolescents

Article 14. The processing of personal data of children and adolescents shall be carried out to their best interest, pursuant to the provisions of this article and of the applicable law.

Paragraph 1 The processing of personal data of children shall be carried out with the specific and separate consent of at least one of the parents or by the legal guardian.

Paragraph 2 In the processing of data set forth in paragraph 1 of this article, the controllers shall maintain public the information on the types of data collected, the form of use thereof and the procedures for exercise of the rights referred to in article 18 of this Law.

Paragraph 3 Personal data of children may be collected without the consent referred to in paragraph 1 of this article whenever the collection is necessary to contact the parents or the legal guardian, used a single time and without storage, or for their protection, and they cannot be transferred to third parties, under any circumstance, without the consent set forth in paragraph 1 of this article.

Paragraph 4 The controllers shall not subject the participation of the data subjects as set forth in paragraph 1 of this article in games, internet applications or other activities to the provision of personal information in addition to those strictly necessary for the activity.

Paragraph 5 The controller shall use all reasonable efforts to confirm that the consent to which paragraph 1 of this article refers was given by the person responsible for the child, considering the available technologies.

Paragraph 6 The information on the processing of data referred to in this article shall be provided in a clear, simple and accessible manner, considering the physical and motor, perceptive, sensorial, intellectual and mental

characteristics of the users, with the use of audiovisual resources whenever appropriate, in order to provide the necessary information to the parents or to the legal guardian, as appropriate for the children's understanding.

Section IV

Termination of the Processing of Personal Data

Article 15. Termination of the processing of personal data shall occur in the following events:

I – verification that the purpose was reached or that the data are no longer necessary or pertinent to attain the specific purpose sought;

II – lapse of the processing period;

III - communication of the data subjects, including in the exercise of their right to revoke the consent as set forth in paragraph 5 of article 8 of this Law, upon protection of the public interest; or

IV – order of the supervisory authority, in the event of breach of the provisions of this Law.

Article 16. The personal data shall be eliminated after termination of the processing thereof, within the scope and technical limits of the activities, and conservation thereof shall be authorized for the following purposes:

I - compliance with a statutory or regulatory obligation by the controller;

II – studies by a research body, guaranteeing, whenever possible, the anonymization of personal data;

III - transfer to third parties, upon compliance with the data processing requirements set forth in this Law; or

IV – exclusive use of the controller, provide the data are anonymized, it being understood that the access thereto by third parties is prohibited.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 17. All natural people are ensured the ownership of their personal data and the guarantee of the fundamental rights to freedom, intimacy and privacy, pursuant to the provisions of this Law.

Article 18. The data subjects are entitled to obtain from the controller, in relation to the data of the data subjects processed by such controller, at any time and upon request:

I – confirmation of the existence of processing;

II – access to the data;

III – correction of incomplete, inaccurate or outdated data;

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

V - portability of the data to other service providers or suppliers of product, at the express request, and observing the business and industrial secrets, in accordance with the regulation of the controlling body;

VI - elimination of the personal data processed with the consent of the data subjects, except in the events set forth in article 16 of this Law;

VII - information of the public and private entities with which the controller carried out the shared use of data;

VIII - information on the possibility of not providing consent and on the consequences of the denial;

IX – revocation of the consent, pursuant to the provisions of paragraph 5 of article 8 of this Law.

Paragraph 1 The data subjects have the right to petition in relation to their data against the controller before the supervisory authority.

Paragraph 2 The data subjects may oppose to the processing carried out based on one of the events of waiver of consent, in the event of noncompliance with the provisions of this Law.

Paragraph 3 The rights set forth in this article shall be exercised at the express request of the data subjects or of legally appointed representatives, to a processing agent.

Paragraph 4 In case it is impossible to immediately adopt the measure set forth in paragraph 3 of this article, the controller shall send to the data subjects an answer in which he or she may:

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

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

Paragraph 5 The request referred to in paragraph 3 of this article shall be met free of charge to the data subjects, within the terms and in accordance with the provisions set forth in the regulations.

Paragraph 6 The person in charge shall immediately inform the processing agents which whom he or she has shared the use of data of the correction, elimination, anonymization or blocking of the data, for them to repeat an identical procedure.

Paragraph 7 The portability of the personal data to which item V of the head provision of this article refer does not include data that have already been anonymized by the controller.

Paragraph 8 The right to which paragraph 1 of this article refers may also be exercised before the consumer defense bodies.

Article 19. Confirmation of the existence of or access to personal data shall be provided, at the request of the data subjects:

I – immediately, in simplified form; or

II - by means of a clear and complete statement indicating the origin of the data, the inexistence of registration, the criteria used and the purpose of the processing, observing the business and industrial secrets, provided within up to fifteen (15) days as from the date of request of the data subject.

Paragraph 1 The personal data shall be stored in a format that favor the exercise of the right to access.

Paragraph 2 The information and data may be provided, at the discretion of the data subjects: I - by safe electronic means appropriate for this purpose; or II – in printed form.

Paragraph 3 Whenever the processing originates from the consent of the data subjects or from an agreement, the data subjects may request full electronic copies of their personal data, observing the business and industrial secrets, pursuant to the provision of the regulations of the supervisory authority, in a format that permits the subsequent use thereof, including in other processing operations.

Paragraph 4 The supervisory authority may differently provide on the terms set forth in items I and II of the head provision of this article for the specific sectors.

~~**Article 20.** The data subjects are entitled to request a review, by a natural person, of decisions made only based on the automatized processing of personal data that affects their interests, including of decisions designed to define their personal, consumption and credit profile or the aspects of their personality.~~

Article 20. The data subject has the right of demand for a revision of the decisions taken solely by automated processing of personal data that affects their interests, including the decisions meant to define their personal, professional, consumption and credit profiling or aspects of their personality.

Paragraph 1 The controller shall provide, upon request, clear and adequate information on the criteria and procedures used for the automatized decision, observing the business and industrial secrets.

Paragraph 2 In the event of failure to offer the information set forth in paragraph 1 of this article based on the observance of business and industrial secrets, the supervisory authority may conduct an audit o confirm discriminatory aspects in the automatized processing of personal data.

Article 21. The personal data relating to the regular exercise of rights by the data subjects cannot be used against them.

Article 22. The defense of the interests and rights of the data subject may be exercised in court, individually or collectively, in the form of the provisions of the applicable law, about the instruments of individual and collective protection.

CHAPTER IV

PROCESSING OF PERSONAL DATA BY PUBLIC AUTHORITIES

Section I

Rules

Article 23. The processing of personal data by the legal entities governed by public law mentioned in the sole paragraph of article 1 of Law No. 12.527, of November 18, 2011 (Law of Access to Information) shall be carried out to achieve its public purpose, in the pursuit of the public interest, for the purpose of performing the legal attributions or duties of the public service, provided:

I – the events in which they process personal data during performance of their duties, providing clear and updated information on the statutory provision, the purpose, the procedures and the practices used to perform these activities, in vehicles of easy access, preferably on their electronic websites;

~~II – the personal data of those who request access to information, pursuant to the provisions of Law No. 12.527, of November 18, 2011 (Law on Access to the Information) are protected and preserved, it being understood that the~~

~~sharing thereof within the scope of the Government and with legal entities governed by private law is prohibited; and~~

III – a data protection officer be appointed whenever the processing of personal data is carried out, pursuant to the provisions of article 39 of this Law.

Paragraph 1 The supervisory authority may provide on the forms of publicity of the processing operations.

Paragraph 2 The provisions of this Law do not exempt the legal entities mentioned in the head provision of this article from instituting the authorities set forth in Law No. 12.527, of November 18, 2011 (Law on the Access to Information).

Paragraph 3 The terms and procedures to exercise the data subjects' rights before the Government shall observe the provisions of the specific law, especially the provisions of Law No. 9.507, of November 12, 1997 (Habeas Data Law), of Law No. 9.784, of January 29, 1999 (General Law on Administrative Proceedings), and of Law No. 12.527, of November 18, 2011 (Law on the Access to Information).

Paragraph 4 The notary office and registration services privately exercised, by delegation of the Government, shall be granted the same treatment granted to the legal entities referred to in the head provision of this article, pursuant to the provisions of this Law.

Paragraph 5 The notary office and registration bodies shall grant access to the data by electronic means to the public administration, in view of the purposes set forth in the head provision of this article.

Article 24. The state-owned companies and the government-controlled private companies that act by means of competitive bid, subject to the provisions of article 173 of the Brazilian Federal Constitution, shall be granted the same treatment granted to the legal entities governed by private law, pursuant to the provisions of this Law.

Sole paragraph. Whenever state-owned companies and government-controlled private companies are operationalizing public policies and within the scope of execution thereof, they shall be granted the same treatment granted to the Government bodies and entities, pursuant to the provisions of this Chapter.

Article 25. The data shall be kept in an interoperable and structured manner for the shared use, aiming at the execution of public policies, the provision of public services, the decentralization of public activities and the dissemination and the access to the information by the general public.

Article 26. The shared use of personal data by the Government shall meet specific purposes of execution of public policies and legal attribution by the public bodies and entities, subject to the principles of protection of personal data listed in article 6 of this Law.

Paragraph 1 The Government may not transfer to private entities personal data included in databases to which it has access, except:

I – in cases of decentralized performance of public activity that requires the transfer, exclusively for this specific and determined purpose, subject to the provisions of Law No. 12.527, of November 18, 2011 (Law on the Access to Information);

~~II – whenever there is a statutory provision and the transfer is based on contracts, agreements or similar instruments~~; and

~~III – whenever the data are publicly accessible, subject to the provisions of this Law. Paragraph 2 The contracts and agreements set forth in paragraph 1 of this article shall be informed to the supervisory authority.~~

III – if a data protection officer is designated for the personal data processing, according to the article 39;
IV – when there is legal provision or the transference is supported by contracts, agreements or similar instruments;

V – in the case of the data transfer have the purpose of fraud and irregularities prevention, or protect and ensure security and integrity of data subject; or

VI – in the cases which data are publicly accessible, according to this law.

~~**Article 27.** The communication or the shared use of personal data of legal entities governed by public law to legal entities governed by private law shall be informed to the supervisory authority and shall be conditional upon the consent of the data subjects, except:~~

Article 27. The communication or the shared use of personal data from a public law entity to a private law entity will need the data subject consent, except:

I – in the events of waiver of consent set forth in this Law;

II – in the events of shared use of data, which shall be granted publicity pursuant to the provisions of item I of the head provision of article 23 of this Law; or

III – in the exceptions set forth in paragraph 1 of article 26 of this Law.

Article 28. The communication or the shared use of personal data among bodies and entities governed by public law shall be granted publicity, pursuant to the provisions of item I of the head provision of article 23 of this Law.

~~**Article 29.** The supervisory authority may request, at any time, to the Government entities, the conduction of personal data processing operations, specific information on the scope and nature of the data and other details of the processing carried out, and it may issue a supplementary technical report to guarantee compliance with this Law.~~

Article 29. The National Authority could demand, any time, to the bodies and entities of Public Authority the processing of personal data, the specific

information about the scope and nature of data and other details of the processing activity and could issue complementary technical report to ensure this law enforcement.

Article 30. The supervisory authority may establish supplementary rules for the communication activities and shared use of personal data.

Section II

Liability

Article 31. In the event of breach of this Law as a result of the processing of personal data by public bodies, the supervisory authority may send a communication with applicable measures to cease the violation.

Article 32. The supervisory authority may request to Government agents the publication of personal data protection impact assessment and suggest the adoption of standards and good practices for the processing of personal data by the Government.

CHAPTER V

INTERNATIONAL TRANSFER OF DATA

Article 33. The international transfer of personal data is permitted solely in the following cases:

I – to countries or international organizations that provide the appropriate level of protection of personal data provided for by this Law;

II – where the controller provides and demonstrates guarantees of compliance with the principles, rights of the data subject and data protection regime established in this Law, in the form of:

a) specific contractual sections for a given transfer;

b) standard contractual sections;

c) global corporate rules;

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

III – where the transfer is required for international legal cooperation between government intelligence, investigation and police bodies, in accordance with the international law instruments;

IV – where the transfer is required for life protection or physical integrity of the data subject or any third party;

V – where the supervisory authority authorizes such transfer;

VI – where the transfer results in a commitment undertaken under an international cooperation agreement;

VII – where the transfer is required for enforcement of a public policy or legal attribution of the public utility, upon disclosure of the provisions of item I of the main provision of article 23 of this Law;

VIII – where the data subject has provided specific and highlighted consent for such transfer, with previous information on the international nature of the operation, clearly distinguishing it from any other purposes; or

IX – where required to meet the hypotheses established in items II, V and VI of article 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 article 1 of Law No. 12.527 of November 18, 2011 (Access to Information Law), within the scope of their legal powers, and in charge, within the scope of their activities, may request to the supervisory authority the assessment of the level of protection to personal data granted by the international country or organization.

Article 34. The level of data protection of the foreign country or international organization mentioned in item I of the main provision of article 33 of this Law shall be assessed by the supervisory authority, which shall take into account:

I – the general and sectorial rules of the applicable law in the country of destination or international organization;

II – the data nature;

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

IV – the adoption of security measures provided for by regulations;

V – the existence of legal and institutional guarantees for compliance with personal data protection rights; and

VI – any other specific circumstances concerning the transfer.

Article 35. The definition of the content of standard contractual sections, and the verification of specific contractual sections for a given transfer, global corporate rules, or seals, certificates and codes of conduct referred to in item II of the main provision of article 33 of this Law shall be carried out by the supervisory authority.

Paragraph 1 For verification of the provisions in the main provision of this article, the requirements, conditions and minimum guarantees for transfer that comply with the rights, guarantees and principles of this Law shall be taken into account.

Paragraph 2 In the analysis of contractual sections, documents or global corporate rules submitted to the supervisory authority for approval, additional information may be requested or procedures of verification of the processing operations may be carried out, as required.

Paragraph 3 The supervisory authority may designate certification organizations to carry out the provisions of the main provision of this article, which shall be subject to its inspection as defined in regulations.

Paragraph 4 The acts performed by any certification organization may be reviewed by the supervisory authority and, in case they are not in compliance with this Law, they shall be revised or annulled.

Paragraph 5 Sufficient guarantees of compliance with the general principles of protection and with the data subject's rights referred to in the main provision of this article shall be also analyzed in accordance with the technical and organizational measures adopted by the processor, as provided for in paragraphs 1 and 2 of article 46 of this Law.

Article 36. Any changes in the guarantees presented as being sufficient guarantees of compliance with the general principles of protection and with the data subjects' rights referred to in item II of article 33 of this Law shall be communicated to the supervisory authority.

CHAPTER VI

PERSONAL DATA PROCESSING AGENTS

Section I

Controller and Processor

Article 37. The controller and the processor shall keep in record the personal data processing operations carried out by them, especially where they are based on a legitimate interest.

Article 38. The supervisory authority may require the controller to prepare a data protection impact assessment, including sensitive data, relating to its data processing operations, as provided for by the regulations, with due regard for trade and industrial secrets.

Sole paragraph. With due regard for the provisions in the main provision of this article, the report shall contain at least a description of the types of data collected, the methodology used for collection and as guarantee of security of the information, and an analysis of the controller in relation to the measures, safeguards and risk mitigation mechanisms adopted.

Article 39. The processor shall carry out the processing in accordance with the instructions supplied by the controller, which shall determine the compliance with its own instructions and the rules on the matter.

Article 40. The supervisory authority may establish interoperability standards for purposes of portability, free access to data and security, and on the retention time of the registrations, especially in view of the need and transparency.

Section II

Data Protection Officer

Article 41. The controller shall indicate a data protection officer.

Paragraph 1 The identity and contact data of the data protection officer shall be publicly, clearly and objectively disclosed, preferably in the controllers' website.

Paragraph 2 The activities of the data protection officer consist of the following:

I – to accept complaints and communications from the data subjects, provide clarifications and take measures;

II – to receive communications from the supervisory authority and take measures;

III – to instruct the employees and contractors of the entity on the practices to be adopted in relation to the personal data protection; and

IV – to carry out any other duties established by the controller or in supplementary rules.

Paragraph 3 The supervisory authority may establish supplementary rules on the definition and duties of the data protection officer, including the cases in which there is no need for appointing such data protection officer, in accordance with the nature and size of the entity or the volume of data processing operations.

Section III

Liability and Compensation

Article 42. Any controller or processor that, in connection with the performance of the activity of personal data processing, causes any property, moral, individual or collective damage to any third party, in violation of the personal data protection law, shall be required to indemnify it.

Paragraph 1 In order to ensure effective indemnity to the data subject:

I – the processor shall be jointly liable for any damages caused by the processing if the processor fails to comply with the obligations of the data protection law or fails to follow the lawful instructions of the controller, in which case the processor shall be equivalent to the controller, except in the events of exclusion established in article 43 of this Law;

II – any controllers that are directly involved in the processing which resulted in damages to the data subject shall be jointly liable, except in the events of exclusion established in article 43 of this Law.

Paragraph 2 The judge, in a civil proceeding, may reverse the burden of proof in favor of the data subject whenever, in the judge's opinion, the allegation is likely, there is lack of assets for purposes of production of evidence, or the production of evidence by the data subject shall be exclusively burdensome for such data subject.

Paragraph 3 Actions for indemnification of collective damages intended to establish liability, as provided for in the main provision of this article, may be collectively conducted in court, with due regard for the provisions of the applicable law.

Paragraph 4 Anyone who compensates a damage to the data subject shall have a right of recourse against the other liable parties, to the extent of their participation in the harmful event.

Article 43. The processing agents shall not be held liable only if they demonstrate:

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

II – that, although they carried out the personal data processing attributed to them, there was no violation of the data protection law; or

III – that the damage results from exclusive fault of the data subject or any third party.

Article 44. The personal data processing shall be irregular if it fails to comply with the law or fails to provide the security that the data subject may expect therefrom, considering the relevant circumstances, including:

I – the way it is performed;

II – the result and the risks that are reasonably expected from it;

III – the personal data processing techniques available at the time it was carried out.

Sole paragraph. Any controller or processor that causes the damage by failing to take the security measures established in article 46 of this Law shall be liable for the damages arising out of the data security violation.

Article 45. The events of violation of the data subjects' right within the scope of the consumption relationships remain subject to the liability rules established in the applicable law.

CHAPTER VII

SECURITY AND GOOD PRACTICES

Section I

Data Security and Confidentiality

Article 46. The processing agents shall adopt security, technical and administrative measures that are capable of protecting the personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, modification, communication or any form of inappropriate or unlawful processing.

Paragraph 1 The supervisory authority may provide for the minimum technical standards to make the provisions in the main provision of this article applicable, considering the nature of the treated information, the specific characteristics of the processing, and the technology current state, especially in case of sensitive personal data, as well as the principles established in the main provision of article 6 of this Law.

Paragraph 2 The measures referred to in the main provision of this article shall be complied with from the product or service conception phase to the performance thereof.

Article 47. The processing agents or any other person that interferes with any of the processing phases shall be required to ensure the information security provided for by this Law in relation to the personal data, including after expiration thereof.

Article 48. The controller shall notify the supervisory authority and the data subject of the occurrence of any security incident that may result in any relevant risk or damage to the data subjects.

Paragraph 1 Such notice shall be delivered within a reasonable term, as defined by the supervisory authority, and contain at least:

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

II – information on the data subjects involved;

III – indication of the technical and security measures used for data protection, with due regard for trade and industrial secrets;

IV – the risks relating to the incident;

V – the reasons for the delay, in case the notice is not immediate; and

VI – the measures that were or shall be adopted to reverse or mitigate the effects of the loss.

Paragraph 2 The supervisory authority shall determine the severity of the incident and, if required for safeguard of the data subjects right, may order the controller to take measures such as:

I – broad disclosure of the fact in media outlets; and

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

Paragraph 3 In the determination of the incident severity, evidence shall be assessed that appropriate technical measures were adopted to make the affected personal data unintelligible, within the scope and the technical limits of its services, to third parties not authorized to access them.

Article 49. The systems used for personal data processing shall be structured in such a manner as to meet the security requirements, the good practices and governance standards, and the general principles established in this Law and in any other regulatory rules.

Section II

Good Practices and Governance

Article 50. The controllers and processors, within the scope of their authority for personal data processing, individually or by means of associations, may prepare good practices and governance rules that provide for organization conditions, operation system, procedures, including complaints and petitions of data subjects, security rules, technical standards, specific obligations for the different parties involved in the processing, educative actions, internal mechanisms of supervision and risk mitigation, and any other aspects relating to personal data processing.

Paragraph 1 When establishing good practices rules, the controller and the processor shall take into account, in relation to the processing and the data,

the nature, scope, purpose and likelihood and severity of the risks and benefits arising out of the data subjects' data processing.

Paragraph 2 In the application of the principles indicated in items VII and VIII of the main provision of article 6 of this Law, the controller, with due regard for the structure, level and volume of its operations, and the sensitivity of the treated data and the likelihood and severity of the damages to the data subjects', may:

I – implement a privacy governance program that shall at least:

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

b) be applicable to the entire set of personal data under its control, regardless of the manner as it carried out the collection thereof;

c) be adapted to the structure, level and volume of its operations, and to the sensitivity of the treated data;

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

e) be intended to establish a trust relationship with the data subject, by means of transparent actions that ensure mechanisms of participation of the data subject;

f) be integrated to its general governance structure and establish and apply internal and external supervision mechanisms;

g) have an incident response and remediation plan; and

h) be constantly updated based on information obtained from continuous monitoring and periodic assessments;

II – demonstrate the effectiveness of its privacy governance program when appropriate, especially at the request of the supervisory authority or any other entity in charge of promoting compliance with good practices or codes of conduct, which independently promote compliance with this Law.

Paragraph 3 The good practices and governance rules shall be published and updated from time to time and may be acknowledged and disclosed by the supervisory authority.

Article 51. The supervisory authority shall encourage the adoption of technical standards for easier control by the data subjects of their personal data.

CHAPTER VIII

INSPECTION

Section I

Administrative Sanctions

Article 52. The data processing agents, in connection with any infractions of the rules established in this Law, shall be subject to the following administrative penalties applicable by the supervisory authority:

I – warning, with indication of a term for adoption of corrective measures;

II – simple fine of up to two percent (2%) of the sales revenue of the legal entity of private law, group or conglomerate in Brazil in its last fiscal year, excluding taxes, limited, in the aggregate, to fifty million Reais (R$50,000,000.00) per infraction;

III – daily fine, with due regard for the total limit referred to in item II;

IV – disclosure of the infraction after it has been duly investigated and its occurrence has been confirmed;

V – blockage of the personal data to which the infraction relates, until regularization thereof;

VI – elimination of the personal data to which the infraction relates;

~~VII – partial or total suspension of the operation of the database to which the infraction relates for a maximum period of six (6) months, which can be extended for an identical term until regularization of the processing activity by the controller;~~

~~VIII – suspension of performance of the personal data processing activity to which the infraction relates, for a maximum term of six (6) months, which can be extended for an identical term;~~

~~IX – partial or total prohibition of the performance of any activities relating to data processing.~~

Paragraph 1 The penalties shall be imposed after an administrative proceeding that provides the chance of broad defense, on a gradual, individual or cumulative basis, in accordance with the peculiarities of the relevant case and considering the following parameters and criteria:

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

II – the good faith of the infractor;

III – the advantage obtained or intended by the infractor;

IV – the infractor economic condition;

V – repeated occurrence;

VI – the level of damage;

VII – cooperation by the infractor;

VIII – repeated and demonstrated adoption of internal mechanisms and procedures that are capable of minimizing the damage, intended for secure and appropriate data processing, in accordance with the provisions in item II of paragraph 2 of article 48 of this Law;

IX – the adoption of good practices and governance policy;

X – the ready adoption of corrective measures; and

XI – the proportionality between the severity of the fault and the penalty intensity.

Paragraph 2 The provisions in this article do not replace the imposition of administrative, civil or criminal penalties defined by the specific law.

Paragraph 3 The provisions in items I, IV, V, VI, VII, VIII and IX of the main provision of this article may be imposed on government entities and bodies, without prejudice to the provisions in Law No. 8.112 of December 11, 1990 (Federal Government Employee Statute), in Law No. 8.429 of June 2, 1992 (Administrative Improbity Law), and in Law No. 12.527 of November 18, 2011 (Access to Information Law).

Paragraph 4 When calculating the amount of the fine referred to in item II of the main provision of this article, the supervisory authority may consider the total sales revenue of the company or group of companies, whenever it does not have the amount of the sales revenue in the business field in which the infraction occurred, as defined by the supervisory authority, or when the amount is presented in an incomplete manner and/or not demonstrated in an unequivocal and suitable manner.

Article 53. The supervisory authority shall define, by means of proper regulations on administrative penalties for infractions to this Law, which shall be the subject-matter of public inquiry, the methodologies that shall guide the calculation of the base amount of the penalties of fine.

Paragraph 1 The methodologies referred to in the main provision of this article shall be previously published, for information of the processing agent, and objectively present the forms and dosimetry for calculation of the base amount of the penalties of fine, which shall contain a detailed justification of all elements thereof, demonstrating compliance with the criteria established in this Law.

Paragraph 2 The regulation of penalties and corresponding methodologies shall establish the circumstances and conditions for adoption of simple or daily fine.

Article 54. The amount of the penalty of daily fine applicable to infractions of this Law shall take into account the severity of the fault and the extension

of the damage or loss caused and be justified by the supervisory authority. Sole paragraph. The notice of imposition of daily fine shall contain at least a description of the obligation imposed, the reasonable term established by the body for compliance therewith, and the amount of the daily fine to be imposed for breach thereof.

~~CHAPTER IX~~

CHAPTER IX

~~THE NATIONAL SUPERVISORY AUTHORITY ("ANPD") AND NATIONAL PERSONAL DATA AND PRIVACY PROTECTION COUNCIL~~

THE NATIONAL DATA PROTECTION AUTHORITY (ANPD) AND THE NATIONAL BOARD OF PERSONAL DATA PROTECTION AND PRIVACY

~~Section I~~

Section I

~~Data Protection Supervisory Authority (ANPD)~~

The National Data Protection Authority (ANPD)

~~Article 55. The National Supervisory Authority ("ANPD") is hereby created as a member of the indirect federal public administration, subject to the special agency regime and related to the Ministry of Justice.~~

~~Paragraph 1 The ANPD shall be governed by the provisions established in Law No. 9.986 of July 18, 2000.~~

~~Paragraph 2 The ANPD shall be composed of the Board of Directors, as the highest body, and by the National Personal Data and Privacy Protection Council, in addition to the specialized units for application of this Law.~~

~~Paragraph 3 The nature of special agency granted to the ANPD is characterized by administrative independence, absence of hierarchical subordination, fixed term of office, and stability of its leaders and financial autonomy.~~

~~Paragraph 4 The ANPD bylaws and organizational structure shall be approved by decree of the President of the Republic.~~

~~Paragraph 5 The Board Of Directors shall be composed of three (3) directors and resolved by a majority.~~

~~Paragraph 6 The term of office of members of the Board of Directors shall be four (4) years.~~

~~Paragraph 7 The terms of office of the first members of the Board of Directors shall be three (3), four (4) and five (5) years, to be established in the appointment decree.~~

~~Paragraph 8 Any former director shall be forbidden from using privileged information obtained in connection with the position held, subject to penalty of committing administrative improbity.~~

Article 55-A. The National Data Protection Authority (ANPD) is created, without increase of expenses, as a body of federal public administration, member of the Presidency of the Republic.

Article 55-B. It is ensured technical autonomy to the ANPD.

Article 55-C. ANPD is composed of:

I - Board of Directors, as the highest body of direction;

II – National Board of Personal Data Protection and Privacy;

III – Internal Affairs Office;

IV – Ombudsman;

V – its own legal advisory body; and

VI – administrative and specialized unities required to the enforcement of this law.

Article 55-D. The Board of Directors of ANPD is composed of five directors, including the Chief Executive Officer.

Paragraph 1 The members of ANPD Board of Directors will be nominated by the President of the Republic and will hold a commission position of the Direction-Group and Superior Advisory – DSA of level 5.

Paragraph 2 The members of the Board of Director will be chosen among Brazilians with unblemished reputation, a high level of education and great reputation in the field of specialty of the position for which they will be nominated for.

Paragraph 3 The members of the Board of Directors shall serve for a four-year term.

Paragraph 4 The first members of the Board of Directors to be nominated shall serve for two, three, four, five and six- year terms, as established in the nomination act.

Paragraph 5 In the case of vacancy of the position during the term of the member of the Board of Directors, the remaining term shall be completed by the successor.

Article 55-E. The members of the Board of Directors shall only lose their positions due to resignation, final and unappealable judicial conviction or dismissal penalty resulting from disciplinary administrative proceeding.

Paragraph 1 According to the lead sentence of this article, the President´s Chief of Staff shall be in charge of initiate the disciplinary administrative proceeding, which will be conducted by a special commission composed of stable federal public servants.

Paragraph 2 The President of the Republic shall determine the preventive work leave, if necessary, and deliver the decision.

Article 55-F. The article 6, Law n. 12.813 of May 16 2013 applies to the members of Board of Directors.

Paragraph Sole The breach of the legal norm in the lead sentence of this article characterizes an act of administrative improbity.

Article 55-G. An act of the President of the Republic shall organize the regimental structure of ANPD.

Paragraph Sole Until the regimental structure of ANPD comes into force, it will receive the technical and administrative support of the Office of the President´s Chief of Staff in order to carry out its activities.

Article 55-H. The commission and the trust positions of ANPD will be relocated from other bodies and entities of federal executive.

Article 55-I. Those in commission and trust positions of ANPD will be indicated by the Board of Directors and nominated or designated by the Chief Executive Officer.

Article 55-J: The NPDA shall:

I – ensure the protection of personal data;

II – enact norms and proceedings on personal data protection;

III – decide, on administrative level, about this law interpretation, its competences and cases in which it is silent;

IV – require information, any time, to controllers and processors of personal data that engage in personal data processing operations;

V- implement simplified mechanisms, including by electronic means, to the register of complains about personal data processing non-compliant with this law;

VI - inspect and sanction in case of data processing non-compliant with law, through administrative proceeding that ensures right to adversary proceedings, full defense and the right to appeal;

VII – report to the appropriate authorities the criminal offenses that come to their knowledge;

VIII – report to the internal affairs bodies the non-compliance of this law by bodies and entities of federal public administration;

IX – disseminate in the society knowledge about legal norms and policy on personal data protection and its security measures;

X – encourage the adoption of standard for services and products that facilitate the control and the protection of personal data by their subjects, considering the specificities of the activities and the size of controllers;

XI – prepare studies about national and international practices on personal data protection and privacy;

XII – promote actions of cooperation with personal data protection authorities from other countries, with international or transnational nature;

XIII – hold public consultations in order to collect suggestions on relevant public interest subject in the areas on the scope of NPDA;

XIV – hold, before issuing resolutions, the hearing of public administration entities or bodies responsible for the specific sectors of economic activity regulation;

XV – coordinate with the public regulatory authorities in order to fulfill their competence in specific sectors of economic and governmental activity bound to regulation; and

XV – draft managing reports on its annual activities.

Paragraph 1 The ANPD, when issuing its rules, shall observe the requirement of minimal intervention, ensured the grounds and the principles in this law and the article 170 of the Constitution.

Paragraph 2 The NPDA and the public bodies and entities responsible for specific sectors of economic and governmental activities shall coordinate its activities, in its respective spheres of action, in order to ensure the fulfillment of its competences with greater efficiency and promote the adequate

functioning of regulated sectors, according to the specific legislation and the processing of personal data, according to this law.

Paragraph 3 The NPDA shall maintain a permanent forum of communication, including through technical cooperation, with bodies and entities of public administration responsible for the regulation of specific sectors of economic and governmental activity, in order to favor the regulatory, inspecting and punitive competences of NPDA.

Paragraph 4 In the exercise of the competences of the lead sentence of this article, the proper authority shall ensure the preservation of business and information secrecy, according to the law, subject to responsibility.

Paragraph 5 The complaints collected as described in the V of the lead sentence of this article could be analyzed in an aggregated manner and the eventual measures arising from it could be adopted standardly.

Article 55-K. The sanctions enforcement established in this law is an exclusive competence of NPDA, whose all the others competences shall prevail above correlated competences of other public bodies or entities of public administration as it regards personal data protection.

Paragraph Sole The NPDA shall coordinate its acts with the National Consumer Defense System of the Ministry of Justice and with other bodies and entities with punitive and normative competences related to the personal data protection subject and will be the central body of interpretation of this law and of the issuing norms and guidelines for its implementation.

~~Article 56. The ANPD shall have the following duties:~~

~~I – guarantee the protection of the personal data, under the law;~~

~~II – ensure compliance with the trade and industrial secrets when considering the protection of personal data and confidentiality of the information when protected by law or where the breach of confidentiality violates the principles established in article 2 of this Law;~~

~~III – prepare guidelines for the National Personal Data and Privacy Protection Policy;~~

~~IV – inspect and impose penalties in case of data processing carried out in violation of the law, by means of an administrative proceeding that guarantees the right to adversary proceeding, broad defense and right of appeal;~~

~~V – respond to petitions of any data subject against the controller;~~

~~VI – promote in the community information on the public rules and policies on personal data protection and security measures;~~

~~VII – conduct studies on national and international personal data and privacy protection practices;~~

~~VIII – encourage the adoption of standards for services and products that enable the control by the data subjects of their personal data, taking into account the specificities of the activities and the size of the parties in charge;~~

~~IX – carry out cooperation actions with personal data protection authorities of other countries, of an international or transnational nature;~~

~~X – provide for the forms of disclosure of the personal data processing operations, with due regard for compliance with trade and industrial secrets;~~

~~XI – request to the entities of the Public Sector carrying out personal data processing, at any time, specific information on the scope and nature of the data and other details on the processing performed, which the possibility of issue of a supplementary technical expert opinion to ensure compliance with this Law;~~

~~XII – prepare annual management reports about its activities;~~

~~XIII – issue regulations and procedures on personal data and privacy protection, and on data protection impact assessment for those cases where the processing poses a high risk to the guarantee of the general principles of personal data protection established in this Law;~~

~~XIV – consult the processing agents and the society in matters of relevant interest, and provide accounts of its activities and planning;~~

~~XV – collect and apply its revenues and disclose its revenues and expenses in details in the management report referred to in item XII of the main provision of this article; and~~

~~XVI – conduct or determine the conduction of audits, within the scope of the inspection activity, about the personal data processing carried out by the processing agents, including the Public Sector.~~

~~Paragraph 1 By imposing administrative conditions to personal data processing by a private processing agent, whether they are limits, charges or subjections, the ANPD shall comply with the requirement of minimum intervention, with guarantee of the fundaments, principles and rights of the data subjects established in article 170 of the Federal Constitution and in this Law.~~

~~Paragraph 2 The regulations and rules enacted by the ANPD shall be necessarily preceded by public inquiry and hearing, and from regulatory impact analyses.~~

~~Article 57. The following are revenues of the ANPD:~~

~~I – the proceeds of execution of its executable tax debt;~~

~~II – the allocations established in the general budget of the Federal Government, any special credits, additional credits, transfers and onlending granted to it;~~

~~III – any donations, legacies, subventions and any other funds assigned to it;~~

~~IV – any amounts obtained from the sale or lease of any assets and real estate properties owned by it;~~

~~V – the amounts obtained from investments of the revenues set forth in this article in the financial market;~~

~~VI – the proceeds of the collection of fees for services provided;~~

~~VII – the funds arising out of contracts, conventions or agreements entered into with national or international public or private entities, organizations or companies;~~

~~VIII – the proceeds of the sale of publications, technical material, data and information, including for purposes of public bidding process. Section II National Personal Data and Privacy Protection Council.~~

~~Article 58. The National Personal Data and Privacy Protection Council shall be composed of twentythree (23) permanent representatives and their alternate members, of the following bodies:~~

~~I – six (6) representatives of the federal Executive Branch;~~

~~II – one (1) representative designated by the Federal Senate;~~

~~III – one (1) representative designated by the Congress;~~

~~IV – one (1) representative designated by the National Justice Council;~~

~~V – one (1) representative designated by the National Council of the Public Prosecutors' Office;~~

~~VI – one (1) representative designated by the Internet Management Committee in Brazil;~~

~~VII – four (4) representatives of the civil society with proven actions in personal data protection;~~

~~VIII – four (4) representatives of a scientific, technological and innovation institution; and~~

~~IX – four (4) representatives of an entity that represents the business sector related to the personal data processing area.~~

~~Paragraph 1 The representatives shall be designated by an act of the President of the Republic, with permission for delegation, and term of office of two (2) years, one (1) reelection permitted.~~

~~Paragraph 2 The participation in the National Personal Data and Privacy Protection Council shall be deemed an activity of relevant public interest and shall not be remunerated.~~

~~Paragraph 3 The representatives referred to in items I to VI of the main provision of this article and their alternate members shall be indicated by the incumbents of the respective bodies and entities.~~

~~Paragraph 4 The representatives referred to in items VII, VIII and IX of the main provision of this article and their alternate members shall be indicated as provided for in the regulations, and shall not be members of the entity referred to in item VI of the main provision of this article.~~

Article 58-A. The National Board of Personal Data Protection and of Privacy shall be composed of twenty-three representatives, full and substitutes, from the following bodies:

I – six from the federal Executive;

II – one from the Federal Senate;

III – um from the House of Representative;

IV – one from the National Council of Justice;

V – one from the National Council of Public Prosecutors;

VI – one from the Brazilian Internet Steering Committee;

VII – four from entities of civil society with proven experience in personal data protection;

VIII – four from scientific, technologic and innovation institutions; and

IX – four from entities representative of business sector related to the field of personal data processing;

Paragraph 1 The representatives shall be designated by the President of the Republic.

Paragraph 2 The representatives referred in I to IV of the lead sentence of this article and its substitutes shall be indicated by the full representative of the respective bodies and entities of public administration.

Paragraph 3 The representatives referred in the VII, VIII and IX of the lead sentence of this article and their substitutes:

I – shall be indicated in as established in regulation;

II – shall have a two-year term with one reappointment allowed;

III – could not be members of the Brazilian Internet Steering Committee.

Paragraph 4 The participation in the National Board of Personal Data Protection and of Privacy shall be considered relevant unpaid public service.

Article 58-B. The National Board of Personal Data Protection and of Privacy shall:

I – provide strategic guidelines to the draft of the National Personal Data Protection and Privacy Policy and for the NDPA procedures;

II – draft annual reports on the evaluation of the performance of National Personal Data Protection and Privacy Policy;

III – suggest measures to be taken to the NDPA;

IV – prepare studies and hold debates and public hearings on personal data protection and privacy; and

V – disseminate knowledge about personal data protection and privacy to the general population.

~~Article 59. It is incumbent upon the National Personal Data and Privacy Protection Council:~~

~~I – to recommend strategic guidelines and provide aids for preparation of the National Personal Data and Privacy Protection Policy and for the actions of the ANPD;~~

~~II – to prepare annual assessment reports of performance of the actions of the National Personal Data and Privacy Protection Policy;~~

~~III – to recommend actions to be carried out by the ANPD;~~

~~IV – to conduct studies and discussions on personal data and privacy protection; and~~

~~V – to disseminate knowledge on personal data and privacy protection to the population in general.~~

CHAPTER X

FINAL AND TRANSITIONAL PROVISIONS

Article 60. Law No. 12.965 of April 23, 2014 (Brazilian Civil Rights Framework for the Internet) shall be hereinafter in effect with the following amendments:

"Article 7 ...

X – definite exclusion of the personal data supplied to a given internet application, at its request, upon expiration of the relationship between the parties, except for the cases of mandatory storage of records provided for by this Law and by the law that provides for personal data protection; ..." (Regulatory Rule)

"Article 16...

II – of personal data that are excessive in relation to the purpose for which consent was given by the data subject thereof, except for the cases provided for by the Law that provides for personal data protection." (Regulatory Rule)

Article 61. The foreign company shall be notified of and summoned in relation to all procedural acts established in this Law, regardless of power of attorney or contractual or statutory provision, by means of its agent or

representative or person in charge of its branch, agency, subsidiary, establishment or office installed in Brazil.

Article 62. The supervisory authority and Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), as part of its duties, shall enact specific regulations for access to data treated by the Federal Government for compliance with the provisions in paragraph 2 of article 9 of Law No. 9.394 of December 20, 1996 (National Education Bases and Guidelines Law), and the provisions relating to the National Higher Education Evaluation System (Sinaes) referred to by Law No. 10.861 of April 14, 2004.

Article 63. The supervisory authority shall establish rules for progressive adequacy of databases created by the date of effectiveness of this Law, considering the complexity of the processing operations and the data nature.

Article 64. The rights and principles expressed in this Law do not exclude any other rights and principles established in the Brazilian legal system concerning the matter or in the international treaties to which the Federative Republic of Brazil is a party.

~~**Article 65.** This Law comes into force after eighteen (18) months as from its official publication.~~

Article 65. This law comes into force:

I – as for the articles 55-A, article 55-B, article 55-C, article 55-D, article 55-E, article 55-F, article 55-G, article 55-H, article 55-I, article 55-J, article 55-K, article 58-A and article 58-B on December 28 2018; and

II – twenty-four months following the date of its publication regarding the other articles.

Brasília, August 14, 2018. Officially Published, August 15, 2018.