The Brazilian General Data Protection Law (LGPD)

Unofficial English Version

Translated by
Luca Belli, Laila Lorenzon, Luã Fergus and Walter Britto

January 2020

THE BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD)

INTRODUCTION TO LGPD AND UNOFFICIAL TRANSLATION

BY LUCA BELLI, LAILA LORENZON, LUÃ FERGUS AND WALTER BRITTO

CYBERBRICS PROJECT AT FGV LAW SCHOOL

Key Points

The Brazilian General Data Protection Law or "*Lei Geral de Proteção de Dados Pessoais*" ("LGPD") was approved by the National Congress in August 2018 and amended by Law 13.853 of 2019. It will enter into force on 14 August 2020 and aims at generally regulating the processing of personal data of all individuals in Brazil.

Principles

- Purpose limitation
- Adequacy
- Necessity
- Free access
- Data quality
- Transparency
- Security
- Non-discrimination
- Prevention
- Accountability

Personal Data

Personal data are defined as any information related to an identified or identifiable natural person.

Data Processing

Personal data processing is any procedure that involves the use of data, such as the collection, classification, processing, storage, sharing, transfer or elimination of personal data.

Scope

The LGPD will apply to all natural persons or legal entities incorporated or doing business in Brazil that collect personal data about data subjects located in the country. They will have to comply with the new law, as long as:

- The processing operation is carried out in Brazil;
- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil;
- The personal data was collected in Brazil.

The law will not apply to data processing:

- Carried out by a natural person exclusively for private and non-economic purposes;
- Performed for journalistic, artistic or academic purposes;
- Carried out for purposes of public safety, national security and defense or activities of investigation and prosecution of criminal offenses (which will be regulated by specific legislation);
- Originated outside the Brazilian 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, as long as the country of origin offers a level of personal data protection adequate to that established by LGPD.

Sanctions

Sanctions for lack of compliance range from a simple warning to bans on data processing and fines that may amount to 2% of the annual incomeof the entity that processes data with 50 million Brazilian Real (approximately USD 12.5 million). This is the complete list of administrative sanctions set out in the LGPD:

- Warning;
- Simple or daily fines;
- Disclosure of the infraction;
- Blockage or elimination of the personal data to which the infraction relates
- Suspension and partial or total prohibition of the performance of activities relating to data processing.

Rights of the Data Subject

Article 18 LGPD establishes the following rights:

- confirmation of the existence of any processing;
- access to data subject's personal data held by a data controller;
- correction of incomplete, inaccurate or outdated data;
- anonymization, blocking or elimination of unnecessary or excessive data, or those data treated in violation of the provisions of this law;
- data portability to another service or product provider, upon express request, in accordance with the national authority regulations, observing commercial and industrial secrets;
- elimination of personal data processed with the consent of the data subject, except in the cases provided for in Article 16 of the law;
- information of any public and private entities with which the controller has made shared use of data;
- information on the possibility of not providing consent and on the consequences of refusal;
- withdrawal of consent, pursuant to paragraph 5 of Article 8 of the law.

Other rights are also granted to data subjects in other parts of the law, such as the following:

Article 9 establishes that data subjects are entitled to facilitated access to the information on the processing of their data, which shall be clearly, adequately and visibly provided.

Article 20, LGPD establishes that data subjects are entitled to request a review, by a natural person, of decisions made solely based on automated personal data processing.

Enforcement

On May 2019, the Brazilian Congress approved the creation of a new National Data Protection Authority called "*Autoridade Nacional de Proteção de Dados*" (ANPD), an entity that is subordinate to the Presidency of the Republic. The ANPD will be responsible for the enforcement and specification of the LGPD. It has been structured as a branch of the Presidency, bringing up doubts about its independency. In up to two years after LGPD comes into force, however, it may be converted into an independent body akin to a regulatory agency (art. 5-A 1st and 2nd).

LAW 13,709/2018 GENERAL DATA PROTECTION LAW (LGPD or "*Lei Geral de Proteção de Dados Pessoais*") as amended by Law 13,853 of 2019.

UNOFFICIAL TRANSLATION

BY LUCA BELLI, LAILA LORENZON AND LUÃ FERGUS

CYBERBRICS PROJECT *AT FGV LAW SCHOOL*

THE NATIONAL CONGRESS APPROVES AND THE PRESIDENT OF THE REPUBLIC SIGNS THE FOLLOWING LAW:

CHAPTER I

PRELIMINARY PROVISIONS

Article 1 This Law regulates the processing of personal data, including by digital means, by any natural person or legal entity governed by public or private law, with the aim of protecting the fundamental rights to freedom and privacy and the free development of the personality of individuals.

Single paragraph. The general rules contained in this Law are of national interest and must be observed by the Union, the States, the Federal District and the Municipalities.

Article 2 The regulation of personal data protection is grounded on:

I. respect for privacy;
II. informational 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 enterprise, 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, regardless of the means, of the country in which its headquarter is located or of the country in which the data are located, provided that:

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; 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 andnon-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;

III. made exclusively for the following purposes:

c) public security;

d) national defense;

e) safety of the Country; or

f) 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 a country other 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 due process of law, 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 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 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, except for that which has capital entirely owned by the public power.

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

I. personal data: information related to an identified or identifiable 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 a data subject who cannot be identified, considering the use of reasonable technical measures available at the time of its processing;

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 processed refers;

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 processes personal data in the name of the controller;

VIII. data protection officer[1]: natural person appointed by the controller, who acts as a channel of communication between the controller and the data subjects and the supervisory authority, Autoridade Nacional de Proteção de Dados (ANPD);

IX. processing agents: the controller and the processor;

X. processing[2]: 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 subject agrees 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, regardless 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

[1]The literal translationoftheterm in Portuguese "Encarregado" wouldbe "person in charge". However, as the role of "Encarregado" isanalogous, albeitnotentirelyequal, tothe "Data Protection Officer", wehavedecidedto use thelatter for thesakeoffacilitatingcomprehension.

[2]Thistermcanbeunderstand as a translationoranalogyoftheterm "treatment".

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 activities that could generate risks to civil liberties and to 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 headquarters in Brazil, that includes basic or applied research of a historical, scientific, technological or statistical character in its institutional mission or bylaws;

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

Article 6 The personal data processing activities shall observe fairness 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. necessity: limitation of the processing to the minimum required for the intended 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 that the data is up to date, 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 personal data from unauthorized access and from accidental or unlawful situations of destruction, 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. responsibility and accountability: proof, by the agent, of adoption of effective measures able to proveobservance 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 Personal data can only be processed in the following events:

I. with 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 pursuant to 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 9.307, of September 23, 1996 (Arbitration Law);

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

VIII. for the protection of health, exclusively, in a procedure performed by health professionals, health services or health authorities;

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 (Repealed)

Paragraph 2 (Repealed)

Paragraph 3 The processing of publicly accessible personal data the access to which is public shall consider the purpose, fairness and justified its publication.

Paragraph 4 The requirement of consent set forth in the head provision[3] of this article is waived for data manifestly made public by the data subject, 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 where consent is waived according to 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.

Paragraph 7 The subsequent processing of personal data referred to in Paragraph 3 and 4 of this article may be carried out for new purposes, provided that the legitimate and specific purposes for the new treatment and the preservation of the rights of the data subject are observed, as well as the grounds and principles foreseen in this Law.

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 Consent shall refer to defined purposes, and generic authorizations

[3] Actually, the requirement is set forth in the item I of the Article 7.

for the processing of personal data shall be null.

Paragraph 5Consent 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 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 its 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 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 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, based on concrete 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 andliberties, pursuant to the provisions of this Law.

Paragraph 1 Whenever 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 business and industrial secrets.

Section II

Processing of Sensitive Personal Data

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

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

II. without 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 laws or regulations;
c) conducting studies by research bodies, guaranteeing, whenever possible, anonymization of 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 9.307, of September 23, 1996 (Arbitration Law);
e) protection of the life or physical safety of the data subjects or of third parties;
f) health protection, exclusively, in a procedure performed by health professionals, health services or health authorities; or
g) guarantee of the prevention of fraud and of the security of 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 event of application of the provisions of letters “a” and “b” of item II of the head provision of this article by 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 orshared 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 Communication or shared use between health-related personal data controllers is prohibited for the purpose of obtaining economic advantage, except in the case of the provision of health services, pharmaceutical and health care, provided paragraph 5 of this article, including ancillary diagnostic and therapy services, for the benefit of the data subjects' interests and to enable:

I. - data portability when requested by the data subject; or

II. - the financial and administrative transactions resulting from the use and provision of the services referred to in this paragraph.

Paragraph 5 The operators of private health care plans are forbidden to process health data for the practice of risk selection in hiring of any kind, as well as in hiring and excluding beneficiaries.

Article 12. Anonymized data shall not be deemed personal data for the purposes of this Law, except when the anonymization process to which they have been submitted is reversed using solely the one's own efforts, 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 one's own means.

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

Paragraph 3 The supervisory authority may determine 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, research bodies may have access to personal databases, which shall be exclusively processed within those bodies and for the sole purpose of conducting 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, including, whenever possible, the anonymization or pseudonymization of the data, and considering 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 Access to the data set forth in this article shall be regulated by the supervisory authority and by health and sanitary authorities, within the scope of their duties.

Paragraph 4 For the effects of this article, pseudonymization is the processing by means of which 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 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 Information on the processing of data referred to in this article shall be provided in aclear, 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 by the data subject, including in the exercise of their right to revoke the consent as set forth in paragraph 5 of article 8 of this Law, observing public interest; or
IV. – byorder of the supervisory authority, in the event of breach of the provisions of this Law.

Article 16. 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, provided 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 data to another service or product provider upon express request, in accordance with national authority regulations, regarding commercial and industrial secrets;

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 denial;

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

Paragraph 1 The data subject 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 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, except in cases where such communication is proven impossible or involves disproportionate effort..

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

Paragraph 8 The right to which paragraph 1 of this article 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 Personal data shall be stored in a format that favors 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;

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 provide distinct provisions provide on the terms set forth in items I and II of the head provision of this article for the specific sectors.

Article 20. Data subjects are entitled to request a review, 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.

Paragraph 1 The controller shall provide, upon request, clear and adequate information on the criteria and procedures used for the automatized decision, observing 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 business and industrial secrets, the supervisory authority may conduct an audit to confirm discriminatory aspects in the automatized processing of personal data.

Paragraph 3 (Vetoed)

Article 21. 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, regarding 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 12.527, of November 18, 2011 (Access to Information Law) 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. – they inform the grounds on which, in accordance with their legal attributions, they process personal data, 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. (Vetoed)

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; and

IV. (Vetoed)

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 12.527, of November 18, 2011 (Access to Information Law).

Paragraph 3 The terms and procedures to exercise the data subjects' rights before the Government shall observe the provisions of specific law, especially the provisions of Law 9.507, of November 12, 1997 (*Habeas Data* Law*),* of Law 9.784, of January 29, 1999 (General Law on Administrative Proceedings), and of Law 12.527, of November 18, 2011 (Access to Information Law).

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 areoperationalizing 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 access to 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 12.527, of November 18, 2011 (Access to Information Law);

II. (Vetoed)

III. – whenever the data are publicly accessible, subject to the provisions of this Law.

IV. – when there is a legal provision or the transfer is based on contracts, conventions or similar instruments; or

V. – in the event that the transfer of data is solely intended to prevent fraud and irregularities, or to protect and safeguard the security and integrity of the data subject, provided that processing for other purposes is prohibited.

VI. (Vetoed)

Paragraph 2 The contracts and agreements set forth in Paragraph 1 of this article shall be informed to the supervisory authority.

Article 27. The communication or shared use of personal data of legal entities governed by public law to legal entities governed by private law will be informed to the national supervisory authority and will depend on the consent of the data subjects, 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.

Single paragraph: Information to the national authority referred to in the head of this article shall be regulated.

Article 28. (Vetoed)

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

Section II

Responsibilities

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 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 head 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 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 head 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 nature of the data;
III. –compliance with the general principles of protection of personal data and rights of the data subjects established in this Law;
IV. –adoption of security measures provided for by regulations;
V. –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 head provision of article 33 of this Law shall be carried out by the supervisory authority.

Paragraph 1 For verification of the provisions in the head of this article, the minimum requirements, conditions and 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 head 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, 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 head 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 head provision of this article, the report shall contain at least a description of the types of data collected, the methodology used for collection and security measures adopted, 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 andobjectively 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 data subjects, provide clarifications and take appropriate measures;
II. – to receive communications from the supervisory authority and take appropriate measures;
III. – to instruct the employees and contractors of the entity on the practices to be adopted in relation to 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.

Paragraph 4 (Vetoed)

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 and severally 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 and severally 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, the data subject is unable to produce evidences, or the production of evidence by the data subject would be exclusively burdensome for such data subject.

Paragraph 3 Actions for indemnification of collective damages as provided for in the head 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 consumes 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 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 head of this article applicable, considering the nature of the treated information, the specific characteristics of the processing, and the current state of technology, especially in case of sensitive personal data, as well as the principles established in the head provision of article 6 of this Law.

Paragraph 2 The measures referred to in the head of this article shall be complied with from the product or service design phase to its implementation.

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 personal data, including after its termination.

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 safeguarding 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 severity of the incident, it shall be assessed whether appropriate technical measures were adopted to make the affected personal data unintelligible, within the scope andthe 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, 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 produce good practices and governance rules that provide for organizational factors, working practices, 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 head 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 broadcompliance with rules and good practices concerning personal data protection;
   b) be applicable to any set of personal data under its control, regardless of how it was collected;
   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) intend 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. - (Vetoed);

VIII. - (Vetoed);

IX. - (Vetoed);

X. - partial suspension of the operation of the database to which the infringement refers for a maximum period of six (6) months, extendable for an equal period, until the controller has regularized its processing activity;

XI. - suspension of the exercise of the activity of processing personal data to which the infringement refers for a maximum period of six (6) months, extendable for the same period;

XII. partial or total ban on data processing activities.

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'seconomic condition;
V. –recidivism;
VI. – thelevel 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 immediate adoption of corrective measures; and
XI. – the proportionality between the severity of the fault and the intensity of the penalty.

Paragraph 2The provisions of this article do not replace the application of administrative, civil or criminal sanctions defined in Law 8.078 of September 11, 1990, and in specific legislation.

Paragraph 3 The provisions of items I, IV, V, VI, X, XI and XII of the head of this article may be applied to public entities and public bodies, without prejudice to the provisions of Law 8.112, of December 11, 1990, Law 8.429, of June 2, 1992, and in Law 12.527, of November 18, 2011.

Paragraph 4 When calculating the amount of the fine referred to in item II of the head 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.

Paragraph 5 The financial gains from the collection of fines imposed by the ANPD,

whether posted or not in the Federal Debt Roster, will be destined to the Diffuse Rights Defense Fund dealt with in art. 13 of Law 7.347 of July 24, 1985, and Law 9.008 of March 21, 1995.

Paragraph 6 The sanctions provided for in items X, XI and XII of the head of this article shall apply:

I. only after at least one (1) of the sanctions referred to in items II, III, IV, V and VI of the head of this article have already been imposed for the same specific case; and

II. in the case of controllers subordinated to other organs and entities with sanctioning powers, after hearing these organs.

Paragraph 7 The individual leaks or unauthorized access referred to in the head of art. 46 of this Law may be subject to direct conciliation between controller and data subject and, if there is no agreement, the controller shall be subject to the application of the penalties referred to in this article.

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 head provision of this article shall be previously published, for information of the processing agents, and objectively present the forms and dosimetry for calculation of the base amount of fines, 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 fines.

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

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

Section I

Data Protection Supervisory Authority (ANPD)

Article 55. (Vetoed)

Article 55-A. It is hereby created without any increase in expenses, The National Data Protection Authority (ANPD), a federal public administration body that is a member of the Presidency of the Republic. (Included by Law. 13.853 of 2019)

Paragraph 1 The legal nature of the ANPD is transitory and may be transformed by the Executive Power into an entity of indirect federal public administration, subject to special autarchic regime and linked to the Presidency of the Republic.

Paragraph 2 The assessment regarding the transformation provided for in paragraph 1 of this article shall occur within two (2) years from the date of entry into force of the ANPD's regimental structure.

Paragraph 3 The provision of positions and functions necessary for the establishment and performance of the ANPD is subject to express physical and financial authorization in the annual budget law and permission in the budget guidelines law.

Article 55-B. Technical and decision-making autonomy is assured to the ANPD.

Art. 55-C. The ANPD is composed of:

I. - Directing Council, highest governing body;
II. - National Council for the Protection of Personal Data and Privacy;
III. - Internal Affairs Audit;
IV. - Ombudsman;
V. - legal advisory body; and
VI. - administrative units and specialized units necessary for the application of

the provisions of this Law.

Art. 55-D. The ANPD Board of Directors will be composed of 5 (five) directors, including the Chief Executive Officer.

Paragraph 1 The members of ANPD's Board of Directors will be chosen by the President of the Republic and appointed by him, after approval by the Federal Senate, under the terms of sub-paragraph f) of item III of art. 52 of the Federal Constitution, and will occupy a position on the committee of the Superior Steering and Advisory Group - DAS, at least level 5.

Paragraph 2 The members of the Board of Directors will be chosen from Brazilians who have an unblemished reputation, a superior level of education and a high level of expertise in the field of specialty of the positions to which they will be appointed.

Paragraph 3 The term of office of the members of the Board of Directors shall be four (4) years.

Paragraph 4 The terms of office of the first members of the Board of Directors chosen shall be 2 (two), 3 (three), 4 (four), 5 (five) and 6 (six) years, as set forth in the appointment.

Paragraph 5 In the event of vacancy in office during the term of office of a member of the Board of Directors, the remaining term shall be completed by the successor.

Art. 55-E. The members of the Board of Directors will only lose their positions as a result of resignation, final court conviction or penalty of dismissal arising from disciplinary administrative proceedings.

Paragraph 1 Pursuant to the head of this article, it is incumbent upon the Minister of State Chief of Staff of the Presidency of the Republic to institute disciplinary administrative proceedings, which shall be conducted by a special commission composed of stable federal public servants.

Paragraph 2 It is for the President of the Republic to determine the preventive

removal, only when so recommended by the special commission referred to in paragraph 1 of this article, and to render the judgment.

Art. 55-F. The provisions of art. 6 of Law 12.813, of May 16, 2013 are applicable to the members of the Board of Directors, after the exercise of the position.

Single paragraph Infringement of the head of this article characterizes an act of administrative misconduct.

Art. 55-G. An Act of the President of the Republic shall provide for ANPD's regimental structure.

Paragraph 1 Until the date of entry into force of its regimental structure, ANPD will receive technical and administrative support from the Civil House of the Presidency of the Republic for the exercise of its activities.

Paragraph 2 The Directing Council shall provide for the internal statute of the ANPD.

Art. 55-H. Commission positions and ANPD's trust functions will be relocated from other organs and entities of the federal executive branch.

Art. 55-I. The occupants of ANPD's commission positions and trust functions shall be appointed by the Board of Directors and appointed or designated by the Chief Executive Officer.

Art. 55-J. It is up to the ANPD:

I. –to ensure the protection of personal data, in accordance with the law;
II. –toensure the observance of commercial and industrial secrets, observing the protection of personal data and confidentiality of information when protected by law or when breach of confidentiality violates the fundaments of art. 2 of this Law;
III. –to develop guidelines for the National Policy on Personal Data Protection and Privacy;
IV. –to supervise and enforce sanctions in case of data processing carried out in breach of the law, through an administrative process that ensures due

process, broad defense and the right of appeal;

V. –to consider petitions from data subjectsagainst controllers after the data subject has substantiated a complaint to the controller that is not resolved within the time limit established in the regulation;

VI. –to promote among the population the knowledge of the norms and the public politics on protection of personal data and the security measures;

VII. –to promote and elaborate studies on national and international practices of personal data protection and privacy;

VIII. –to encourage the adoption of standards for services and products that facilitate the exercise of control of the data subjects over their personal data, which should take into account the specificities of the activities and the size of those responsible;

IX. –to promote cooperation actions with personal data protection authorities of other countries, of an international or transnational nature;

X. –to provide for the forms of advertising of personal data processing operations, respecting commercial and industrial secrets;

XI. –to request, at any time, the public authorities to carry out personal data processing operations to provide specific information on the scope, nature of the data and other details of the processing performed, with the possibility of issuing a complementary technical opinion to ensure the compliance with this law;

XII. –to prepare annual management reports on its activities;

XIII. - to edit regulations and procedures on protection of personal data and privacy, as well as on reports of impact to the protection of personal data for cases where the treatment represents high risk to the guarantee of the general principles of protection of personal data foreseen in this Law;

XIV. –to listen to treatment agents and society on matters of relevant interest and report on their activities and planning;

XV. –to collect and apply its income and publish, in the management report referred to in item XII of the head of this article, a breakdown of its income and expenses;

XVI. –to perform audits, or determine their performance, within the scope of the inspection activity dealt with in item IV and with due observance of the

provisions of item II of the head of this article, on the processing of personal data by the processing agents, including the public power;

XVII. –to enter into, at any time, a commitment to treatment agents to eliminate irregularity, legal uncertainty or contentious situation in the context of administrative proceedings, in accordance with Decree-Law 4.657 of September 4, 1942;

XVIII. - edit simplified and differentiated rules, guidelines and procedures, including deadlines, so that micro and small businesses, as well as incremental or disruptive business initiatives that call themselves startups or innovation companies, can adapt to this Law;

XIX. –to ensure that the data processing of the elderly is carried out in a simple, clear, accessible and appropriate way to their understanding, pursuant to this Law and Law 10.741, of October 1, 2003 (Statute of the Elderly);

XX. –to decide, at the administrative level, on a terminative basis, on the interpretation of this Law, its powers and omitted cases;

XXI. –to report to the competent authorities the criminal offenses of which it is aware;

XXII. –to report to the internal control organs non-compliance with the provisions of this Law by federal public administration agencies and entities;

XXIII. –to articulate with public regulatory authorities to exercise their powers in specific sectors of economic and governmental activities subject to regulation; and

XXIV. –toimplement simplified mechanisms, including by electronic means, for the registration of complaints about the processing of personal data in breach of this Law.

Paragraph 1 When imposing administrative constraints on the processing of personal data by private processing agents, whether limits, charges or obligations, the ANPD must comply with the requirement of minimum intervention, ensuring the grounds, principles and rights of the data subjects provided for in art. 170 of the Federal Constitution and this Law.

Paragraph 2 Regulations and standards issued by the ANPD should be preceded

by public consultation and hearing, as well as regulatory impact analysis.

Paragraph 3 The ANPD and the public bodies and entities responsible for the regulation of specific sectors of economic and governmental activity shall coordinate their activities, in the corresponding spheres of activity, in order to ensure the fulfillment of their duties with the greatest efficiency and to promote the proper functioning of regulated sectors, according to specific legislation, and the processing of personal data, pursuant to this Law.

Paragraph 4 The ANPD shall maintain a permanent communication forum, including through technical cooperation, with public administration bodies and entities responsible for the regulation of specific sectors of economic and governmental activity, in order to facilitate the ANPD's regulatory, supervisory and punitive powers.

Paragraph 5 In exercising the powers referred to in the main section of this article, the competent authority shall ensure the preservation of business secrecy and confidentiality of information, in accordance with the Law.

Paragraph 6 Complaints collected in accordance with the provisions of section V of the head of this article may be analyzed in aggregate form, and any measures resulting from them may be adopted in a standardized manner.

Art. 55-K. The application of the sanctions provided for in this Law rests exclusively with the ANPD, and its powers shall prevail, regarding the protection of personal data, over the related competences of other public administration entities or bodies.

Single paragraph The ANPD will articulate its activities with other bodies and entities with sanctioning and normative competences related to the subject of personal data protection and will be the central body for the interpretation of this Law and the establishment of rules and guidelines for its implementation.

Art. 55-L. ANPD's revenues are:

I. - the allocations, set out in the general budget of the Union, special credits, additional credits, transfers and onlendings granted to it;

II. - donations, legacies, grants and other resources intended for it;

III. - the amounts determined on the sale or rental of movable and immovable property owned by it;

IV. - the amounts calculated on investments in the financial market of the revenues provided for in this article;

V. - (Vetoed);

VI. - resources arising from agreements, arrangements or contracts concluded with public or private entities, organizations or companies, national or international;

VII. - the proceeds from the sale of publications, technical material, data and information, including for public bidding purposes.

Article 56. (Vetoed)

Article 57. (Vetoed)

Section II

National Personal Data and Privacy Protection Council

Article 58. (Vetoed)

Art. 58-A. The National Council for the Protection of Personal Data and Privacy will be composed of 23 (twenty-three) representatives, full and alternates, from the following bodies:

I. - 5 (five) from the Federal Executive Branch;

II. - 1 (one) from the Federal Senate;

III. - 1 (one) from the Chamber of Deputies;

IV. - 1 (one) fromthe National Council of Justice;

V. - 1 (one) from the National Council of the Public Prosecution Service;

VI. - 1 (one) from the Brazilian Internet Steering Committee;

VII. - 3 (three) from civil society entities related to the protection of personal data;

VIII. - 3 (three) fromscientific, technological and innovation institutions;

IX. - 3 (three) from trade union confederations representing the economic categories of the productive sector;

X. - 2 (two) from entities representing the business sector related to the area of personal data processing; and

XI. - 2 (two) fromentities representing the labor sector.

Paragraph 1 Representatives shall be appointed by act of the President of the Republic, with delegation permitted.

Paragraph 2 The representatives referred to in items I, II, III, IV, V and VI of the main section of this article and their alternates shall be appointed by the full members of the respective organs and entities of the public administration.

Paragraph 3 The representatives referred to in items VII, VIII, IX, X and XI of the head of this article and their alternates:

I. - will be indicated in the form of a regulation;

II. - may not be members of the Internet Steering Committee in Brazil;

III. - will have a term of office of 2 (two) years, with 1 (one) renewal allowed.

Paragraph 4 Participation in the National Council for the Protection of Personal Data and Privacy shall be considered as relevant, unpaid public service provision.

Art. 58-B. The National Council for the Protection of Personal Data and Privacy is responsible for:

I. - proposing strategic guidelines and providing subsidies for the elaboration of the National Policy of Personal Data Protection and Privacy and for ANPD's performance;

II. - preparing annual reports evaluating the execution of the actions of the National Policy for the Protection of Personal Data and Privacy;

III. - suggesting actions to be performed by the ANPD;

IV. - preparing studies and holding public debates and hearings on the protection of personal data and privacy; and

V. - disseminating knowledge about the protection of personal data and privacy to the population.

Art. 59. (Vetoed).

CHAPTER X

FINAL AND TRANSITIONAL PROVISIONS

Article 60. Law 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 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 PesquisasEducacionaisAnísio 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 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 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 nature of the

data.

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:

I. On the 28th December 2018 for articles 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A and 58-B; and

II. 24 (twenty-four) months after its publication date, as for the other articles.

Brasília, August 14, 2018.

Officially Published, August 15, 2018.