

# Brazilian Data Protection Law LGPD

LAW No. 13,709 OF AUGUST 14, 2018



O texto traduzido da Lei Geral de Proteção de Dados (LGPD) para o inglês representa uma primeira versão destinada a facilitar a consulta e utilização pela comunidade que utiliza essa legislação. Ressaltamos que a tradução pode passar por revisões e aprimoramentos futuros. Estamos abertos a sugestões que possam contribuir para a melhoria e maior precisão deste documento. As sugestões podem ser enviadas para a Ouvidoria da ANPD por meio da Plataforma Fala.BR (<https://falabr.cgu.gov.br/>).

## **LAW No. 13,709 OF AUGUST 14, 2018**

Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019)

**The President of the Republic** I hereby make known that the National Congress decrees and I sanction the following Law:

### **CHAPTER I**

#### **PRELIMINARY PROVISIONS**

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

Sole paragraph. The general provisions of this Law are of national interest and must be observed by the Federal Union, States, Federal District and Municipalities. (Included by Law No. 13,853/2019)

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

- 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 natural persons.

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

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

II – the processing activity is aimed at offering or supplying goods or services, or the processing of data of individuals located in the national territory; or (New wording given by Law No. 13,853/2019)

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

Paragraph 1. Personal data is considered to be collected in the national territory when the data subject is in that territory at the time of collection.

Paragraph 2. The processing of data provided for in item IV of the head provision of article 4 of this Law is excepted from the provisions of item I of this article.

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

I – is carried out by a natural person purely for private and non-economic purposes;

II – is carried out exclusively for:

a) journalistic and artistic purposes; or

b) academic purposes, this event being subject to articles 7 and 11 of this Law;

III – is carried out exclusively for purposes of:

a) public security;

b) national defense;

c) State security; or

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

IV– have their origin outside the national territory and are not the object of communication, shared use of data with Brazilian processing agents or the object of international transfer of data with a third country other than the country of origin, provided that the country of origin offers a level of personal data protection consistent with the provisions of this Law.

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

Paragraph 2. Processing of the data referred to in item III of the head provision of this article is forbidden for legal entities of private law, except in procedures under the authority of a legal entity of public law, which shall be subject to specific reporting to the national authority and observe the limitation imposed in paragraph 4 of this article.

Paragraph 3. The national authority shall issue technical opinions or recommendations regarding the exceptions set forth in item III of the head provision of this article and shall request data protection impact assessments from those responsible for data processing.

Paragraph 4. Under no circumstances the entirety of personal data contained in a database, as provided for in item III of the head provision of this article, may be processed by a

legal entity of private law, unless its capital is integrally held by a government authority. (New wording given by Law No. 13,853/2019)

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

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

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

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

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

V – data subject: natural person to whom the personal data that is object of the processing refers to;

VI – controller: natural person or legal entity of either public or private law in charge of making the decisions regarding the processing of personal data;

VII – processor: natural person or legal entity of either public or private law that processes personal data on behalf of the controller;

VIII – data protection officer: person appointed by the controller and processor to act as a communication channel between the controller, the data subjects and the National Data Protection Authority (ANPD); (New wording given by Law No. 13,853/2019)

IX – processing agents: the controller and the processor;

X – processing: any operation performed on personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, erasure, information evaluation or control, modification, communication, transfer, dissemination or retrieval;

XI – anonymization: use of reasonable technical means available at the time of processing, by which a given data loses the possibility of direct or indirect association with an individual;

XII – consent: freely, informed and unambiguous manifestation whereby the data subject agrees to the processing of their personal data for a given purpose;

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

XIV – erasure: removal of data or a set of data stored in a database, regardless of the procedure used;



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

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

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

XVIII - research body: body or entity from the direct or indirect administration or non-profit legal entity of private law, legally organized under Brazilian laws, with headquarters and jurisdiction in the country, which includes basic or applied research of historical, scientific, technological or statistical nature in its institutional mission or in its corporate or statutory purposes; and (New wording given by Law No. 13,853/2019)

XIX - national authority: body of the public administration responsible for ensuring, implementing and supervising the compliance with this Law in all national territory. (New wording given by Law No. 13,853/2019).

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

I - purpose: processing for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with such 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 accomplishment of its purposes, encompassing relevant, proportional and non-excessive data in relation to data processing purposes;

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

V – data quality: guarantee to the data subjects of accuracy, clarity, relevance and updating of data, according to the necessity and for achieving the purpose of the processing;

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

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

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

IX – non-discrimination: impossibility of carrying out the processing for unlawful or abusive discriminatory purposes;

X – liability and accountability: proof, by the agent, of the adoption of effective measures capable of demonstrating observance of and compliance with personal data protection rules, including the effectiveness of such measures.

## **CHAPTER II**

### **PROCESSING OF PERSONAL DATA**

#### **Section I**

##### **Requirements for the Processing of Personal Data**

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

I – with the consent of the data subject;

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

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

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

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

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

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

VIII – for protection of health, exclusively, in procedures carried out by health professionals, health services or sanitary authorities; (New wording given by Law No. 13,853/2019)

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

X – for the protection of credit, including the provisions in relevant legislation.

Paragraph 1. (Repealed). (New wording given by Law No. 13,853/2019)

Paragraph 2. (Repealed). (New wording given by Law No. 13,853/2019)

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

Paragraph 4. The consent requirement set forth in the head provision of this article shall not apply to data manifestly made public by the data subject, safeguarding the rights of the data subject and the principles set forth in this Law.

Paragraph 5. The controller who 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 shall obtain specific consent of the data subject for such purpose, except when the need for such consent is waived as provided for in this Law.

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

Paragraph 7. The subsequent processing of personal data referred to in paragraphs 3 and 4 of this article may be carried out for new purposes, provided that legitimate and specific purposes for the new processing and the preservation of the rights of the data subject are observed, as well as the grounds and principles set forth in this Law. (Included by Law No. 13,853/2019).

Article 8. The consent set forth in item I of article 7 of this Law shall be given in writing or by other means able to demonstrate the manifestation of intention of the data subject.

Paragraph 1. If consent is given in writing, it shall be included in a clause that stands out from the other contractual clauses.

Paragraph 2. The controller shall bear the burden of proving that the consent has been obtained in accordance with the provisions of this Law.

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

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

Paragraph 5. The consent may be revoked at any time upon express request of the data subject, via a free-of-charge and facilitated procedure, with processing carried out under previously given consent remaining valid as long as there is no request for erasure, pursuant to item VI of the head provision of article 18 of this Law.

Paragraph 6. In the event of alteration in the information referred to in items I, II, III or V of article 9 of this Law, the controller shall inform the data subject, specifically emphasizing the content of such changes, in which case the data subject, when consent is required, may revoke it if they disagree with the change.

Article 9. The data subject is entitled to facilitated access to information concerning the processing of her/his data, which shall be made available in a clear, adequate and visible manner, concerning, among other aspects provided in regulation for complying with the principle of free access:

I – specific purpose of the processing;

II – the type and duration of the processing, complying with trade and industrial secrets;

III – identification of the controller;

IV – contact information of the controller;

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

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

VII – the data subject's rights, explicitly mentioning the rights provided for in Art. 18 of this Law.

Paragraph 1. When consent is required, it shall be considered void if the information provided to the data subject contains misleading or abusive content or has not been previously presented in a transparent, clear and unambiguous way.

Paragraph 2. When consent is required, if there are changes in the purpose of the processing of personal data that are not compatible with the original consent, the controller shall inform the data subject in advance about such changes, and the data subject may revoke the consent in case they disagree with the changes.

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

Article 10. The legitimate interest of the controller may only provide a legal basis for processing personal data for legitimate purposes, based on particular situations, which include but are not limited to:

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

II – protection of data subject’s regular exercise of their rights or provision of services for their benefit, subject to their legitimate expectations and fundamental rights and freedoms, pursuant to the provisions of this Law.

Paragraph 1. When the processing is based on the legitimate interest of the controller, only the personal data strictly necessary for the intended purpose may be processed.

Paragraph 2. The controller shall adopt measures to ensure the transparency of data processing based on their legitimate interest.

Paragraph 3. The national authority may request a data protection impact assessment from the controller, when processing is based on their legitimate interest, complying with trade and industrial secrets.

## **Section II**

### **Processing of Sensitive Personal Data**

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

I – when the data subject or their legal representative specifically and emphatically consents, for specific purposes;

II – without the data subject’s consent, in the events in which it is indispensable for:

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

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

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

d) the regular exercise of rights, including in a contract and in a judicial, administrative or arbitration procedure, the latter pursuant to the provisions laid out in Law No. 9.307, of September 23, 1996 (Arbitration Law);

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

f) protection of health, exclusively, in procedures carried out by health professionals, health services or sanitary authorities; (New wording given by Law No. 13,853/2019)

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

Paragraph 1. The provisions of this article shall apply to any processing of personal data that discloses sensitive personal data and that may cause damage to the data subject, except for situations provided for in specific legislation.

Paragraph 2. When the provisions laid out in subitems "a" and "b" of item II of the head provision of this article are applied by public agencies and entities, such waiver of consent shall be publicized, pursuant to item I of the head provision of Article 23 of this Law.

Paragraph 3. Communication or shared use of sensitive personal data among controllers for the purpose of obtaining an economic advantage may be prohibited or regulated by the national authority, after hearing the sectoral Government entities, within their regulatory capacity.

Paragraph 4. Communication or shared use of sensitive data relating to health among controllers for the purpose of obtaining an economic advantage is prohibited, except in events of provision of health services, pharmaceutical assistance and health insurance, as long as paragraph 5 of this article is observed, including auxiliary diagnostic and therapeutic services, in benefit of the interests of data subject and also to allow: (New wording given by Law No. 13,853/2019)

I - data portability at the data subject's request; or (Included by Law No. 13,853/2019)

II - the financial and administrative transactions resulting from the use and provision of the services referred to in this paragraph. (Included by Law No. 13,853/2019)

Paragraph 5. Private healthcare plan operators are prohibited from processing health data for the purpose of risk selection under any contracting mode, as well as for including and excluding beneficiaries. (Included by Law No. 13,853/2019)

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 exclusively own means, or when it may be reversed applying reasonable efforts.

Paragraph 1. The determination of what is considered reasonable shall take objective factors into account, such as cost and time required to reverse the anonymization process, according to the technologies available, and the exclusive use of own means.

Paragraph 2. For purposes of this Law, data used to formulate a behavioral profile of a particular natural person, if that person is identified, may be also considered personal data.

Paragraph 3. The national authority may provide for standards and techniques to be used in anonymization processes, and carry out security checks, making sure to hear the National Council for Personal Data and Privacy Protection.

Article 13. When carrying out public health studies, research bodies may have access to personal databases, which shall be exclusively processed within the body and for the sole

purpose of carrying out studies and research. Those databases shall be kept in a controlled and secure environment, according to the security practices set forth in the specific regulation and which include, whenever possible, the anonymization or pseudonymization of the data, as well as the proper ethical standards related to studies and research.

Paragraph 1. Under no circumstances shall the disclosure of the results or of any excerpt of the study or the research referred to in the head provision of this article reveal personal data.

Paragraph 2. The research body shall be held liable for the security of the information referred to in the head provision of this article, and it is forbidden, under any circumstances, to transfer said data to third parties.

Paragraph 3. Access to data as provided for in this article shall be regulated by the national authority and by the health and sanitation authorities, within their regulatory capacity.

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

### **Section III**

#### **Processing of Children's and Adolescents' Personal Data**

Article 14. The processing of children's and adolescents' personal data shall be carried out in their best interest, pursuant to the provisions of this article and of relevant legislation.

Paragraph 1. The processing of children's personal data shall be carried out with the specific and distinguishable consent given by at least one of the parents or by the legal representative.

Paragraph 2. In the data processing set forth in paragraph 1 of this article, controllers shall make public the information on the types of collected data, the way they are used and the procedures to exercise the rights referred to in article 18 of this Law.

Paragraph 3. Children's personal data may be collected without the consent referred to in paragraph 1 of this article when the collection is necessary to contact the parents or the legal representative, used only once and without storage, or for their protection, and under no circumstances may such data be transmitted to a third party without consent as provided in paragraph 1 of this article.

Paragraph 4. 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 for providing personal information beyond what it is strictly necessary for the activity.

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

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

## **Section IV**

### **Termination of Data Processing**

Article 15. The processing of personal data shall cease in the following events:

- I – upon evidence that the purpose has been achieved or that the data are no longer necessary or pertinent to attain the intended specific purpose;
- II – upon expiration of the processing period;
- III – upon notice from the data subject, including when exercising the right to revoke the consent as set forth in paragraph 5 of Article 8 of this Law, subject to the public interest; or
- IV – at the order of the national authority, upon violation of the provisions of this Law.

Article 16. Personal data shall be erased following the termination of their processing, within the scope and technical limits of the activities, but their storage is authorized for the following purposes:

- I - compliance with a legal or regulatory obligation by the controller;
- II – study by a research body, ensuring, whenever possible, the anonymization of personal data;
- III - transfer to a third party, upon compliance with the data processing requirements set forth in this Law; or
- IV – exclusive use by the controller, with access by a third party being prohibited, and provided the data has been anonymized.

## **CHAPTER III**

### **DATA SUBJECT'S RIGHTS**

Article 17. Every natural person is assured ownership of their personal data and the guarantee of the fundamental rights of freedom, intimacy and privacy, pursuant to the provisions of this Law.

Article 18. Data subjects shall have the right to obtain from the controller, regarding their data processed by said controller, at any time and upon request:

- I – confirmation of the existence of the processing;
- II – access to the data;
- III – correction of incomplete, inaccurate or outdated data;
- IV - anonymization, blocking or erasure of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law;



V - portability of data to another service provider or product provider, upon express request, according to the regulations of the national authority, complying with trade and industrial secrets; (New wording given by Law No. 13,853/2019)

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

VII – information on government and private entities with which the controller has shared data;

VIII - information on the possibility of denying consent and the consequences of such denial;

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

Paragraph 1. Data subjects have the right to petition, regarding their data, against the controller before the national authority.

Paragraph 2. Data subjects may oppose to the processing based on one of the events of waiver of consent, in case of noncompliance with the provisions of this Law.

Paragraph 3. The rights set forth in this article shall be exercised upon express request by the data subject, or a legally appointed representative, to a processing agent.

Paragraph 4. In case it is impossible to immediately adopt the measure mentioned in paragraph 3 of this article, the controller shall send a reply to the data subject, in which he or she may:

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

II – indicate the reasons *de facto* or *de jure* that prevent the 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 subject, within the time periods and terms provided in regulation.

Paragraph 6. The controller shall immediately communicate the processing agents with whom he or she has shared data about any correction, erasure, anonymization or blocking of data, so that they can repeat an identical procedure, except in cases in which this action is proven impossible or involves disproportionate effort (New wording given by Law No. 13,853/2019)

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

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

Article 19. Confirmation of the existence or access to personal data shall be provided, upon the data subject's request:

I – immediately, in simplified format; or

II - by means of a clear and complete statement, indicating the origin of data, the non-existence of registration, the criteria used and the purpose of the processing, complying with

trade and industrial secrets, provided within fifteen (15) days from the date of the data subject's request.

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

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

I – by electronic means that is safe and suitable for this purpose; or

II – in printed form.

Paragraph 3. When processing originates from the consent of the data subject or from a contract, the data subject may request full electronic copy of their personal data, complying with trade and industrial secrets, pursuant to the regulations of the national authority, in a format that permits their subsequent use, including in other processing operations.

Paragraph 4. The national authority may provide differently regarding the time periods set forth in items I and II of the head provision of this article for the specific sectors.

Article 20. The data subject is entitled to request the review of decisions made solely based on automated processing of personal data that affect his/her interests, including decisions intended to define his/her personal, professional, consumer and credit profile or aspects of his/her personality. (New wording given by Law No. 13,853/2019)

Paragraph 1. The controller shall provide, upon request, clear and adequate information on the criteria and procedures used for an automated decision, complying with trade 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 compliance with trade and industrial secrets, the national authority may carry out an audit to verify discriminatory aspects in the automated processing of personal data.

Paragraph 3. (vetoed). (Included by Law No. 13,853/2019)

Article 21. Personal data concerning the regular exercise of rights by the data subject cannot be used to her/his detriment.

Article 22. The defense of the interests and rights of the data subject may be exercised in court, individually or collectively, in accordance with the provisions in relevant legislation regarding the instruments of individual and collective protection.

## **CHAPTER IV**

### **PROCESSING OF PERSONAL DATA BY GOVERNMENT AUTHORITIES**

#### **Section I**

##### **Rules**

Article 23. Processing of personal data by legal entities of public law mentioned in the sole paragraph of Article 1 of Law No. 12,527, of November 18, 2011 (Access to Information Act) shall be carried out to achieve their public purpose, in benefit of the public interest, with a view to enforcing their legal powers or fulfilling the legal duties of public service, provided that:

I – they inform the events in which they process personal data, while performing their duties, providing clear and updated information on the legal base, purpose, procedures and practices used to perform such activities, in an easily accessible media, preferably on their websites;

II – (vetoed); and

III – a data protection officer is appointed when carrying out personal data processing operations, pursuant to the provisions of Article 39 of this Law; and (New wording given by Law No. 13,853/2019)

IV – (vetoed). (Included by Law No. 13,853/2019)

Paragraph 1. The national authority may provide for the forms of disclosing information on data processing operations.

Paragraph 2. The provisions in this Law shall not exempt the legal entities mentioned in the head provision of this article from establishing the authorities as set forth in Law No. 12,527, of November 18, 2011 (Access to Information Act).

Paragraph 3. The time periods and procedures for exercising data subjects' rights before the government authorities shall observe the provisions laid out in specific laws, especially the provisions in Law No. 9,507, of November 12, 1997 ( Habeas Data Act), in Law No. 9,784, of January 29, 1999 (Administrative Procedure Act), and in Law No. 12,527, of November 18, 2011 (Access to Information Act).

Paragraph 4. Notary and registration services, privately exercised by government delegation, shall have 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. Notarial and registration bodies shall grant access to data by electronic means to the public administration, for the purposes set forth in the head provision of this article.

Article 24. State-owned companies and government-controlled companies operating under a competition system, subject to the provisions in article 173 of the Brazilian Federal Constitution, shall have the same treatment granted to the private legal entities, pursuant to the provisions of this Law.

Sole paragraph. State-owned and government-controlled companies, when implementing public policies and within the scope of their enforcement, shall receive the same treatment given to government bodies and entities, pursuant to the provisions of this Chapter.

Article 25. Data shall be kept in interoperable formats and structured for shared use intended for the enforcement of public policies, provision of public services, decentralization of public activities, dissemination and access to the information by the public in general.

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

Paragraph 1. Government authorities are forbidden to transfer personal data included in databases to which they have access to private entities, except:

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

II – (vetoed);

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

IV – when there is a legal provision or the transfer is grounded on contracts, agreements or similar instruments; or (Included by Law No. 13,853/2019)

V – in the event that the transfer of data is exclusively intended to prevent fraud and irregularities, or to protect and safeguard the data subject's security and integrity, provided that processing is forbidden to be carried out for other purposes. (Included by Law No. 13,853/2019)

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

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

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

II – when there is shared use of data, which shall be made public pursuant to 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.

Sole paragraph. The information to the national authority referred to in the head provision of this article shall be subject to regulation. (Included by Law No. 13,853/2019)

Article 28. (vetoed)

Article 29. The national authority may request, at any time, to government bodies and entities, the conduction of personal data processing operations, specific information on the scope and nature of the data and other details of the processing performed and may issue a supplementary technical report to ensure compliance with this Law. (New wording given by Law No. 13,853/2019)

Article 30. The national authority may establish supplementary rules for communication or shared use of personal data activities.

## **Section II**

### **Liability**

Article 31. In the event of infringement of this Law as a result of the processing of personal data by government bodies, the national authority may issue a statement with applicable measures to cease the violation.

Article 32. The national authority may request to government authority agents the publication of impact assessment reports on personal data protection and may suggest the adoption of standards and good practices for the processing of personal data by government authorities.

## **CHAPTER V**

### **INTERNATIONAL DATA TRANSFER**

Article 33. The international transfer of personal data is only allowed in the following cases:

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

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

- a) specific contractual clauses for a given transfer;
- b) standard contractual clauses;
- c) binding corporate rules;
- d) regularly issued seals, certificates and codes of conduct;

III – when the transfer is required for international legal cooperation among intelligence, investigation and prosecution government bodies, in accordance with the instruments of international law;

IV – when the transfer is required to protect the life or physical integrity of the data subject or of a third party;

V – when the national authority authorizes the transfer;

VI – when the transfer results in a commitment made in international cooperation agreements;

VII – when the transfer is required for enforcement of a public policy or legal attribution of public service, upon disclosure pursuant to item I of the head provision of article 23 of this Law;

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

IX – when required to meet the hypotheses provided in items II, V and VI of Article 7 of this Law.

Sole paragraph. For the 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 Act), within the scope of their legal powers, and those parties in charge, within the scope of their activities, may request the national authority to evaluate the level of protection of personal data granted by a third country or international organization.

Article 34. The level of data protection of the foreign country or international organization as mentioned in item I of the head provision of article 33 of this Law shall be evaluated by the national authority, which shall take into consideration:

I – the general and sectorial rules of the legislation in effect in the country of destination or in the international organization;

II – the nature of the data;

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

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

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

VI – other specific circumstances concerning the transfer.

Article 35. The national authority shall define the content of standard contractual clauses, as well as verify specific contractual clauses for a given transfer, binding corporate rules or seals, certificates and codes of conduct, referred to in item II of the head provision of Article 33 of this Law.

Paragraph 1. To verify the provisions of the head provision of this article, one must consider the requirements, conditions and minimum guarantees for the transfer that comply with the rights, guarantees and principles of this Law.

Paragraph 2. In the analysis of contractual clauses, documents or binding corporate rules submitted to the national authority for approval, supplementary information may be requested or procedures of verification of the processing operations may be carried out, when necessary.

Paragraph 3. The national authority may designate certification entities for the activities referred to in the head provision of this article, which shall remain under its supervision as defined in regulations.

Paragraph 4. The acts performed by a certification entity may be reviewed by the national authority and, if not compliant with this Law, shall be revised or voided.

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

Article 36. Amendments to the guarantees presented as sufficient for compliance with the general principles of protection and of the data subject's rights referred to in item II of Article 33 of this Law shall be communicated to the national authority.

## **CHAPTER VI**

### **PERSONAL DATA PROCESSING AGENTS**

#### **Section I**

##### **Controller and Processor**

Article 37. The controller and the processor shall maintain records of the personal data processing operations they perform, especially when based on legitimate interest.

Article 38. The national authority may require the controller to prepare a data protection impact assessment report, including sensitive data, relating to data processing operations, pursuant to regulation, complying with trade and industrial secrets.

Sole paragraph. Subject to 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 collecting and ensuring information security, as well as the analysis of the controller regarding the adopted measures, safeguards and risk mitigation mechanisms.

Article 39. The processor shall carry out the processing according to the instructions provided by the controller, who shall assess the compliance with both his/her own instructions and the rules on the matter.

Article 40. The national authority may provide for interoperability standards for portability purposes, free access to data and security, as well as for the registration storage period, notably in terms of necessity and transparency.

## **Section II**

### **Data Protection Officer**

Article 41. The controller shall appoint a data protection officer for the processing of personal data.

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

Paragraph 2. Data Protection Officer's activities consist of:

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

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

III – Instructing entity's employees and contractors on the practices to be adopted in relation to personal data protection; and

IV – performing other duties determined by the controller or established in supplementary rules.

Paragraph 3. The national authority may establish supplementary rules on the definition and duties of the data protection officer, including cases in which the appointment of such person may be waived, according to the nature and size of the entity or the volume of data processing operations.

Paragraph 4. (Vetoed) (Included by Law No. 13,853/2019)

## **Section III**

### **Liability and Damage Compensation**

Article 42. The controller or the processor that, when performing personal data processing activities, causes any pecuniary, moral, individual or collective damage to others, in violation of the personal data protection legislation, shall be required to compensate for such damage.

Paragraph 1. In order to ensure effective compensation to the data subject:

I – the processor shall be jointly liable for the damages caused by the processing when it fails to comply with the obligations of the data protection legislation or acts contrary to lawful instructions of the controller, in which case the processor shall be equivalent to the controller, except in events of exclusion as established in Article 43 of this Law;

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

Paragraph 2. The judge, in a civil proceeding, at his/her discretion, may reverse the burden of proof in favor of the data subject when the allegation appears to be true, there is hyposufficiency for the purpose of producing evidence, or when the evidence to be produced by the data subject is overly burdensome.

Paragraph 3. Judicial proceedings for compensation for collective damages, intended to establish liability pursuant to the terms of the head provision of this article, may be exercised collectively in court, subject to the provisions of relevant legislation.

Paragraph 4. Anyone who pays compensation for damages to the data subject has the right to demand compensation from other liable parties to the extent of their participation in the damaging event.

Article 43. Processing agents shall not be held liable only when they prove that:

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

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

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

Article 44. Processing of personal data shall be deemed irregular when it fails to comply with the law or when it does not provide the security expected by the data subject, considering the relevant circumstances of the processing, including:

I – the way it is performed;

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

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

Sole paragraph. The controller or the processor who causes damage by failing to adopt the security measures provided in Article 46 of this Law shall be liable for the damages deriving from data security violation.

Article 45. The events of violation of the data subject's right within the scope of consumer relations remain subject to the liability rules provided in relevant legislation.

## **CHAPTER VII**

### **SECURITY AND GOOD PRACTICES**

#### **Section I**

##### **Data Security and Confidentiality**

Article 46. Processing agents shall adopt technical and administrative security measures able to protect the personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication, or any form of improper or unlawful processing.

Paragraph 1. The national authority may provide minimum technical standards to make the provisions in the main provision of this article applicable, considering the nature of the processed information, the specific characteristics of the processing, and the current state



of technology, especially in the case of sensitive personal data, as well as the principles set forth in the head provision of Article 6 of this Law.

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

Article 47. Processing agents or any other person involved in one of the processing phases shall be required to ensure the information security provided for in this Law in relation to personal data, even after the conclusion of the processing in question.

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

Paragraph 1. Communication shall be made as soon as reasonably feasible, as defined by the national authority, and shall contain, at least:

- I – 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, complying with trade and industrial secrets;
- IV – the risks related to the incident ;
- V – the reasons for delay, in cases in which communication was not immediate; and
- VI – the measures that have been or shall be adopted to reverse or mitigate the effects of the damage.

Paragraph 2. The national authority shall determine the severity of the incident and, if required for safeguarding the data subjects' rights, may order the controller to adopt measures such as:

- I – full disclosure of the event in the media; and
- II – measures to reverse or mitigate the effects of the incident.

Paragraph 3. When assessing the severity of the incident, consideration shall be given to any evidence that appropriate technical measures were taken to render the affected personal data unintelligible, within the scope and technical limits of its services, to third parties who were not authorized to access them.

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

## **Section II**

### **Good Practices and Governance**

Article 50. Controllers and processors, within the scope of their duties for personal data processing, individually or by associations, may formulate rules for good practices and governance that provide for organization conditions, operational arrangements, procedures, including complaints and requests from data subjects, security rules, technical standards, specific obligations for those involved in the processing, educational activities, internal mechanisms for supervision and risk mitigation, and other aspects relating to personal data processing.

Paragraph 1. When establishing rules of good practices, the controller and the processor shall consider the nature, scope and purpose, regarding the processing and the data, as well as the probability and severity of the risks and benefits arising from the processing of the data subject's data.

Paragraph 2. When applying the principles indicated in items VII and VIII of the head provision of Article 6 of this Law, and subject to the structure, scale and volume of its processing operations, as well as the sensitivity of the processed data and the probability and severity of the damages to data subjects, the controller may:

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

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

b) apply to the entire set of personal data under his/her control, regardless the way it was collected;

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

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

e) intend to establish a relationship of trust with the data subject, by means of transparent actions that ensure mechanisms for the data subject's participation;

f) be integrated into his/her general governance structure and establish and apply internal and external supervision mechanisms;

g) have incident response and remediation plans; and

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

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

Paragraph 3. Rules on good practices and governance shall be published and updated periodically and may be acknowledged and disseminated by the national authority.

Article 51. The national authority shall encourage the adoption of technical standards that facilitate control by data subjects over their personal data.

## **CHAPTER VIII**

### **ENFORCEMENT**

#### **Section I**

#### **Administrative Sanctions / Penalties**

Article 52. Data processing agents, due to infringement of the rules established in this Law, shall be subject to the following administrative sanctions applicable by the national authority:

I – warning, indicating a deadline for adopting corrective measures;

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

III – daily fine, subject to the total limit referred to in item II;

IV – public disclosure of the infraction after its due investigation and confirmation;

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

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

VII – (vetoed);

VIII – (vetoed);

IX – (vetoed);

X – partial suspension of operations of the database to which the infraction relates for a maximum period of 6 (six) months, extendable for an equal period, until the controller regularizes the processing activity; (Included by Law No. 13,853/2019)

XI – suspension of the personal data processing activity to which the infraction relates for a maximum period of six (6) months, extendable for an equal period; (Included by Law No. 13,853/2019)

XII – partial or full prohibition of activities related to data processing. (Included by Law No. 13,853/2019)

Paragraph 1. The sanctions shall be applied following an administrative proceeding that provides opportunity for a full defense, in a gradual, single or cumulative manner, according to the peculiarities of the particular case and considering the following parameters and criteria:

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

II – the good faith of the offender;

III – the advantage obtained or intended by the offender;

IV – the economic condition of the offender;

V – recidivism;

VI – the extent of damage;

VII – the cooperation of the offender;

VIII – repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing the damage, aimed at safe and proper data processing, in accordance with the provisions of item II of paragraph 2 of Article 48 of this Law;

IX – adoption of a policy of good practices and governance;

X – prompt adoption of corrective measures; and

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

Paragraph 2. The provisions of this article do not replace the application of administrative, civil or criminal sanctions provided in Law No. 8,079, of September 11, 1990, and in specific legislation. (New wording given by Law No. 13,853/2019)

Paragraph 3. The provisions in items I, IV, V, VI, VII, VIII and IX of the head provision of this article may be applied to government entities and bodies, without prejudice to the provisions of Law No. 8,112 of December 11, 1990, Law No. 8,429, of June 2, 1992, and Law No. 12,527, of November 18, 2011. (New wording given by Law No. 13,853/2019)

Paragraph 4. When calculating the amount of the fine referred to in item II of the head provision of this article, the national authority may consider the total revenue of the company or group of companies, whenever it is unable to obtain the amount of revenue from the business field in which the infraction occurred, as defined by the national authority, or when the amount is presented in an incomplete form or is not demonstrated in an unequivocal and proper manner.

Paragraph 5. The proceeds from the collection of fines applied by the ANPD, whether or not registered as active debt, shall be allocated to the Diffuse Rights Defense Funds, as referred to in Article 13 of Law No. 7,347, of July 24, 1985, and in Law No. 9,008, of March 21, 1995. (Included by Law No. 13,853/2019)

Paragraph 6. The sanctions provided for in Items X, XI and XII of the head provision of this article shall be applied: (Included by Law No. 13,853/2019)

I - only after at least one (1) of the sanctions mentioned in items II, III, IV, V and VI of the head provision of this article have been imposed, for the same specific case; and (Included by Law No. 13,853/2019)

II – in case controllers are subject to other bodies and entities with sanctioning powers, after hearing those bodies. (Included by Law No. 13,853/2019)

Paragraph 7. Individual data breaches or unauthorized access referred to in the head provision of Article 46 of this Law may be subject of direct conciliation between the controller and the data subject, and, if no settlement is reached, the controller shall be subject to the application of the penalties referred to in this article. (Included by Law No. 13,853/2019)

Article 53. The national authority shall define, through its own regulation on administrative sanctions for infractions to this Law, which shall be subject of public consultation, the methodologies that will guide the calculation of the base value of fine sanctions.

Paragraph 1. The methodologies referred to in the head provision of this article shall be previously published, for the knowledge of the processing agents, and shall objectively present the forms and dosimetries for calculation of the base value of fines, which shall contain a detailed justification of all their elements, demonstrating compliance with the criteria provided for in this Law.

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

Article 54. The amount of daily fines applied to infractions of this Law shall consider the severity of the fault and the extent of the damage or loss caused and shall be justified by the national authority.

Sole paragraph. The daily fine notice shall contain at least a description of the obligation imposed, the reasonable deadline established by the body for compliance, and the amount of the daily fine to be applied for non-compliance.

## **CHAPTER IX**

### **THE NATIONAL DATA PROTECTION AUTHORITY (ANPD) AND THE NATIONAL COUNCIL FOR PERSONAL DATA AND PRIVACY PROTECTION**

#### **Section I**

##### **The National Data Protection Authority (ANPD)**

Article 55. (vetoed)

Article 55-A. The National Data Protection Authority (ANPD) is hereby created, a government agency of special nature, endowed with technical and decision-making autonomy, with its own assets and its headquarters and jurisdiction in the Federal District. (New wording given by Law No. 14,460/2022)

Article 55-B. (Repealed by Law No. 14,460/2022)

Article 55-C. ANPD is comprised of: (Included by Law No. 13,853/2019)

I – the Board of Directors, highest governing body; (Included by Law No. 13,853/2019)

II- the National Council for Personal Data and Privacy Protection; (Included by Law No. 13,853/2019)

III – the Disciplinary Board Office; (Included by Law No. 13,853/2019)

IV – the Ombudsman’s Office; (Included by Law No. 13,853/2019)

V - (Repealed). (New wording given by Law No. 14,460/2022)

V-A – the Office of Legal Affairs , and (Included by Law No. 14,460/2022)

VI - Administrative units and specialized units required for the enforcement of the provisions of this Law. (Included by Law No. 13,853/2019)

Article 55-D. ANPD’s Board of Directors shall consist of five (5) directors, including the Director-President. (Included by Law No. 13,853/2019)

Paragraph 1. The members of ANPD’s Board of Directors shall be chosen and appointed by the President of the Republic, after approval by the Federal Senate, pursuant to Article 52, item III, subitem “f”, of the Federal Constitution, and shall hold at least a commissioned position of the Higher Management and Advisory Group - DAS Level 5. (Included by Law No. 13,853/2019)

Paragraph 2. The members of the Board of Directors shall be chosen among Brazilians with unblemished reputation, higher education level and renowned for their expertise in the specialty field of the positions to which they will be appointed. (Included by Law No. 13,853/2019)

Paragraph 3. The term of office of the members of the Board of Directors shall be of 4 (four) years. (Included by Law No. 13,853/2019)

Paragraph 4. The terms of office of the first members of the Board of Directors shall be of 2 (two), 3 (three), 4 (four), 5 (five) and 6 (six) years, as provided for in the appointment act. (Included by Law No. 13,853/2019).

Paragraph 5. In the event of a vacancy during the term of office of a member of the Board of Directors, the remaining term shall be completed by the successor. (Included by Law No. 13,853/2019)

Article 55-E. The members of the Board of Directors shall only lose their positions by virtue of resignation, a final and unappealable judicial conviction or a dismissal penalty resulting from an administrative disciplinary proceeding. (Included by Law No. 13,853/2019)

Paragraph 1. Pursuant to the terms of the head provision of this article, the Chief of Staff of the Presidency of the Republic shall be responsible for initiating the correspondent administrative disciplinary proceeding, which shall be conducted by a special committee comprised of tenured federal civil servants. (Included by Law No. 13,853/2019)

Paragraph 2. The President of the Republic shall be responsible for ordering the preventive work leave, solely when so recommended by the special committee referred to in Paragraph 1 of this article, and then render the decision. (Included by Law No. 13,853/2019)

Article 55-F. The provisions in Article 6 of Law No. 12,813, of May 16, 2013 shall apply to the members of the Board of Directors, once their term comes to an end. (Included by Law No. 13,853/2019)

Sole Paragraph. Violation of the provisions laid out in the head provision of this article shall characterize an act of misconduct in public office. (Included by Law No. 13,853/2019)

Article 55-G. The regimental structure of ANPD shall be determined by an act issued by the President of the Republic. (Included by Law No. 13,853/2019)

Paragraph 1. Until the date of entry into force of its regimental structure, ANPD will be provided with technical and administrative support from the Office of the Chief of Staff of the Presidency of the Republic for the exercise of its activities. (Included by Law No. 13,853/2019)

Paragraph 2. The Board of Directors shall provide for the internal regulations of ANPD. (Included by Law No. 13,853/2019)

Article 55-H. The commission offices and positions of trust of ANPD shall be relocated from other bodies and entities of the Federal Executive Branch. (Included by Law No. 13,853/2019)

Article 55-I. The occupants of commission offices and positions of trust in ANPD shall be recommended by the Board of Directors and appointed or designated by the Director-President. (Included by Law No. 13,853/2019)

Article 55-J. ANPD shall be responsible for: (Included by Law No. 13,853/2019)

I – ensuring the protection of personal data, as provided in legislation; (Included by Law No. 13,853/2019)

II – ensuring compliance with trade and industrial secrets, observing the protection of personal data and the confidentiality of information when protected by law or when the breach of confidentiality violates the grounds established in Article 2 of this Law; (Included by Law No. 13,853/2019)

III – preparing guidelines for the National Policy for the Protection of Personal Data and Privacy; (Included by Law No. 13,853/2019)

IV – monitoring and applying sanctions in case of data processing carried out in non-compliance with the legislation, through an administrative proceeding that ensures right to adversary proceeding, full defense and right to appeal; (Included by Law No. 13,853/2019)

V – considering petitions from data subjects against controllers after the data subject has proven that a complaint has been submitted to the controller and has not been solved within the period established in the regulations; (Included by Law No. 13,853/2019)

VI – raising public awareness of the rules and public policies on the protection of personal data and security measures; (Included by Law No. 13,853/2019)

VII – promoting and conducting studies on national and international practices for the protection of personal data and privacy; (Included by Law No. 13,853/2019)

VIII – encouraging the adoption of standards for services and products that facilitate the control of data subjects over their personal data, considering the specificities of the activities and the size of the parties in charge; (Included by Law No. 13,853/2019)

IX – promoting international or transnational cooperation actions with personal data protection authorities of other countries; (Included by Law No. 13,853/2019)

X – providing for the forms of disclosure of personal data processing operations, subject to trade and industrial secrets; (Included by Law No. 13,853/2019)

XI – requesting, at any time, from the government entities carrying out personal data processing activities, a specific report on the scope, nature of the data and other details of the processing performed, with the possibility of issuing a supplementary technical opinion to ensure compliance with this Law; (Included by Law No. 13,853/2019)

XII – preparing annual management reports on its activities; (Included by Law No. 13,853/2019)

XIII – issuing regulations and procedures on the protection of personal data and privacy, as well as on data protection impact assessment reports for cases where the processing represents a high risk to the guarantee of the general principles of personal data protection established in this Law; (Included by Law No. 13,853/2019)

XIV – consulting processing agents and society on matters of relevant interest, and reporting on its activities and planning; (Included by Law No. 13,853/2019)

XV – collecting and investing its revenues, and disclosing the details of its revenues and expenses in the management report referred to in item XII of the head provision of this article; (Included by Law No. 13,853/2019)

XVI – conducting or determining the conduction of audits, within the scope of the inspection activity referred to in item IV, and with due observance of the provisions of item II of the head provision of this article on the processing of personal data by processing agents, including government authorities; (Included by Law No. 13,853/2019)

XVII – entering into commitments with processing agents, at any time, in order to eliminate irregularities, legal uncertainty or disputes in administrative proceedings, in accordance with the provisions of Decree-Law No. 4,657 of September 4, 1942; (Included by Law No. 13,853/2019)

XVIII – issuing simplified and special rules, guidelines and procedures, including information on deadlines, so that microenterprises and small businesses, as well as incremental or disruptive business initiatives that declare themselves startups or innovation companies, shall be able to adapt to this Law ; (Included by Law No. 13,853/2019)

XIX – ensuring that data processing of elderly people is carried out in a simple, clear, accessible and easy-to-understand manner, pursuant to this Law and Law No. 10,741, of October 1, 2003 (Statute of the Elderly); (Included by Law No. 13,853/2019)

XX – deliberating, at the administrative level, on a definitive basis, on the interpretation of this Law, its powers and matters on which the Law is silent; (Included by Law No. 13,853/2019)

XXI – reporting to the competent authorities any criminal offenses of which it becomes aware; (Included by Law No. 13,853/2019)

XXII – reporting to the internal control bodies the non-compliance with the provisions of this Law by bodies and entities of the federal public administration; (Included by Law No. 13,853/2019)

XXIII – coordinating with public regulatory authorities to exercise their powers in specific sectors of economic and governmental activities subject to regulation; and (Included by Law No. 13,853/2019)

XXIV – implementing simplified mechanisms, including by electronic means, for the record of complaints on the processing of personal data in non-compliance with this Law. (Included by Law No. 13,853/2019)

Paragraph 1. When imposing administrative conditions on the processing of personal data by private processing agents, whether in the form of limits, charges or obligations, ANPD must observe the requirement of minimum intervention, ensuring the grounds, principles and rights of data subjects established in Article 170 of the Federal Constitution and in this Law. (Included by Law No. 13,853/2019)

Paragraph 2. The rules and regulations issued by ANPD shall be preceded by public hearing and consultation, as well as by regulatory impact assessments. (Included by Law No. 13,853/2019)

Paragraph 3. ANPD and other government bodies and entities responsible for regulating specific sectors of economic and governmental activity shall coordinate their efforts, within the respective spheres of action, in order to ensure the fulfillment of their duties efficiently and to promote the proper functioning of regulated sectors, according to specific legislation, and the processing of personal data, pursuant to this Law. (Included by Law No. 13,853/2019)

Paragraph 4. ANPD shall maintain a permanent communication forum, including by way of technical cooperation, with bodies and entities of the public administration responsible for the regulation of specific sectors of economic and governmental activity, in order to facilitate ANPD's regulatory, monitoring and punitive powers. (Included by Law No. 13,853/2019)

Paragraph 5. When exercising the powers referred to in the head provision of this article, the competent authority shall ensure the preservation of business secrets and the confidentiality of information, as provided by law. (Included by Law No. 13,853/2019)

Paragraph 6. Complaints collected in conformity with the provisions of item V of the head provision of this article may be analyzed in an aggregate manner, and any measures arising therefrom may be adopted in a standardized manner. (Included by Law No. 13,853/2019)

Article 55-K. ANPD shall be exclusively responsible for applying the sanctions provided for in this Law, and its powers shall prevail, as far as the protection of personal data is concerned, over the related powers of other entities or bodies of the public administration. (Included by Law No. 13,853/2019)



Sole Paragraph. ANPD shall coordinate its actions with other bodies and entities with sanctioning and regulatory powers related to matters of personal data protection, and it shall be the central body for the interpretation of this Law and for setting the rules and guidelines for its implementation. (Included by Law No. 13,853/2019)

Article 55-L. ANPD's revenues comprise: (Included by Law No. 13,853/2019)

I - budget allocations, registered in the general budget of the Federal Government, special credits, supplementary credits, transfers and payments that are granted to it; (Included by Law No. 13,853/2019)

II - donations, bequests, subsidies and other funds assigned to it; (Included by Law No. 13,853/2019)

III – the amounts collected from the sale or rental of movable and immovable property of its own; (Included by Law No. 13,853/2019)

IV - the amounts collected from investments in the financial market of the revenues provided for in this article; (Included by Law No. 13,853/2019)

V – (vetoed); (Included by Law No. 13,853/2019)

VI - the funds from agreements, covenants or contracts entered into with national or international entities, bodies or companies, of either public or private law; (Included by Law No. 13,853/2019)

VII - the proceeds from the sale of publications, technical material, data and information, including for public bidding purposes. (Included by Law No. 13,853/2019)

Article 55-M. ANPD's assets and rights comprise: (Included by Law No. 14,460/2022)

I - those transferred to it by the Presidency of the Republic; and (Included by Law No. 14,460/2022)

II - those it shall acquire or incorporate. (Included by Law No. 14,460/2022)

Article 56. (vetoed)

Article 57. (vetoed)

## Section II

### The National Council for the Protection of Personal Data and Privacy

Article 58. (vetoed)

Article 58-A. The National Council for the Protection of Personal Data and Privacy shall be composed of twenty-three (23) representatives, permanent and alternates, from the following bodies: (Included by Law No. 13,853/2019)

I – five (5) representatives from the Federal Executive Branch; (Included by Law No. 13,853/2019)

II – one (1) representative from the Federal Senate; (Included by Law No. 13,853/2019)

III – one (1) representative from the Chamber of Deputies; (Included by Law No. 13,853/2019)

IV – one (1) representative from the National Council of Justice; (Included by Law No. 13,853/2019)

V – one (1) representative from the National Council of Prosecution Services; (Included by Law No. 13,853/2019)

VI – one (1) representative from the Brazilian Internet Steering Committee; (Included by Law No. 13,853/2019)

VII – three (3) representatives from entities of the civil society with activities related to the protection of personal data; (Included by Law No. 13,853/2019)

VIII – three (3) representatives from scientific, technological and innovative institutions; (Included by Law No. 13,853/2019)

IX – three (3) representatives from trade-union confederations representing the economic categories of the productive sector; (Included by Law No. 13,853/2019)

X – two (2) representatives from entities representing the business sector related to the area of personal data processing; and (Included by Law No. 13,853/2019)

XI – two (2) representatives from entities representing the labor sector. (Included by Law No. 13,853/2019)

Paragraph 1. The representatives shall be designated by an act of the President of the Republic, either directly or by delegation of authority. (Included by Law No. 13,853/2019)

Paragraph 2. The representatives referred to in items I, II, III, IV, V and VI of the head provision of this article and their alternates shall be appointed by the chief officers of the respective bodies and entities of the public administration. (Included by Law No. 13,853/2019)

Paragraph 3. The representatives referred to in items VII, VIII, IX, X and XI of the head provision of this article and their alternates: (Included by Law No. 13,853/2019)

I - shall be appointed as provided in relevant regulation; (Included by Law No. 13,853/2019)

II - must not be members of the Brazilian Internet Steering Committee; (Included by Law No. 13,853/2019)

III - shall have a two-year term of office, with one reappointment being allowed. (Included by Law No. 13,853/2019)

Paragraph 4. Participation in the National Council for the Protection of Personal Data and Privacy shall be considered a relevant unpaid public service. (Included by Law No. 13,853/2019)

Article 58-B. The National Council for the Protection of Personal Data and Privacy is responsible for: (Included by Law No. 13,853/2019)

I – proposing strategic guidelines and providing background information for the preparation of the National Policy for the Protection of Personal Data and Privacy and for ANPD's activities; (Included by Law No. 13,853/2019)

II – preparing annual reports to evaluate the implementation of the actions of the National Policy for the Protection of Personal Data and Privacy; (Included by Law No. 13,853/2019)

III – recommending actions to be performed by the ANPD; (Included by Law No. 13,853/2019)

IV – conducting studies and holding public debates and public hearings on the protection of personal data and privacy; and (Included by Law No. 13,853/2019)

V – disseminating knowledge about the protection of personal data and privacy to the general population. (Included by Law No. 13,853/2019)

Article 59. (vetoed)

## **CHAPTER X**

### **FINAL AND TRANSITIONAL PROVISIONS**

Article 60. Law No. 12,965, of April 23, 2014 (Brazilian Civil Rights Framework for the Internet) is hereby amended as follows:

“Article 7. (...)

X – definitive exclusion of the personal data provided to a particular internet application, upon the user’s request, at the end of the relationship between the parties, except for the cases of mandatory log retention provided for in this Law and in that which governs personal data protection;

(...)”

“Article 16. (...)

II – personal data that are excessive in relation to the purpose for which data subject’s consent was given, except in the events provided for in the Law that governs personal data protection.”

Article 61. The foreign company shall be notified and summoned of all procedural acts established in this Law, regardless of power of attorney or contractual or statutory provisions, in the person of the agent or representative or person in charge of its branch, agency, subsidiary, establishment or office located in Brazil.

Article 62. The national authority and the Anísio Teixeira National Institute for Educational Studies and Research (Inep), within their powers and regulatory capacity, shall enact specific regulations for accessing data processed by the Federal Government for compliance with the provisions of paragraph 2 of Article 9 of Law No. 9,394, of December 20, 1996 (Brazilian National Education Basis and Guidelines Act- LDB), and those relating to the National Higher Education Evaluation System (Sinaes), as provided for in Law No. 10,861, of April 14, 2004.

Article 63. The national authority shall establish rules on the progressive adjustment of databases created up to the date of entry into force 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 shall not exclude others provided for in the Brazilian legal system concerning the matter or in international treaties to which the Federative Republic of Brazil is a party.

Article 65. This Law shall enter into force: (New wording given by Law No. 13,853/2019)

I – on December 28, 2018, as 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 e 58-B; and (Included by Law No. 13,853/2019)

I-A – on August 1, 2021, as for arts. 52, 53 and 54; (Included by Law No. 14,010/2020)

II – 24 (twenty-four) months following its official publication, as for the remaining articles. (Included by Law No. 13,853/2019)

Brasília, August 14, 2018; the 197th Anniversary of the Independence and the 130th Anniversary of the Republic.

**MICHEL TEMER**

*Torquato Jardim*

*Aloysio Nunes Ferreira Filho*

*Eduardo Refinetti Guardia*

*Esteves Pedro Colnago Junior*

*Gilberto Magalhães Occhi*

*Gilberto Kassab*

*Wagner de Campos Rosário*

*Gustavo do Vale Rocha*

*Ilan Goldfajn*

*Raul Jungmann*

*Eliseu Padilha*