Rennó Penteado Sampaio
ADVOGADOS

Brazilian General Data Protection Law

Translation by Ronaldo Lemos, Natalia Langenegger, Juliana Pacetta Ruiz, Sofia Lima Franco, Andréa Guimarães Gobbato, Daniel Douek, Ramon Alberto dos Santos and Rafael A. Ferreira Zanatta. ***As amended by Law no. 13,583, after congressional override of presidential vetoes.***
This translation was based on an initial version by Monica Hruby (www.mhruby.com)

~~Amends Law No. 13,709 of August 14, 2018, to provide for the protection of personal data and to create the National Data Protection Authority; and makes other arrangements.~~
Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019)

The NATIONAL CONGRESS decrees:

CHAPTER I
PRELIMINARY PROVISIONS

Art. 1 This Law provides for the processing of personal data, including by digital means, by a natural person or a legal entity of 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. (by Law No. 13,853/2019)

Art. 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 image;

V – economic and technological development and innovation;

VI – free enterprise, free competition and consumer defense;

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

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

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

~~II – the processing activity is aimed at the offering or provision of goods or services, or at the processing of data of individuals located on the national territory;~~

II – the processing activity is aimed at the offering or provision of goods or services, or at the processing of data of individuals located on 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.

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

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

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

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

II – is done exclusively:

a) for journalistic and artistic purposes; or

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

III – is done exclusively for purposes of:

a) public safety;

b) national defense;

c) state security; or

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

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

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

§2 Processing of the data referred to in item III of the lead sentence of this article is forbidden for legal entity of private law, except in procedures under the authority of legal entity of public law, of which the national authority shall be specifically informed and which shall observe the limitation imposed in §4 of this article.

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

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

§4 §4 Under no circumstances the entirety of the personal data in a database, as provided in Item III of the lead sentence of this article, may be processed by a legal entity of private law, unless its capital is integrally held by public entities. (New Wording Given by Law No. 13,853/2019)

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

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

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

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

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

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

VI – controller: natural person or legal entity of 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 in the name of the controller;

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

VIII - data protection officer: person named by the controller and processor to act as a channel of communication between the controller, the subjects of such data 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 carried out with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction;

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

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

XIII – blocking: temporary suspension of any processing operation, by means of

retention of the personal data or the database;

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

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

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

XVII – data protection impact assessment[1] : documentation from the controller that contains the description concerning the proceedings of the personal data processing that could pose risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate said risk;

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

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

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

XIX - national authority: body of the public administration responsible for supervising, implementing and monitoring the compliance with this Law in all national

[1] The LGPD uses the expression “relatório de impacto” (impact report) instead of “impact assessment”. However, considering that Data Protection Impact Assessment is the regular expression in laws of data protection, we chose to translate “relatório de impacto à proteção de dados pessoais” as “data protection impact assessment” (Translator’s Note).

territory." (New Wording Given by Law No. 13,853/2019).

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

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

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

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

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

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

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

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

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

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

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

CHAPTER II

PROCESSING OF PERSONAL DATA

Section I

Requirements for the Processing of Personal Data

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

I – with the consent of the data subject;

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

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

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

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

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

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

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

VIII – to protect the health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities; (New Wording Given by Law No. 13,853/2019)

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

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

§1-(Revoked). (New Wording Given by Law No. 13,853/2019)

§2-(Revoked). (New Wording Given by Law No. 13,853/2019)

§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.

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

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

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

§7 The subsequent processing of the 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 to 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).

Art. 8 The consent provided in item I of Art. 7 of this Law shall be given in writing or by other means able to demonstrate the manifestation of the will of the data subject.

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

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

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

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

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

§6 If there is a change in the information as referred to in items I, II, III or V of Art. 9 of this Law, the controller shall inform the data subject, with specific highlight of the content

of the changes, in which case the data subject, in those cases where her/his consent is required, may revoke it if she/he disagrees with the change.

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

I – the specific purpose of the processing;

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

III – identification of the controller;

IV – the controller's contact information;

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

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

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

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

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

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

Art. 10. Controller's legitimate interest can only be grounds for processing personal data for legitimate purposes, based on particular situations, which include but are not limited to:

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

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

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

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

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

Section II
Processing of Sensitive Personal Data

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

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

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

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

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

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

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

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

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

f) to protect the health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities; (New Wording Given by Law No. 13,853/2019)

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

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

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

§3 Communication or shared use of sensitive personal data between controllers for the purpose of obtaining an economic advantage may be prohibited or regulated by the national authority, being heard the sectoral entities of the public authority, within their regulatory capacity.[2]

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

§4 Communication or shared use between controllers of sensitive personal data referring to health in order to obtain an economic advantage is prohibited, except in hypotheses related to the provision of health services, pharmaceutical assistance and health insurance[3], as long as the paragraph 5 of this article is observed, including auxiliary diagnostic and therapeutic services, in benefit of the interests of the data subject and also to allow:

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

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

§5 Operators of private health care plans are prohibited from processing health data

[2] We translated “dentro de suas competências” as “within their regulatory capacity” and not “within their competence” because it is not common to use “competence” in this context in English (Translator’s Note).
[3] Following the official terminology of the Brazilian Regulatory Agency for Private Health Insurance and Plans (ANS), we translated “serviços de assistência à saúde” as “health insurance”. We have also substituted “competence” for “capabilities”, in some cases (Translator’s Note).

for the practice of risk evaluation in any modality of hiring, as well as the hiring and exclusion of beneficiaries. (Included by Law No. 13,853/2019)

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

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

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

§3 The national authority may provide for standards and techniques to be used in processes of anonymization, and carry out security checks, with opinions from the National Board for the Protection of Personal Data.

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

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

§2 The research entity shall be held liable for the security of the information provided in the lead sentence of this article, and it is forbidden, under any circumstances, to transfer the data to a third party.

§3 Access to data as provided in this article shall be the object of regulation by the national authority and of the authorities in the area of health and sanitation, within the scope of their regulatory capacity.[4]

§4 For purposes of this article, pseudonymization is the processing by means of which

[4] See footnote number 2.

data can no longer be directly or indirectly associated with an individual, except by using additional information kept separately by the controller in a controlled and secure environment.

Section III
Processing of Children and Adolescents' Personal Data

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

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

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

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

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

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

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

Section IV

Termination of Data Processing

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

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

II – end of the processing period;

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

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

Art. 16. Personal data shall be deleted following the termination of their processing, within the scope and technical limits of the activities, 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 entity, ensuring, whenever possible, the anonymization of the personal data;

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

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

CHAPTER III
DATA SUBJECTS' RIGHTS

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

Art. 18. The data subject[5], regarding the data subject's data being processed by the controller, at any time and by means of request, has the right to obtain the following from the controller:

I – confirmation of the existence of the processing;

II – access to the data;

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

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

~~V - portability of the data to another service or product provider, by means of an express request and subject to commercial and industrial secrecy, pursuant to the regulation of the controlling agency;~~

V – portability of the data to another service provider or product provider, by the means of an express request, pursuant with the regulations of the national authority, and subject to commercial and industrial secrets; (New Wording Given by Law No. 13,853/2019)

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

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

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

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

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

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

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

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

[5] For reasons of objectivity and clarity, we translated "titular dos dados pessoais" simply as "data subject" in the whole document (Translator's Note).

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

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

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

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

§6 The controller shall immediately inform the processing agents with which she/he has carried out the shared use of data of the correction, deletion, anonymization or blocking of data, so that they can repeat an identical procedure, except in cases in which this action is proven impossible or involves disproportionate effort. (New Wording Given by Law No. 13,853/2019)

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

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

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

I – in a simplified format, immediately; or

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

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

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

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

II – in printed form.

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

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

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

Art. 20. The data subject has the right to request for the review of decisions made solely based on automated processing of personal data affecting her/his interests, including decisions intended to define her/his personal, professional, consumer and credit profile, or aspects of her/his personality. (New Wording Given by Law No. 13,853/2019)

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

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

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

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

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

CHAPTER IV
PROCESSING OF PERSONAL DATA BY PUBLIC AUTHORITIES

Section I

Rules

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

I – they communicate the situations in which, in the exercise of their regulatory capacities, they carry out the processing of personal data, supplying clear and up-to-date information about the legal base, purpose, procedures and practices used to carry out these activities in 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, in accordance with Art. 39 of this Law; and (New Wording Given by Law No. 13,853/2019)

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

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

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

§3 The time periods and procedures for exercising data subjects' rights before the public authorities shall obey the provisions of specific legislation, especially the provisions stated in Law No. 9,507, of November 12, 1997 (the "Brazilian Habeas Data Law"), of Law No. 9,784, of January 29, 1999 (the "Federal Administrative Procedure Law"), and of Law No. 12,527, of November 18, 2011 (the "Brazilian Access to Information Law").

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

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

article.

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

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

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

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

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

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

II – (vetoed);

III – in cases in which 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)

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

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

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

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

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

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

Art. 28. (vetoed)

~~**Art. 29.** The national authority may request, at any time, that entities of the public authority carry out operations of processing of personal data, specific report about the scope and nature of the data and other details of the processing, and may issue complementary technical opinion to ensure compliance with this Law.~~

Art. 29. The national authority may request, at any time, for bodies and entities of the Public Administration to carry out personal data processing operations, the specific information on the scope and nature of the data and other details of the processing performed and may issue complementary technical report to ensure compliance with this Law." (New Wording Given by Law No. 13,853/2019)

Art. 30. The national authority may establish complementary rules for communication or shared used of personal data activities.

Section II
Accountability

Art. 31. When there is an infringement of this Law as a result of personal data processing by public agencies, the national authority may issue a statement with applicable

measures to stop the violation.

Art. 32. The national authority may request agents of the public authorities to publish impact reports on protection of personal data and may suggest the adoption of standards and good practices for processing personal data by the public authorities.

CHAPTER V
INTERNATIONAL TRANSFER OF DATA

Art. 33. International transfer of personal data is only allowed in the following cases:

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

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

a) specific contractual clauses for a given transfer;

b) standard contractual clauses;

c) binding corporate rules[6];

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

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

IV – when the transfer is necessary to protect the life or physical safety 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 undertaken through international cooperation;

VII – when the transfer is necessary for the execution of a public policy or legal

[6] Following the language of General Data Protection Regulation, we translated “normas corporativas globais” as “binding corporate rules”, also known as BCRs (Translator’s Note).

attribution of public service, which shall be publicized pursuant to item I of the lead sentence of Art. 23 of this Law;

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

IX – when it is necessary to satisfy the situations provided in items II, V and VI

of Art. 7 of this Law.

Sole paragraph. For purposes of item I of this article, the legal entities of public law referred to in the sole paragraph of Art. 1 of Law No. 12,527, of November 18, 2011 (the "Brazilian Access to Information Law"), within their legal capabilities, and those parties accountable, within the scope of their activities, may request the national authority to evaluate the level of protection of personal data provided by a country or international organization.

Art. 34. The level of data protection in the foreign country or international organization referred to in item I of the lead sentence of Art. 33 of this Law shall be evaluated by the national authority, which shall take into consideration:

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

II – the nature of the data;

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

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

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

VI – other specific circumstances relating to the transfer.

Art. 35. The definition of the content of standard contractual clauses, as well as the verification of specific contractual clauses for a particular transfer, binding corporate rules or stamps, certificates and codes of conduct, referred to in item II of the lead sentence of Art. 33 of this Law, will be done by the national authority.

§1 To verify the provision of the lead sentence of this article, one must consider the

requirements, conditions and minimum guarantees for the transfer that are in accordance with the rights, guarantees and principles of this Law.

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

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

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

§5 Guarantees that are sufficient for compliance with the general principles of protection and data subject's rights referred to in the lead sentence of this article shall also be analyzed in accordance with the technical and organizational measures adopted by the processor, according to the provisions of §§1 and 2 of Art. 46 of this Law.

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

CHAPTER VI
PERSONAL DATA PROCESSING AGENTS
Section I
Controller and Processor

Art. 37. The controller and the processor shall keep records of personal data processing operations carried out by them, especially when based on legitimate interest.

Art. 38. The national authority may determine that the controller must prepare a data protection impact assessment, which shall include personal data, sensitive data, and refer to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy.

Sole paragraph. Subject to the provisions of the lead sentence of this article, the report

must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards and mechanisms of risk mitigation.

Art. 39. The processor shall carry out the processing according to the instructions provided by the controller, which shall verify the obedience of her/his own instructions and of the rules applicable to the subject and the situation at hand.

Art. 40. The national authority may provide standards of interoperability for purposes of portability, free access to data and security, as well as standards for periods in which records on personal data must be kept, considering the necessity and the transparency.

Section II
Data Protection Officer

Art. 41. The controller shall appoint a data protection officer to be in charge of processing personal data.

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

§2 Data Protection Officer's activities consist of:

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

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

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

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

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

§4 (vetoed). (Included by Law No. 13,853/2019)

Section III

Liability and Loss Compensation

Art. 42. The controller or the processor that, as a result of carrying out their activity of processing personal data, cause material, moral, individual or collective damage to others, in violation of legislation for the protection of personal data, are obligated to redress it.

§1 In order to ensure the effective compensation to the data subject:

I – processors are jointly liable for damages caused by the processing when they do not comply with the obligations of data protection legislation or when they have not followed controller's lawful instructions. In this last case, the processor is deemed equivalent to the controller, save from cases of exclusion as provided in Art. 43 of this Law;

II – controllers directly involved in the processing from which damages resulted to the data subject shall jointly answer, save from cases of exclusion as provided in Art. 43 of this Law.

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

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

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

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

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

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

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

Art. 44. Processing of personal data shall be deemed irregular when it does not obey the legislation or when it does not provide the security that its data subject can expect, considering the relevant circumstances of the processing, among which are:

I – the way in which the processing was carried out;

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

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

Sole paragraph. The controller or the processor who neglect to adopt the security measures provided in Art. 46 of this Law shall be held liable for damages caused by the violation of the security.

Art. 45. When there is a violation of data subject's rights in the scope of consumer relations, the rules of liability provided in the pertinent legislation shall apply.

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

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

§1 The national authority may provide minimum technical standards to make the provisions of the lead sentence of this article applicable, taking into account the nature of the

processed information, the specific characteristics of the processing and the current state of technology, especially in the case of sensitive personal data, as well as the principles provided in the lead sentence of Art. 6 of this Law.

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

Art. 47. Processing agents or any other person that intervenes in one of the processing phases commit themselves to ensure the security of the information as provided in this Law regarding personal data, even following the conclusion of the processing in question.

Art. 48. The controller must communicate to the national authority and to the data subject the occurrence of a security incident that may create risk or relevant damage to the data subjects.

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

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

II – information on the data subjects involved;

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

IV – the risks related to the incident;

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

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

of the damage.

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

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

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

§3 When judging the severity of the incident, there will be an analysis of eventual demonstrations that, within the scope and the technical limits of the services, adequate technical measures were adopted to render the affected personal data unintelligible to third

parties who were not authorized to access them.

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

Section II
Good Practice and Governance

Art. 50. Controllers and processors, within the scope of their functions, concerning the processing of personal data, individually or by associations, may formulate rules for good practices and governance that set forth conditions of organization, a regime of operation, the procedures, including those for complaints and petitions from data subjects, security norms, technical standards, specific obligations for the various parties involved in the processing, educational activities, internal mechanisms of supervision and risk mitigation and other aspects related to the processing of personal data.

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

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

I – implement governance program for privacy that, at the very least:

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

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

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

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

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

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

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

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

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

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

Art. 51. The national authority shall encourage the adoption of technical standards that facilitate data subjects' control of their personal data.

CHAPTER VIII
MONITORING
Section I
Administrative Sanctions

Art. 52. Data processing agents that commit infractions of the rules provided in this Law are subject to the following administrative sanctions, to be applied by the national authority:

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

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

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

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

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

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

VII – (vetoed);

VIII – (vetoed);

IX – (vetoed);

X – partial suspension of the operation of the database related to the infraction for a maximum period of 6 (six) months, extendable for the same period, until the normalization of the processing activity by the controller; (Included by Law No. 13,853/2019)

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

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

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

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

II – the good faith of the offender;

III - the advantage received or intended by the offender;

IV – the economic condition of the offender;

V – recidivism;

VI – the level of damage;

VII – the cooperation of the offender;

VIII – repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing the damage, for secure and proper data processing, in accordance with the provisions of item II of §2 of Art. 48 of this Law.

IX – adoption of good practices and governance policy;

X – the prompt adoption of corrective measures; and

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

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

§2 The provisions in this article are not a replacement to the application of administrative, civil and criminal sanctions in the Law No. 8,079, September 11th, 1990, or in specific legislation. (New Wording Given by Law No. 13,853/2019)

§3 The provisions of Items I, IV, V, VI, X, XI and XII of the lead sentence of this article may be applied to public entities and bodies, without prejudice to the provisions of Laws Nos. 8,112, of December 11, 1990, 8,429, of June 2, 1992, and 12,527, of November 18, 2011.

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

§5 The sum of the collection of fines applied by the ANDP, whether or not registered as active debt, shall be allocated to the Diffuse Rights Defense Funds, as referred to in the art. 13 of Law No. 7,347 of July 24, 1985, and Law No. 9,008 of March 21, 1995.

§6 Sanctions provided for in Items X, XI and XII of the lead sentence of this article shall be applied:

I - only after at least one (1) of the sanctions mentioned in items II, III, IV, V and VI of the lead sentence of this article have been imposed, for the same facts; and

II - in the case of controllers subject to other agencies and entities with sanctioning powers, after those entities and agencies are heard. (Included by Law No. 13,853/2019)

§7 The individual data leaks or unauthorized access mentioned in the lead sentence of the art. 46 of this Law may be subject of direct conciliation between controller and data subject, and, in the absence of an agreement, the controller shall be subject to the penalties referred to in this article.” (Included by Law No. 13,853/2019)

Art. 53. The national authority shall define the methodologies that will be used for the

calculation of the base value for fines, by means of its own regulations concerning administrative sanctions for violations of this Law, which must be the object of a public consultation.

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

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

Art. 54. The amount of daily fines applied to infractions of this Law shall observe the severity of the infraction and the extent of the damage or losses caused, and with grounded reasoning by the national authority.

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

CHAPTER IX
THE NATIONAL DATA PROTECTION AUTHORITY ("ANPD") AND THE NATIONALCOUNCIL FOR PROTECTION OF PERSONAL DATA AND PRIVACY

Section I
The National Data Protection Authority ("ANPD")

Art. 55. (vetoed)

Art. 55-A The National Data Protection Authority ("ANPD") is hereby created, without any increase in expenses, an entity part of the federal public administration, pertaining to the Presidency of the Republic.

§1 The legal nature of the ANPD is transitional and may be transformed by the Executive Branch into an indirect federal public administration entity, subject to a special autarchic regime and pertaining to the Presidency of the Republic.

§2 The assessment of the transformation referred in the §1 of this article shall occur within two (2) years from the date of entry into force of the ANPD's regulatory framework.

§3 The provisions of necessary positions and functions to the creation and performance of the ANPD are conditioned to express physical and financial authorization in the annual Budget Law and to the permission in the Budget Directives Law. (Included by Law No. 13,853/2019)

Art. 55-B Technical and operative autonomy is ensured to ANPD.

Art. 55-C ANPD is comprised of:

I - Board of Directors, highest governing body;

II- National Council for Personal Data and Privacy Protection;

III - Internal Affairs Office;

IV - Ombudsman Office;

V - Its own legal advisory body; and

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

Art. 55-D ANPD Board of Directors shall be comprised of five (5) chief officers, including the Chief Executive Officer

§1 The members of ANPD Board of Directors shall be chosen and appointed by the President of the Republic, after approval by the Federal Senate in the terms of line f of Item III of the art. 52 of the Federal Constitution, and they will hold a commission position of the Direction-Group and Superior Advisory - Level 5 DAS.

§2 The members of the Board of Directors shall be chosen among Brazilians, with an immaculate reputation, a high level of education and considered renowned in the field of the positions for which they will be appointed.

§3 Members of the Board of Directors shall serve four-year (4) terms.

§4 The term of the first members of the Board of Directors will be of two, three, four, five and six years, as provided for in the appointment.

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

Art. 55-E The members of the Board of Directors will only lose their position upon resignation, final and unappealable judicial conviction or dismissal penalty due to disciplinary administrative proceeding.

§1 Pursuant to the lead sentence of this article, the President's Chief of Staff shall be responsible for initiating the disciplinary administrative proceeding, which shall be conducted by a special commission composed of stable federal public servants.

§2 The President of the Republic shall be responsible for determining the preventive work leave, solely when recommended by the special commission referred in the §1 of this article, and then hand down the decision. (Included by Law No. 13,853/2019)

Art. 55-F The provision set forth in art. 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.

Sole Paragraph. Breach to the provisions set forth in the lead sentence of this article shall characterize an act of administrative improbity.

Art. 55-G The ANPD regimental structure shall be determined by an act from the President of the Republic.

§1 Until ANPD regimental structure comes into force, ANPD will be provided with technical and administrative assistance from the Office of the President's Chief of Staff in order to fulfill its activities.

§2 The Board of Directors shall decide on the internal regulations of the ANPD. (Included by Law No. 13,853/2019)

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

Art. 55-I Those servers in commission and trust positions in ANPD shall be recommended by the Board of Directors and appointed or designated by the Chief Executive Officer. (Included by Law No. 13,853/2019)

Art. 55-J The National Authority has the following duties:

I – to ensure the protection of personal data, as provided in legislation;

II – to ensure the observance of commercial and industrial secrets, as long as the protection of personal data and the confidentiality of information when it is protected by law or when the breach of confidentiality violates the grounds of art. 2 of this Law;

III – to elaborate guidelines for the Personal Data Protection and Privacy National Policy;

IV – to monitor and apply sanctions for data processing that is not compliant with legislation, through an administrative process that ensures right to adversary proceeding, full defense and the right to appeal;

V – to receive pleadings from the data subject against the controller after the data subject has demonstrated that he/she presented a complaint against the controller that was not solved in the timeframe established in regulation;

VI – to promote the knowledge of the norms and public policies on the protection of personal data and of the security measures to the general population;

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

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

IX – to promote cooperation initiatives with data protection authorities of other countries, of international or transnational nature;

X – to decide on the forms of publicity regarding personal data processing operations, observing commercial and industrial secrecy;

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

XII – to draft annual management reports of its activities;

XIII – to amend regulations and procedures on the protection of personal data and privacy, as well as on data protection impact assessment reports in cases in which the processing represents a high risk to the guarantee of the general principles of personal data protection foreseen in this Law;

XIV – to listen to processing agents and to the society in matters of relevant interest and to report on their activities and planning;

XV– to collect and apply its revenues and publish the breakdown of its revenues and expenses in the management report referred to in item XII of the lead sentence of this article;

XVI – to carry out audits, or to determine their occurrence regarding the processing of personal data carried out by processing agents, including public authorities;

XVII – to hold, at any time, agreements with processing agents in order to eliminate irregularities or legal uncertainties in administrative proceedings, in accordance with other provisions in Brazilian Law;

XVIII – to enact rules, guidelines and simplified and special procedures, including deadlines, so that microenterprises and small businesses are able to adapt to this Law, as well as incremental or disruptive business initiatives that declare themselves startups or innovation companies;

XIX – to ensure that data processing of elderly people is carried out in a simple, clear, accessible and adequate form to their understanding, in accordance with this Law the Statute of the Elderly;

XX – to discuss, at the administrative level, on the interpretation of this Law, its authorities and matters on which the Law is silent;

XXI – to report criminal offenses that it becomes aware of to competent authorities;

XXII – to report to the internal control bodies any violation to the provisions set forth in this Law performed by bodies and entities of the federal public administration;

XXIII – to coordinate with public regulatory authorities to exert their authority in specific sectors of economic and governmental activities bound to regulation; and

XXIV – to implement simplified mechanisms, including by electronic means, in order to collect and record complaints on the processing of personal data non-compliant with this Law.

§1 When imposing administrative constraints on the processing of personal data by a private agent, whether they are constituted of limits, charges or subjections, the ANPD must observe the requirement of minimum intervention, ensuring the grounds, principles and rights of data subjects set forth in art. 170 of the Federal Constitution and in this Law.

§2 Regulation and rules enacted by ANPD shall be preceded by public consultation and hearings, as well as regulatory impact assessments.

§3 The ANPD and other public bodies and entities responsible for regulating specific sectors of economic and governmental activity shall coordinate their activities, in their respective spheres of action, in order to ensure the fulfillment of their duties efficiently and to promote the adequate functioning of regulated sectors, according to specific and sectoral legislation, and the processing of personal data, in conformity with this Law.

§4 The ANPD shall maintain a permanent communication forum, including by 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 duties.

§5 In the exercise of the powers referred to in the lead sentence of this article, the relevant authority shall ensure the preservation of industrial and information secrecy, in the terms of the law.

§6 Complaints collected in accordance with the provisions set forth in item V of the lead sentence 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)

Art. 55-K Applying the sanctions as provided for herein shall be the sole responsibility of the ANPD, and in matters concerning the protection of personal data, its powers and jurisdiction shall prevail over the jurisdiction of other entities or bodies of the public administration.

Sole Paragraph. ANPD shall articulate its operation and practices with other bodies and entities with sanctioning and normative 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 standards and guidelines for the implementation thereof. (Included by Law No. 13,853/2019)

Art. 55-L Revenues from ANPD are:

I - budget allocations, provided in the general budget of the Union, special credits, additional credits, transfers and payments that are conferred to it;

II - donations, bequests, subsidies and other resources destined to it;

III - amounts determined in the sale or lease of movable and immovable assets of its property;

IV - amount calculated in financial market applications of the revenues provided in

this article;

V – (vetoed);

VI - resources derived from agreements, contracts or similar instruments held with entities, bodies or companies, of either public or private law, national or international;

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

Art. 56. (vetoed)

Art. 57. (vetoed)

Section II

The National Council for the Protection of Personal Data and Privacy

Art. 58. (vetoed)

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

I – five (5) representatives from the federal Executive Branch;

II – one (1) representative from the Federal Senate;

III – one (1) representative from the House of Representatives;

IV – one (1) representative from the National Council of Justice;

V – one (1) representative from the National Council of Public Prosecutors;

VI – one (1) representative from the Brazilian Internet Steering Committee;

VII – three (3) representatives from entities of the civil society with experience related to personal data protection;

VIII – three (3) representatives from scientific, technological and innovative institution;

IX – three (3) representatives from trade union confederations representing the economic categories of the sector;

X – two (2) representatives from entities representatives of the business sector related to the area of personal data processing; and

XI – two (2) representatives from labor sector.

§1 The representatives shall be appointed by the President of the Republic, and the

delegation of this function is allowed.

§2 The representatives referred to in items I, II, III, IV, V and VI of the lead sentence of this article and their alternate shall be appointed by the full representatives of their respective bodies and entities of the public administration.

§3 The representatives referred to in items VII, VIII, IX, X and XI of the lead sentence of this article and their alternate thereof:

I - shall be appointed as provided for in the regulation;

II - must not be members of the Brazilian Internet Steering Committee (*Comitê Gestor da Internet no Brasil*);

III - shall have a two-year (2) term, with one reappointment being allowed.

§4 Participation in the National Council of Personal Data Protection and Privacy will be considered a relevant unpaid public service.

Art. 58-B It is incumbent on the National Council of Personal Data Protection and Privacy to:

I - propose strategic guidelines and provide subsidies for the preparation of Personal Data Protection and Privacy National Policy and for the operation of ANPD;

II - prepare annual reports to evaluate the execution of the actions of the Personal Data Protection and Privacy National Policy;

III – suggest actions to be performed by ANPD;

IV – prepare studies and hold public debates and public hearing on personal data 8 protection and privacy; and

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

Art. 59 (vetoed)

CHAPTER X
FINAL AND TRANSITIONAL PROVISIONS

Art. 60. Law No. 12,965, of April 23, 2014 (the "Brazilian Internet Law"), shall henceforth contain the following alterations:

"Art. 7 …

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

"Art. 16…

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

Art. 61 The foreign company shall be notified and summonsed of all procedural acts provided in this Law, irrespective of power of attorney or contractual or statutory provisions, in the person of the agent or representative or person responsible for its subsidiary, agency, branch, establishment or office located in Brazil.

Art. 62. The national authority and the Anísio Teixeira National Institute for Educational Studies and Research (Inep), within the scope of their regulatory capacity, shall enact specific regulations for accessing data processed by the Union for compliance with the provisions of §2 of Art. 9 of Law No. 9,394, of December 20, 1996 (the "Directive and Bases of National Education Act"), and those relating to the National Higher Education Evaluation System (Sinaes), as provided in Law No. 10,861, of April 14, 2004.

Art. 63. The national authority shall establish rules on the progressive suitability of databases established up to the date this Law comes into force, taking into account the complexity of the data processing operations and the nature of the data.

Art. 64. The rights and principles expressed in this Law do not exclude others provided in the Brazilian legal system related to the matter or in international treaties to which the Federative Republic of Brazil is a party.

~~**Art. 65.** This Law shall come into force eighteen (18) months following its official publication.~~

Art. 65. This Law shall come into force: (New Wording Given by Law No. 13,853/2019)

I – 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

I-A – August 1st, 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 other articles." (Included by Law No. 13,853/2019)

Brasília, August 14, 2018.