Congreso Nacional
H. Cámara de Diputados

LAW N°.....

ON THE PROTECTION OF PERSONAL DATA IN THE REPUBLIC OF PARAGUAY

- -

THE CONGRESS OF THE PARAGUAYAN NATION HEREBY ENACTS WITH FORCE OF LAW

L E Y :

TITLE I
GENERAL PROVISIONS

Chapter I
Object and scope of application.

Article 1°.- Purpose of the law.

The purpose of this law is the comprehensive protection of the personal data of natural persons in order to guarantee the full exercise of their rights and the free flow of information, in accordance with the provisions of the Constitution, international treaties, agreements and conventions to which the Republic of Paraguay is a party.

Article 2°.- Scope of Application.

1. The present law applies to any processing of personal data, totally or partially automated, as well as to non-automated processing when it concerns personal data that form part of a file, or are intended to be so, carried out by natural or legal persons, regardless of the medium, country of their headquarters or the country where the data are located, in the following cases:

a) By a controller or processor established in the Republic of Paraguay, even if the processing is carried out in another country;

b) By a controller or processor not established in national territory, in the following cases:

i. When performing data processing of natural persons located in Paraguayan territory, except in cases of transit purposes;

ii. when the data processing activities are related to the offer of goods or services directed to residents of the Republic of Paraguay;

iii. when the data processing activities are related to the control of the behavior of natural persons, insofar as it takes place in the territory of the Republic of Paraguay.

Congreso Nacional
H. Cámara de Diputados

2. The present law shall not apply in the following cases:

a) To the processing of personal data when they are intended for activities exclusively within the framework of the family or domestic life of a natural person, which are not intended for commercial disclosure or use;

b) To the processing of data intended for the purpose of public security, relating to migration, defense, national security and its activities in criminal matters, investigation and suppression of crime.

Article 3°.- Definitions.

For the purposes of this law, the following definitions are considered:

1. **Anonymization:** The application of measures of any nature aimed at preventing the identification or re-identification of a natural person.

2. **Data blocking:** The identification and reservation of personal data, adopting technical and organizational measures, to prevent its processing, including its visualization, except for making the data available to judges and courts, public prosecutors and other competent public authorities, in the manner and under the conditions established in the regulations in force.

3. **Consent:** Any free, express, specific, informed and unequivocal manifestation of will by which a natural person accepts and authorizes, either by a declaration or a clear affirmative action made in writing or by electronic means, as well as by any equivalent form that technology allows, the processing of personal data concerning him/her.

4. **Biometric data:** Personal data obtained from a specific technical processing, relating to the physical and/or physiological characteristics of a natural person, allowing or confirming the unique identification of such person, such as facial images, iris recognition or dactyloscopic data.

5. **Genetic data:** Personal data relating to inherited or acquired genetic characteristics of a natural person that provide unique information about that person's physiology or health, obtained in particular from the analysis of a biological sample of that person.

6. **Personal data:** Information of any kind relating to specific or identifiable natural persons. Determinable shall be understood as a person who can be identified, directly or indirectly, by means of an identifier or by one or more characteristic elements of the physical, physiological, genetic, psychological, economic, cultural or social identity of such person.

7. **Sensitive personal data:** Those referring to racial or ethnic origin; religious, philosophical and moral beliefs or convictions; union or political affiliation; data related to health, sexual preference or orientation, genetic data or biometric data aimed at univocally identifying a natural person and all those data whose improper use may give rise to discrimination or entail a serious risk for the holder.

Congreso Nacional
H. Cámara de Diputados

8. Profiling: The result of the automated and semi-automated processing of personal data to evaluate certain aspects of a natural person, to analyze or predict issues related to professional or work performance, economic situation, health, personal preferences, behaviors, interests and others that may be contemplated in the Regulation.

9. Processor: The natural or legal person, public or private, or other body or agency that processes personal data on behalf of or under a mandate from the controller.

10. Data protection impact assessment: Prior analysis of those data processing operations that may pose a risk to the rights and freedoms of individuals.

11. Personal data security incident: An incident resulting in the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the unauthorized communication of or access to such data.

12. Controller: The natural or legal person, public or private, or other body which, alone or jointly with others, determines the purposes and means of data processing.

13. Third party: Natural or legal person, national or foreign, public or private, other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process personal data.

14. Data subject: Natural person to whom the personal data refer or to whom the personal data correspond.

15. International data transfer: Transfer of personal data between two or more natural or legal persons (data controllers or processors) in which one of the legal entities is based in a jurisdiction outside the Republic of Paraguay.

16. Processing: Any operation or set of operations carried out by means of manual, automated or partially automated procedures, performed on personal data, related, but not limited to, obtaining, accessing, collecting, recording, registering, organizing, structuring, adapting, indexing, modifying, extracting, consulting, storing, keeping, blocking, processing, transferring, assigning, disseminating, possessing, exploiting and, in general, any use or disposal of personal data.

Article 4.- General principles of personal data protection.

The processing of personal data is governed by the following principles:

a) Principle of data accuracy: The data shall be accurate. The accuracy of the data provided by its owner is presumed. The data processed shall accurately reflect the information provided by the data subject. Data controllers and data processors must take all reasonable steps to ensure that the data is kept up to date and that inaccurate data is deleted or rectified without delay.

b) Principle of lawfulness: Personal data must be processed in a lawful and fair manner, in accordance with the provisions and principles established by law.

Congreso Nacional
H. Cámara de Diputados

The data controller must be able to prove the lawfulness of the processing of personal data it carries out.

c) Principle of purpose: Personal data must be collected and processed for specified, explicit, legitimate and time-limited purposes, and shall not be further processed in a manner incompatible with or different from those purposes.

Further processing for archiving and public interest purposes, scientific and historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes, provided that measures are taken to ensure that the principle of minimization of personal data is respected.

d) Principle of minimization or proportionality: The personal data processed must be strictly limited to that which is necessary, adequate and relevant in relation to the purposes of the processing and may be kept only for the period of time necessary to fulfill the purposes of the processing. The regulations shall determine the cases in which, by way of exception and in view of historical, statistical, scientific or administration of justice values, personal data may be kept even when such need or relevance has ceased to exist.

e) Principle of fairness and transparency: Personal data must be processed in a fair and transparent manner in relation to the data subject.

The data controller must provide the data subject, in clear and simple language, with all the information on the existence and main characteristics of the personal data. information on the existence and main characteristics of the processing to which their data will be subjected, as well as the necessary information for the exercise of the rights established in this law. This information must be permanently accessible, by easily accessible means to the data owner.

f) Principle of reconciliation of public transparency and protection: The obligation of publicity of acts of State Agencies and Entities shall take into account the principles of personal data protection established in the present law and, in particular, the principle of minimization. The publication and dissemination of personal data whose inclusion is necessary and proportional to the purpose of transparency pursued by means of publicity in the specific case shall be allowed. Personal data that exceed such purpose, or whose publication is not necessary, shall be excluded or crossed out from the acts or documents to be published. The publication of sensitive data is prohibited.

g) Due diligence principle: The person responsible for the database or processing and the person in charge, if applicable, must adopt appropriate measures, including privacy by design, privacy by default, data protection impact assessment, appointment of a data protection officer, among others, in order to ensure an adequate processing of personal data and demonstrate its effective implementation.

h) Principle of security and confidentiality: In the processing of personal data, technical and organizational measures must be adopted to ensure the security of the data, with the purpose of preventing accidental alteration, loss, destruction or damage, unauthorized or unlawful processing or access. In the case of data defined as sensitive, additional measures may be adopted to ensure their security, which will be determined in the regulations of this law.

i) Those responsible for and in charge of the processing of personal data, as well as any person intervening in any phase thereof, shall be subject to the duty of confidentiality, an obligation that shall subsist even after the termination of their relationship with the owner. They may be relieved of the duty of confidentiality by judicial decision or legal obligation.

TITLE II
PROCESSING OF PERSONAL DATA

Chapter I
On the legal basis for the processing of personal data.

Article 5°.- Conditions.

The processing of personal data may only be carried out if at least one of the following conditions is met:

1. The owner of the data grants his consent, for one or more specific purposes, in accordance with the provisions of this law;

2. The processing is necessary for compliance with a legal obligation on the part of the data controller;

3. The processing and shared use of necessary and proportional data, by the powers of the State, public companies and companies with majority State participation, for the exercise of their own functions, the implementation of public policies provided for in laws and regulations subject to the provisions of this law;

4. When the processing of personal data is necessary for the execution of a contract or preliminary procedures related to a contract to which the holder is a party, at his request;

5. When it is necessary for the regular exercise of rights in judicial, administrative or arbitration proceedings;

6. The processing is necessary for the satisfaction of legitimate interests pursued by the data controller or by a third party, except when the interests or fundamental rights and freedoms of the data owner prevail over such interests, which require the protection of personal data, in particular when the data owner is a child and/or adolescent. This paragraph shall not apply to the processing of personal data by the State;

7. For the protection of life, physical or psychological safety and/or the protection of the health of the data subject or a third party, exclusively, in a procedure carried out by health professionals, health services or health authority, or for the legal protection of a natural person ordered by a competent authority in judicial proceedings.

The regulation shall determine the corresponding measures according to the types of data, treatments and responsible parties, as well as the opportunity for its revision and updating.

Article 6°.- Conditions for consent.

Congreso Nacional
H. Cámara de Diputados

If the legal basis for the processing of personal data is consent, such consent must be prior, free, informed and unequivocal, for one or more specific purposes, either by means of a statement or a clear affirmative action.

If the data subject's consent is given in the context of a written statement that also relates to other matters, the request for consent shall be presented in such a way as to be clearly distinguishable from the other matters, in an intelligible and easily accessible form and using clear and plain language. A statement or part thereof in breach of this Act shall not be binding.

The data subject shall have the right to withdraw his or her consent at any time and shall be informed thereof before giving his or her consent. The data controller shall establish simple, agile, effective and free mechanisms for the exercise of this right, which may not exceed in complexity those processes established for giving consent. Withdrawal of consent shall not affect the lawfulness of the processing carried out on the basis of consent prior to its withdrawal.

In all cases, the controller has the burden of proving that the data subject consented to the use of his or her personal data.

Article 7. - Consent of children and adolescents.

In the processing of personal data of a child or adolescent, the protection of their best interests must be prioritized, in accordance with the Convention on the Rights of the Child and other international instruments signed and ratified by the Republic of Paraguay and national laws.

Adolescents, once they have reached the age of fourteen, may validly consent to the processing of their personal data, except in the case of sensitive personal data, in which case their legal representatives must intervene.

The processing of personal data of those who have not reached the age of fourteen, based on consent, will only be lawful if the consent of the holder of parental authority, guardianship or guardianship of the same is recorded, with the scope determined by the same.

The information on consent and data processing referred to in this article must be provided in a simple, clear and accessible manner, considering the physical-motor, perceptive, sensory, sensory, intellectual and mental characteristics of the data owner or his/her legal representative, with the use of audiovisual resources when appropriate.

Congreso Nacional
H. Cámara de Diputados

Article 8°.- Legitimate interest.

The legitimate interest of the data controller or that of a third party constitutes a legal basis for the processing of personal data, provided that the processing is necessary for the satisfaction of such interest and provided that the fundamental rights and freedoms of the data owner do not prevail.

Processing based on legitimate interest must always take place within the framework of a relevant and appropriate relationship between the data subject and the controller, and be in accordance with the reasonable expectations of the data subject.

The data controller must process the data strictly necessary and take measures to ensure the transparency of such processing, informing the data subject of the legitimate interest pursued.

the supervisory authority may require from the controller a prior analysis on the protection of personal data, justifying its legitimate interest and the need to collect or process the data in each case, observing commercial and industrial secrets.

The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data based on the legitimate interest of the controller.

Chapter II
Obligations of the data controller and data processor.

Article 9. - Data Controller.

Taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is in compliance with this law and its regulations. Such measures shall be reviewed and updated as necessary.

The regulation shall determine the measures that correspond according to the types of data, processing and controllers, the opportunity for their review and updating, as well as the protection measures by design and by default.

Article 10.- Joint controllers.

When two or more controllers jointly determine the purposes and means of the processing, they shall be considered jointly responsible for the processing. The joint controllers shall determine inter partes in a transparent manner and by mutual agreement their respective responsibilities in the fulfillment of the obligations imposed by the present law. Such agreements, although they may designate a common point of contact for data subjects, shall not exonerate the joint controllers from their joint responsibility vis-à-vis the data subject.

Regardless of the terms of the agreement referred to in the preceding paragraph, data subjects may exercise their rights against and against each of the data controllers, jointly or separately.

Congreso Nacional
H. Cámara de Diputados

Article 11.- Data processor.

Where processing is to be carried out on behalf of a data controller, the latter shall choose only processors who offer sufficient guarantees to implement appropriate technical and organizational measures, so that the processing complies with the requirements of this Act and ensures the protection of the data subject's rights.

The processing by the processor shall be governed by a contract or other legal act in accordance with the legal system, which binds the processor vis-à-vis the controller and establishes the subject matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

The processor may have recourse to another processor. In the event of non-compliance by the other processor, the initial processor shall remain fully liable to the controller for compliance with the other processor's obligations.

If a processor determines the purposes and means of such processing, in breach of this law, he shall be held liable in respect of such processing.

Article 12.- Representatives of controllers or processors not established in the Republic of Paraguay.

The regulations of this Law shall establish the cases and conditions in which it shall be mandatory for data controllers or processors to appoint a representative.

The representative may respond to the request made by the data owner as well as to that of the supervisory authority.

Article 13. Binding self-regulatory mechanisms.

The supervisory authority shall promote the development of binding self-regulatory mechanisms, the purpose of which shall be to contribute to the correct application of this law.

The binding self-regulatory mechanisms may consist of codes of conduct, good practices, binding corporate rules, trust seals, certifications or other mechanisms that contribute to the aforementioned objectives, and the regulations may establish the necessary requirements for their approval by the supervisory authority. The codes of conduct may include mechanisms for the extrajudicial resolution of conflicts, but the use of the latter must not entail additional costs for the data owner or oblige him to travel disproportionately far from the location of his domicile.

Article 14.- Impact assessment.

Prior to the implementation of data processing operations which, due to their nature, scope, context or purposes, may pose significant risks to the rights of data subjects, the data controller shall carry out an assessment of the impact of such operations on the protection of personal data.

The impact assessment relating to data protection is mandatory, in case of:

a) Systematic and comprehensive evaluation of personal aspects of natural persons that is based on automated data processing, including profiling, and on the basis of which decisions are made that produce legal effects for natural persons or significantly affect them in a similar way;

b) Large-scale processing of sensitive data, or of personal data relating to criminal convictions and offenses; or,

c) Systematic processing on a large scale for the observation of a publicly accessible area.

The supervisory authority shall establish and publish a list of the types of processing operations requiring a data protection impact assessment in accordance with the first paragraph of this Article. The supervisory authority may also establish and publish a list of the types of processing operations that do not require a data protection impact assessment.

The content of the impact assessment shall be established in the regulations of this law.

Article 15. Prior consultation.

The controller shall consult the supervisory authority before proceeding with the processing where an impact assessment demonstrates that the processing would entail a risk if the controller does not take measures to mitigate it.

The controller may not start processing data until the supervisory authority has given its opinion on the report.

The supervisory authority shall, within 30 (thirty) working days of the consultation, advise the controller or processor in writing, in accordance with the duties set forth in this law. These deadlines may be suspended until the supervisory authority has obtained the information requested for the purposes of the consultation.

Article 16.- Security measures.

The controller and the processor shall carry out a series of actions that guarantee the establishment, implementation, operation, monitoring, review, revision, maintenance and continuous improvement of the security measures applicable to the processing of personal data, on a periodic basis.

The supervisory authority shall regulate the minimum technical security and integrity conditions to be applied by data controllers and processors.

Article 17.- Notification of a security incident of the processing of personal data to the supervisory authority and to the data subject.

In the event of a personal data security incident, the data controller shall notify the supervisory authority and, where appropriate, the data subject, without undue delay , within the term, conditions and with the requirements that shall be established in the regulations of this Law.

Article 18.- Data Protection Officer.

Data controllers and data processors shall appoint a data protection officer in the cases to be established in the regulations of this law.

The data protection officer shall be appointed on the basis of his or her professional qualities and ability to perform the functions to be established in the regulations of this Law.

A business group may appoint a single data protection officer provided that he or she is easily accessible from each establishment.

Where the controller or processor is a public authority or body, a single data protection officer may be appointed for several such authorities or bodies, taking into account their organizational structure and size.

The data protection officer may be part of the staff of the controller or processor or perform his or her duties under a service contract.

The regulations shall lay down other aspects relating to the data protection officer.

Chapter III International transfer of data.
On the international transfer of data.

Article 19.- General rules for international transfers of personal data.

Transfers of personal data outside the national territory, including onward transfers, may be made only if the recipient country maintains adequate levels of protection in accordance with this law.

In the event that the recipient country does not have an adequate level of protection, the controller or processor must take all necessary steps to ensure that the processing of personal data is carried out in accordance with the provisions of this law.

The provisions of the preceding paragraph do not apply in the following cases:

1. Agreements within the framework of international treaties to which the Republic of Paraguay is a party;

2. International judicial cooperation;

3. International cooperation between intelligence agencies for the fight against terrorism, illicit drug trafficking, money laundering, corruption, trafficking in persons and other forms of organized crime;

4. When the personal data is necessary for the execution of a contractual relationship in which the personal data holder is a party, including what is necessary for activities such as user authentication, service improvement and support, service quality monitoring, support for account maintenance and billing and those activities that the management of the contractual relationship requires;

5. In the case of bank or stock exchange transfers, in relation to the respective transactions and in accordance with the applicable law;

Congreso Nacional
H. Cámara de Diputados

6. When the cross-border flow of personal data is carried out for the protection, prevention, diagnosis or medical or surgical treatment of the holder; or when it is necessary for the performance of epidemiological or analogous studies, as long as adequate anonymization procedures are applied;

7. When the owner of the personal data has given prior, informed, express and unequivocal consent;

8. When the data controller offers and accredits guarantees of compliance with the principles, the rights of the data subject and the data protection regime provided for in this law, in the form of:

a) Specific contractual clauses for a particular transfer;

b) Standard contractual clauses;

c) Global corporate standards;

d) Periodically issued seals, certificates and codes of conduct.

The regulations of this law shall establish the other cases in which data controllers or data processors are exempted from the provisions of this paragraph, always within the principles, guidelines and purposes pursued by this law.

Chapter IV.
Processing of certain categories of data.

Article 20.- Processing of sensitive data.

The processing of sensitive personal data is prohibited unless:

1. The owner has given his consent to the processing of such personal data, except where it is established that the aforementioned prohibition cannot be lifted by the consent of the data owner; such consent shall have no value if obtained within the framework of asymmetrical relationships, where the granting of consent has been directly or indirectly imposed on the data owner;

2. The processing relates to personal data which the data subject has manifestly made public;

3. The processing is necessary for the performance of obligations and the exercise of specific rights of the controller or of the data subject in the field of labor and social security law, to the extent authorized by law and provided that adequate safeguards are in place to ensure respect for the fundamental rights of the data subjects;

4. The processing is necessary to protect the vital interests of the data subject, in the event that the data subject is physically or legally incapable of giving his consent, and his legal representatives are unable to give their consent in a timely manner;

5. The processing is carried out, within the scope of its legitimate activities and with due guarantees, by a foundation, an association or any other non-profit organization,

whose purpose is political, philosophical, religious or trade union, provided that the processing relates exclusively to the current members of such organizations or to persons who maintain regular contacts with them in connection with their purposes and provided that the personal data are not communicated outside them without the consent of the data subjects;

6. The processing is necessary for the formulation, exercise or defense of claims or when the competent jurisdictional authorities act in the exercise of their judicial function;

7. Processing is necessary for reasons of public interest in the field of public health by the competent health authority, such as protection against serious cross-border threats to health, or to ensure high standards of quality and safety of healthcare or food provision and of medicinal products or medical devices or foodstuffs, where appropriate and specific measures must be laid down to protect the rights and freedoms of the data subject, in particular professional secrecy;

8. The processing is necessary for the purposes of preventive or occupational medicine, assessment of the worker's working capacity, medical diagnosis, provision of health or social care or treatment, or management of the health and social care service systems, in compliance with special regulations or pursuant to a contract with a health care professional. The personal data covered by this paragraph may be processed whenever they are processed by or under the responsibility of a professional subject to the obligation of professional secrecy or confidentiality, or by any other person subject to the obligation of secrecy in accordance with the law;

9. The processing is carried out in the context of humanitarian assistance in cases of natural disasters;

10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, which must be proportionate to the purpose pursued, respect in substance the right to data protection and provide for adequate and specific measures to protect the interests and fundamental rights of the holder. The data must be effectively anonymized;

11. The processing and sharing of necessary and proportional data, by the powers of the State, for the exercise of their own missionary functions, the implementation of public policies provided for in laws and regulations.

Article 21.- Processing of credit information data.

The protection of credit data, the regulation of the activity of collection and access to credit information data, as well as the constitution, organization, operation, rights, obligations and extinction of legal entities engaged in the collection and provision of credit information shall be governed by the specific law in force in this regard.

Except for the functions and attributions expressly assigned to the Central Bank of Paraguay, the other functions and attributions required for the implementation of the law regulating credit data shall be exercised by the control and supervisory authority of the present law.

Congreso Nacional
H. Cámara de Diputados

The present law shall be of supplementary application for matters not provided for in the law regulating credit data, provided that such matters are compatible with the nature of such information.

Article 22.- Processing for video-surveillance purposes.

Natural or legal persons, whether public or private, may carry out the processing of images through camera or video camera systems for the purpose of preserving the security of persons and property, as well as of their facilities.

Images of the public highway may only be captured to the extent that it is essential for the purpose mentioned in the previous paragraph.

However, it will be possible to capture images of the public road in a greater extension when it is necessary to guarantee the security of goods or strategic installations or infrastructures linked to transport, but in no case may it imply or imply the capture of images of the interior of a private home.

The data that would have to be kept to prove the commission of acts against the integrity of persons, goods or facilities must be made available to the competent authority to take action in the investigation and prosecution of criminal and/or administrative offenses within a maximum period of 72 hours (seventy-two hours) from the time the existence of the recording is known, without prejudice to the powers of investigation of the competent authorities within the framework of an open investigation.

The processing by a natural person of images that only capture the interior of his own home is excluded from the scope of application of this article.

This exclusion does not apply to the processing carried out by a private security entity that has been contracted for the surveillance of a home and has access to the images.

Article 23.- Processing of data of a criminal nature, sanctions and administrative offenses.

The processing of personal data relating to punishable acts, as well as related precautionary and security procedures and measures, shall be governed by the respective law.

The processing of data related to administrative infractions and sanctions shall be governed by the respective law.

Technical and organizational measures shall be in place to ensure compliance with the principle of minimization and other personal data protection principles and provisions.

Congreso Nacional
H. Cámara de Diputados

Chapter V
Data processing in the public sector.

Article 24.- Access to Public Information and Data Protection.

The right of access to information held in public sources may be denied or limited, when such a measure is necessary to avoid a concrete prejudice to the protection of one of the private interests inherent to the protection of personal data, in accordance with the provisions of this law and in accordance with the procedure provided for in this article.

If the State agency or entity to which the request for access to information is addressed notices that the same could interfere with the right to the protection of personal data, it shall notify the owner of the data concerned, within a period not exceeding five (5) days of receipt of the request. Failing that, the State agency or entity shall issue a decision regarding the request of the data subject within fifteen 15 (fifteen) days, in accordance with the provisions of Law No. 5282/2014 "ON FREE CITIZEN ACCESS TO PUBLIC INFORMATION AND GOVERNMENT TRANSPARENCY".

The owner of the data shall have a period of 5 (five) days to submit reasoned opposition to the access request made with respect to the personal data concerning him/her.

In the event that the data owner files an objection based on the right to the protection of his personal data, within the legal term, the State entity or body receiving the request for access shall request a non-binding opinion from the supervisory authority on the compatibility of the request for access to the information with an adequate level of protection of personal data. The supervisory authority shall issue its opinion within 10 working days.

State agencies and entities shall have a term of fifteen (15) days to resolve the request for access to information. If there is no objection, the period shall start to run from the expiration of the term the data owner had to file it; and, if there is an objection, from the receipt of the opinion from the supervisory authority or from the expiration of the legal term he had to file it.

If the request for access is deemed admissible despite the data owner's opposition, the State entity or body shall notify the data owner and transmit the requested data or documents to the applicant within a period not exceeding ten (10) days.

In cases of total or partial denial of access or lack of response within the indicated term, the applicant shall have expeditious legal action, under the terms of Title V of Law No. 5282/2014 ON FREE CITIZEN ACCESS TO PUBLIC INFORMATION AND GOVERNMENT TRANSPARENCY.

Article 25.- Exchange of personal data between public institutions.

The communication of personal data between public institutions shall be lawful, to the extent that:

1. The public institution responsible for the database has obtained the data in the exercise of its legally attributed functions and powers;

2. The processing by the public institution receiving the database is necessary for the fulfillment of its legal functions and the purpose of such data processing is within the framework of its competences;

Congreso Nacional
H. Cámara de Diputados

3. The data involved are adequate, proportional and do not exceed the limit of what is necessary in relation to the latter purpose;

4. The owner of the sensitive data has given his consent or the exceptions set forth in article 20 of this law apply.

TITLE III

OF THE RIGHTS RELATED TO PERSONAL DATA

Sole Chapter

On the rights of data owners.

Article 26.- General provisions on the exercise of rights.

Without prejudice to the other rights deriving from the provisions of this law, the data owner or his representative may, at any time, request from the data controller, access, rectification, erasure, objection and portability of the personal data concerning him.

The exercise of any of the aforementioned rights is not a prerequisite nor does it prevent the exercise of any other right.

The data controller shall establish simple, expeditious, accessible and free of charge means and procedures that allow the data owner to exercise his or her rights.

The data controller shall have a term of 30 (thirty) calendar days computed from the submission of the request to provide a response.

Upon expiration of the term without satisfying the request or if, in the opinion of the data owner, the response is insufficient, the data owner may appeal to the supervisory authority or, if appropriate, may file a habeas data action. In the event of opting for the habeas data action, or of having initiated it previously, he/she may not initiate the procedure before the supervisory authority.

The exercise of the rights provided for in this Chapter cannot be waived.

Article 27.- Right to information.

The data owner has the right to receive sufficient and easily accessible information, in clear, simple and easily understandable language, particularly if it is addressed to children and adolescents or persons with physical, mental or psycho-social disabilities, on how the processing of their personal data is carried out, whether they have provided it directly or not.

The data controller shall provide the data subject, at the time the data is collected, with at least the following information:

1. The categories of personal data that will be the subject of the processing;

2. The identity and contact details, which will be at least the legal address, telephone number and e-mail or equivalent channel;

Congreso Nacional
H. Cámara de Diputados

3. Legal basis and purposes of the processing to which your personal data will be subjected;

4. The communications or international transfers of personal data that the controller intends to make, including the recipients or categories of recipients and the purposes for which they are to be made;

5. The existence, form and mechanisms or procedures through which you may exercise your rights of access, rectification, opposition, deletion and portability;

6. Time of conservation of personal data, or in its absence, the criteria used to determine the period of time;

7. The existence of automated decisions, including profiling and, at least in such cases, significant information on the logic applied, without affecting the intellectual rights of the data controller;

8. Where appropriate, the origin of the personal data when the controller has not obtained them directly from the data subject;

9. The right to appeal to the supervisory authority.

The information provided, as well as the communication and any action taken must be free of charge. Where requests are manifestly unfounded or excessive, especially due to their repetitive nature, the controller may: **a)** charge a reasonable fee based on the administrative costs incurred in providing the information or communication or performing the requested action, or **b)** refuse to act on the request.

The controller shall bear the burden of proving the manifestly unfounded or excessive nature of the request.

The data controller shall keep a detailed record of the requests refused and the reasons for such refusal.

Article 28.- Right of access.

The data owner shall have the right to request and obtain access to his personal data held by the data controller and/or a copy thereof, subject to proof of identity. The information shall be provided in a clear, intelligible form, free of codifications and, if necessary, accompanied by an explanation of the terms used, in language accessible to the average knowledge of the population.

In no case may the report reveal data belonging to third parties, even when linked to the owner of the data, unless they have been provided by the owner himself.

Congreso Nacional
H. Cámara de Diputados

Article 29.- Right of rectification.

The data owner shall have the right to obtain from the data controller the rectification of his personal data, when they prove to be inaccurate, incomplete or outdated.

In the event of assignment or international transfer of erroneous or outdated data, the data controller must notify the rectification to the transferee within the fifth working day of having become aware of the error or outdatedness.

During the process of verification and rectification of the error or falsity of the information in question, the data controller must block the data, or else state, when providing information relating thereto, the circumstance that it is subject to review.

Article 30.- Right to object.

The data subject shall have the right to object, at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her, including profiling based on such provisions.

Where the data subject objects to the processing of his or her personal data, the processing shall cease within 10 (ten) working days from the sending of the objection request, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or the processing is necessary for the establishment, exercise or defense of a right in legal proceedings.

Where the data subject objects to the processing for direct marketing purposes, including profiling insofar as it is related to such marketing, his or her personal data shall cease to be processed for such purposes within 15 (fifteen) working days from the sending of the objection request.

Article 31.- Right of suppression.

The data owner shall have the right to obtain from the data controller the deletion of his or her personal data without undue delay, in order for the same to cease to be processed by the latter, in the following cases:

1. When the personal data have been unlawfully processed;

2. When the personal data are no longer necessary in relation to the purpose for which they were collected or processed;

3. When the term of conservation of the personal data has expired;

4. When the data owner has revoked the consent on which the processing is based and there is no other lawful basis for the processing;

5. When the data owner has exercised his or her right to object in accordance with the provisions of this law, and no other legitimate grounds for the processing of his or her data prevail;

6. Personal data that must be deleted in order to comply with a legal obligation.

Congreso Nacional
H. Cámara de Diputados

Deletion shall not proceed when it could cause prejudice to the right to information and freedom of expression or legitimate interests of third parties duly proven; when duly proven reasons of public interest prevail for the processing of questioned data, or the personal data must be kept for the periods provided for in the applicable mandatory legal provisions.

Article 32.- Right to portability.

When personal data is processed electronically or by automated means, the data owner may request that his or her personal data be transferred directly from controller to controller in accordance with the technical regulations.

This right shall not apply when:

1. Its exercise imposes a duly demonstrated excessive or unreasonable financial or technical burden on the data controller or processor;

2. Infringes the privacy of another data subject;

3. It violates legal obligations that may be imposed on the data controller or processor;

4. It concerns data that have already been anonymized by the data controller.

Article 33.- Rights in the face of automated or semi-automated individual decisions.

The data subject has the right to request the review of decisions taken on the basis of automated or semi-automated processing of personal data, which adversely affect his interests or produce legal effects, including decisions aimed at defining his personal, professional, consumer, credit, and personality aspects. They also have the right to express their point of view and to challenge the decision.

The data controller must provide, whenever requested, clear, complete and adequate information on the criteria and procedures used for the automated or semi-automated decision, in compliance with the respect for commercial and industrial secrets of the data subject or which the data subject is obliged by law or contract to keep.

It must take appropriate measures to safeguard the rights of the Data Subject.

This right does not suppress or replace the exercise of other rights that may take place.

Congreso Nacional
H. Cámara de Diputados

TITLE IV

OF THE CONTROL AND SUPERVISORY AUTHORITY AND ITS POWERS

Chapter I

The Control and Supervisory Authority.

Article 34.- Control and supervisory authority. Legal nature.

The National Agency for the Protection of Personal Data is hereby created as a deconcentrated unit within the organic structure of the Ministry of Information and Communication Technologies, with the rank of General Directorate, which is constituted as the control and supervisory authority of the present law.

The National Agency for the Protection of Personal Data shall enjoy functional autonomy and independence, and shall have sufficient powers of decision, action, regulation, supervision, control, sanction and all other functions necessary for compliance with this law, acting in accordance with the principles set forth herein.

The National Agency for the Protection of Personal Data shall have broad powers to organize itself administratively. It shall have the human and material resources necessary for the fulfillment of its functions.

The organizational and administrative structure of the National Agency for the Protection of Personal Data shall be established in the regulatory decree of the present law and shall comprise, at least, the Director General as the highest authority and a deputy.

The National Agency for the Protection of Personal Data shall have broad powers to issue such internal regulations as may be necessary to supplement the regulatory provisions expressly mentioned in this law.

Article 35.- Functions and Powers of the National Agency for the Protection of Personal Data.

The National Agency for the Protection of Personal Data is constituted as the controlling authority of this law and has sufficient powers and attributions of action, decision, resolution, regulation, promotion, investigation, supervision, oversight, control, sanction and others that may be necessary to guarantee its effective compliance, as well as the effective exercise and respect of the right to the protection of personal data.

The National Agency for the Protection of Personal Data shall have the following functions and powers:

1. Exercise the supervision, control and evaluation of the activities carried out by the person responsible and in charge of the processing of personal data;

2. To assist and advise the persons who so require about the scope of the present law and the legal means available to them for the defense of their rights;

3. To dictate the rules, regulations, guidelines and guiding criteria to be observed in the development of the activities included in the present law;

Congreso Nacional
H. Cámara de Diputados

4. To process the claims and/or complaints filed, to carry out preliminary proceedings and, if deemed appropriate, to institute administrative proceedings for alleged non-compliance with the present law and its regulatory provisions;

5. Conduct technical audits of the processing of personal data, in accordance with this law and the regulations;

6. To request information corresponding to its area of competence from public and private institutions, which shall respond within the term established for such purpose;

7. To impose administrative sanctions, prior administrative summary, for violation of the provisions of the present law and its regulations;

8. To homologate binding self-regulation mechanisms or codes of conduct and supervise their compliance;

9. To dictate standard data protection clauses;

10. To draw up and maintain a list relating to the requirement of data protection impact assessment;

11. Create data protection certification mechanisms, in order to provide the established guarantees;

12. Assess the adequacy of the recipient country or agency in the international transfer of data;

13. Request information from data protection officers, under the terms provided for in this law and its regulatory provisions;

14. Promote cooperation actions with personal data protection authorities of other countries, being able to sign international administrative and non-regulatory agreements on the matter;

15. To issue a non-binding technical opinion when the right of access to public information and the right to the protection of personal data must be weighed in administrative or judicial proceedings, when there are doubts about their application;

16. Prepare annual management reports on its activities;

17. To collaborate with State agencies and entities in matters related to its competence;

18. The other functions assigned to it by this law or its regulatory decree, as well as those that may be necessary to guarantee the effective implementation and compliance with this law.

Article 36.- On the financial resources of the National Agency for the Protection of Personal Data.

The financial resources of the National Agency for the Protection of Personal Data shall be made up of the following:

1. The resources annually allocated to it in the General Budget of the Nation, which shall be incorporated into the budget of the Ministry of Information and Communication Technologies, and shall be fully individualizable therein;

2. Revenues from fines applied in the exercise of its sanctioning powers established in this law;

3. Funds from agreements and/or accords, credits granted, loans, financing, contributions, donations, legacies, or any other concept, of national or international origin, as long as it does not imply a conflict of interest.

The income listed in numeral 2 shall be deposited in a special account of the Ministry of Information and Communication Technologies exclusively destined to the resources of the National Agency for the Protection of Personal Data.

In no case shall the aforementioned resources be used for any purpose other than that set forth in this law and its regulations.

Chapter II
The Directorate of the National Agency for the Protection of Personal Data.

Article 37.- Appointment of the Director General of the National Agency for the Protection of Personal Data.

The National Agency for the Protection of Personal Data shall be headed by a Director General. The Director General shall be assisted by a Deputy to whom he may delegate his functions in the manner and under the conditions set forth in the law and the corresponding regulations.

The General Director and the Deputy shall be appointed by decree of the Executive Power, from a list of three candidates proposed by the Ministry of Information and Communication Technologies, after a merit-based competition.

The Agency shall exercise its functions with exclusivity, independence and objectivity, the hierarchical power of the highest authority of the Ministry of Information and Communication Technologies being limited to those matters that are not related to the functions of exclusive competence of the National Agency for the Protection of Personal Data, except in the case of administrative summary proceedings.

Article 38.- Functions of the Director General of the National Agency for the Protection of Personal Data.

It is incumbent upon the Director General of the National Agency for the Protection of Personal Data:

Congreso Nacional
H. Cámara de Diputados

1. To comply with and ensure compliance with the present law and its regulatory provisions;

2. To exercise the regulatory power under the terms provided for in this law;

3. To direct and organize the structure and functions of the Agency, issuing the internal regulations and manuals that may be necessary for such purpose;

4. Exercise the representation of the National Agency for the Protection of Personal Data, being able to sign documents and grant general and special powers of attorney for judicial and administrative actions on behalf of the same;

5. Appoint, remove or transfer the personnel of the Agency and set office hours and work shifts, in accordance with the provisions of the respective regulations;

6. To enter into contracts, agreements, with national, binational, international, public or private institutions and organizations, for the fulfillment of the objectives and purposes of the Agency and of the present law;

7. To order inspections and/or technical or administrative inspections and/or audits to the subjects subject to the present law;

8. To order the instruction of administrative summaries and the application of sanctions when, as a consequence thereof, they may be pertinent;

9. To perform any other function related to the protection of personal data within the framework of the provisions of this law.

Article 39.- Requirements for the position of Director General of the National Agency for the Protection of Personal Data.

The following are the requirements to hold the position of Director General and Deputy Director General of the National Agency for the Protection of Personal Data:

1. Be of Paraguayan nationality, at least 30 (thirty) years of age;

2. Possess a university degree;

3. Have proven conditions of suitability, capacity and experience in the field of personal data protection, which ensure independence of judgment, efficiency, objectivity and impartiality in the performance of their duties;

4. To enjoy a good reputation and not to have been convicted for a punishable act that seriously affects the public concept of fame.

Article 40.- Term of office and removal.

The Director General of the National Agency for the Protection of Personal Data and the Deputy shall hold office for three (3) years, and may be reappointed for subsequent periods.

Likewise, they shall cease to hold office, prior to the expiration of their term of office, in the following circumstances:

Congreso Nacional
H. Cámara de Diputados

a) By removal motivated in bad performance of their duties. The administrative summary to verify the grounds for removal shall be processed in accordance with the provisions of the law governing the civil service;

b) Resignation submitted to the President of the Republic;

c) Supervening incapacity for the exercise of his or her functions;

d) Final conviction for the commission of a punishable act involving deprivation of liberty.

In no case shall the positions of General Director or Deputy Director of the National Agency for the Protection of Personal Data be considered positions of trust or subject to free disposition.

The Director General and the Deputy shall be personally liable for the consequences of their technical, administrative and financial management; and for any decision adopted in contravention of the legal and regulatory provisions.

TITLE V
ADMINISTRATIVE SUPERVISION
Chapter I
Misdemeanors and their consequences.

Article 41.- Administrative protection.

Without prejudice to the judicial action of habeas data, the owner of the data may file claims or complaints before the Agency in order to enforce his rights, in the manner and under the conditions provided for in the present law and in its regulations.

The Agency may initiate proceedings for the purpose of ascertaining compliance with the provisions of this law at the request of the owner of the Data, his legal or conventional representative, of a third party having a legitimate interest or ex officio.

In the proceedings, the provisions of this law, its regulations and the provisions of Law No. 6715/2021 "ON ADMINISTRATIVE PROCEEDINGS" or equivalent, as applicable, shall apply.

Without prejudice to the administrative protection, the holder may resort to judicial protection in order to be compensated when he/she has suffered damages as a consequence of a violation of his/her rights to the protection of personal data, in accordance with the provisions of this law.

Article 42.- Corrective measures.

In the event of non-compliance with the provisions of this Law, without prejudice to the administrative sanction that may be imposed, the Agency may issue corrective measures for the purpose of eliminating, avoiding or stopping the effects of the offenses, as well as deterring relapses.

The corrective measures may consist, among others, of:

1. The cessation or suspension of processing, under certain conditions or deadlines;

2. The deletion of data; and,

3. The imposition of technical, legal, and organizational measures that guarantee an adequate processing of personal data.

Article 43.- Conduct constituting misconduct.

Any action or omission that implies non-compliance with the provisions set forth in the law and its regulatory provisions, including those issued by the Agency, shall be considered a misdemeanor.

Misdemeanors are classified as minor and serious.

The administrative action motivated by the aforementioned conducts will be independent of the actions carried out in judicial instance in the cases of conducts typified in the Penal Code, as will be the sanctions or penalties applied in each case.

The appeal against the corrective measures shall not have suspensive effects on their execution.

Article 44.- Minor offenses.

The following offenses shall be considered minor offenses and shall be subject to a statute of limitations of one (1) year:

1. Collecting personal data for use in a database without sufficient and ample information being granted to the person concerned, in accordance with the technical specifications set forth in the implementing regulations of this law;

2. Collect, store and transmit personal data of third parties by means of insecure mechanisms or mechanisms that in any way do not guarantee the security and inalterability of the data;

3. Failure to comply with the rights of access, rectification, erasure, limitation of processing or data portability in processing operations in which the identification of the data subject is not required, when the data subject, in order to exercise these rights, has provided additional information that allows for his or her identification;

4. Failure by the processor to comply with the stipulations imposed in the contract or legal act regulating the processing or the instructions of the data controller, unless legally obliged to do so under other laws of the Republic of Paraguay and this law or in cases where it was necessary to prevent the infringement of data protection legislation and the data controller or processor had been warned of this;

5. Incomplete, late or defective notification to the supervisory authority of information related to a security breach of personal data in accordance with the provisions of this law;

6. Unjustifiably refusing to grant access to a data owner about his data contained in files and databases, in order to verify their quality, collection, storage and use in accordance with this law;

Congreso Nacional
H. Cámara de Diputados

7. The hiring by the data controller of a data processor that does not provide sufficient guarantees to implement appropriate technical and organizational measures in accordance with the provisions of this law and its regulations;

8. Failure to maintain available personal data protection policies related to the processing of personal data.

Article 45.- Serious misconduct.

The following infringements shall be considered serious offenses and shall be subject to the statute of limitations after 2 (two) years:

1. Transferring personal data to other persons or companies in contravention of the rules set forth herein.

2. Reiteration in the unjustified refusal to grant access to a holder of his data contained in files and databases, in order to verify their quality, collection, storage and use in accordance with this law.

3. Unjustifiably refusing to delete or rectify the data of a person who has so requested by clear and unequivocal means.

4. The processing of personal data of a minor without obtaining his or her consent, when he or she has the capacity to do so, or that of the holder of his or her parental authority or guardianship.

5. Failure to demonstrate that reasonable efforts have been made to verify the validity of the consent given by a minor or by the holder of parental authority or guardianship over the minor.

6. The impediment or hindrance or repeated non-observance of the rights of access, rectification, erasure or data portability in processing operations in which the identification of the data subject is not required, when the data subject, in order to exercise these rights, has provided additional information that allows his or her identification.

7. Failure to adopt those technical and organizational measures that are appropriate to effectively apply the principles of data protection from the design, as well as the failure to integrate the necessary safeguards in the processing.

8. Failure to adopt appropriate technical and organizational measures to ensure that, by default, only personal data necessary for each of the specific purposes of the processing will be processed.

9. Failure to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing.

10. The breach, as a consequence of the lack of due diligence, of the technical and organizational measures that have been implemented, in accordance with the provisions of this law.

Congreso Nacional
H. Cámara de Diputados

11. Failure to comply with the obligation to appoint a representative of the data controller or data processor not established in the Republic of Paraguay, in accordance with the provisions of article 12 of this law.

12. Entrusting the processing of data to a third party without the prior formalization of a contract or other written legal act, as required by this law.

13. The contracting by a data processor of other data processors without the prior authorization of the data controller, or without having informed the data controller of the changes in the subcontracting when legally required.

14. The breach of the duty of the processor to notify the data controller of any security breaches of which he/she becomes aware.

15. Failure to comply with the duty to notify the supervisory authority of a personal data security breach in accordance with the provisions of article 17 of this law.

16. The processing of personal data without having carried out the assessment of the impact of the processing operations on the protection of personal data in the cases in which it is required.

17. The processing of personal data without having previously consulted the supervisory authority in the cases in which the law establishes the obligation to carry out such consultation.

18. Failure to comply with the obligation to appoint a data protection officer when his or her appointment is required in accordance with article 18 of this law.

19. Failure to enable the effective participation of the data protection officer in all matters relating to the protection of personal data, failure to support him or her or interference in the performance of his or her duties.

20. The use of a false national or international data protection seal or certification or in the event that the validity of the same has expired.

21. Collecting, storing and transmitting personal data of third parties by means of insecure mechanisms or mechanisms that in any way do not guarantee the security and unalterability of the data.

22. Failure to comply with the obligation of notification by those responsible or in charge regarding the rectification or deletion of personal data required by articles 29 and 31 of this law.

23. Failure to comply with the requirements of this law in relation to the validity of consent.

24. The omission of the duty to inform the holder about the processing of his personal data in accordance with the provisions of article 27 of this law.

25. The requirement of payment of a fee for the exercise of any of the rights established in Title III, Sole Chapter of the rights of data owners.

26. Collect, store, transmit or in any other way use, by private individuals or legal entities, sensitive data, without having one of the legal bases established in the legislation in force.

27. Obtain, from the owners or third parties, personal data of a person by means of deceit, violence or threat.

28. Disclose information recorded in a personal database whose secrecy is required by law.

29. To provide a third party with false or different information contained in a data file, with knowledge of it.

30. Transferring, to the databases of third countries, personal information of Paraguayan inhabitants or foreigners residing in the country, without the consent of the owners when it is required.

31. The processing of personal data relating to criminal convictions and offenses or related security measures outside the cases allowed in Article 23.

32. Violation of the principle of confidentiality established in article 4, paragraph h) of this law.

33. Failure to facilitate the access of the supervisory authority to personal data, information, premises, equipment and means of treatment that are required by this authority for the exercise of its investigative powers.

34. Resisting or obstructing the exercise of the inspection function by the competent supervisory authority.

35. The deliberate reversal of an anonymization or pseudonymization procedure in order to allow the re-identification of data subjects.

36. Collecting, storing, transmitting or in any other way using personal data without having one of the legal bases established in this law.

Article 46.- Administrative sanctions.

The sanctions to be applied by the Agency for the proven faults, may consist of:

1. Warning, indicating the term and the form for the adoption of corrective measures, as the case may be;

2. Fines: from 20 (twenty) to 2,500 (two thousand five hundred) minimum wages for unspecified miscellaneous activities in the Republic of Paraguay.

2.1. In the case of violations committed in the processing of sensitive data, the amounts of the penalties may be increased up to 5,000 (five thousand) minimum wages for various activities not specified in the Republic of Paraguay.

2.2. In the case of infractions committed in the processing of sensitive data of children and adolescents, the amounts of the penalties may be increased up to 10,000

Congreso Nacional
H. Cámara de Diputados

(ten thousand) minimum wages for various unspecified activities in the Republic of Paraguay.

3. Suspension of activities related to the processing of personal data.

The application of the different types of sanctions may be indistinct or cumulative.

The Agency is empowered to issue complementary and/or clarifying rules to the present article.

Article 47.- Criteria for the application of administrative sanctions.

The administrative penalties shall be determined considering the following criteria:

1. The seriousness and nature of the infringements and the damage or danger to the legal interests protected by this law;

2. The good faith of the offender or the express acknowledgement or acceptance by the person under investigation of the commission of the infraction prior to the imposition of the sanction that may be applicable;

3. The degree of responsibility of the infringer, as well as the intention or negligence in the nature of the infringement;

4. The advantage or economic benefit obtained or intended by the infringer by virtue of the commission of the infringement;

5. The economic situation of the offender;

6. Recidivism in the conduct;

7. The cooperation of the infringer in the investigative action of the control authority;

8. The repeated and proven adoption of internal mechanisms and procedures capable of minimizing the damage, aimed at the safe and proper treatment of data;

9. The adoption of a best practices policy or code of conduct;

10. The prompt adoption of corrective measures;

11. Others that may be considered by the supervisory authority, depending on the nature of the case.

Congreso Nacional
H. Cámara de Diputados

Article 48.- Prescription of sanctions.

The statute of limitations for sanctions shall be as provided in Law No. 6715/2021 "ON ADMINISTRATIVE PROCEDURES" or its equivalent.

Article 49.- Payment of fines.

The amount of the fines shall be paid within 30 (thirty) working days, counted from the notification.

The regulation shall establish the consequences derived from non-compliance, including interest, as well as any other relevant aspect for the effective compliance with the imposed sanction.

Article 50.- Supposition of non-compliance by public institutions.

In the event that the supervisory authority notices an alleged breach of the provisions of this law by public institutions, it shall issue a warning and a resolution establishing corrective measures to be adopted so that the effects of the breach cease or be corrected.

The resolution by which the implementation of measures is ordered shall be notified to the highest authority of the public institution in which the offense has occurred and to the affected data owner, if any.

Without prejudice to the provisions of the preceding paragraphs, the public institution, after analyzing the facts in question, shall take the appropriate measures with respect to the alleged perpetrators, including, but not limited to, the instruction of an administrative summary for the imposition of disciplinary sanctions in accordance with the procedure established for such purpose.

Chapter II
The filing of a complaint or claim.

Article 51.- Complaint to the supervisory authority.

The data owner or his legal representative may file a claim or complaint, free of charge, by any means provided for such purpose by the supervisory authority, clearly stating the content of his request and the provisions of this Law that he considers to have been violated, and proving that he has made the notification provided for in the law.

The presentation must be made within 15 (fifteen) working days following the date on which the response to the notification is communicated by the data controller or data processor, or at any time if the term established for this purpose has expired without a response from the data controller or data processor. The response, if any, shall accompany the filing of the complaint.

Article 52.- Resolution of the supervisory authority.

After receiving a claim or complaint, the supervisory authority may, by means of a well-founded resolution:

a) Dismiss the claim or complaint filed;

Congreso Nacional
H. Cámara de Diputados

b) If it considers that the data owner is entitled, require the data controller or data processor to enforce the exercise of the rights subject to protection, and shall inform the supervisory authority in writing of such compliance within fifteen (15) working days of its occurrence;

c) In the event that a fault is found to have been committed, apply the sanctions provided for in this law.

Chapter III
Verification of faults and application of administrative sanctions.

Article 53.- Procedure for the verification of faults and application of sanctions.

The faults to the provisions of the present law and its regulations must be proved in an administrative summary.

The investigation of the summary shall be ordered by resolution of the Director General of the Agency and shall contain a complete list of the facts, acts or omissions imputed to the alleged offender, as well as the designation of the Examining Judge from among those who render services in the control authority.

The regulations shall determine the procedure and time limits to be followed, including the time limit for the Instructing Judge to submit his final report to the Director General and the time limit for the issuance of the corresponding resolution. All other aspects of the procedure shall be governed by the provisions of Law No. 6715/2021 "DE PROCEDIMIENTOS ADMINISTRATIVOS" or that which may eventually replace it.

Article 54.- Precautionary measures.

Once the sanctioning procedure has been initiated, the adoption of provisional measures to ensure the effectiveness of the final resolution that may be issued in the referred procedure may be ordered by means of a reasoned resolution.

Article 55.- Appeal for reconsideration.

Against any resolution or administrative act of a non-regulatory nature issued by the Agency, an appeal for reconsideration may be filed before the Director General of the Agency.

The administrative instance is exhausted with the resolution of the Director General of the Agency for the Protection of Personal Data. The Ministry of Information and Communication Technologies shall not be competent for the processing of applications and other proceedings related to personal data protection rights or other competencies of this Agency.

Congreso Nacional
H. Cámara de Diputados

Article 56.- Contentious-administrative action.

The contentious-administrative action may be filed before the Court of Accounts, within the term established by Law No. 6715/2021 "ON ADMINISTRATIVE PROCEDURES" or the one that may eventually replace it.

The appeal for reconsideration and the contentious-administrative action shall have suspensive effect in the cases in which they are filed against a resolution that applies administrative sanctions, but they shall not suspend the precautionary measures dictated or the corrective measures that tend to avoid the occurrence of damages.

TITLE VI

FINAL AND TRANSITORY PROVISIONS

Article 57.- Entry into force.

The present law shall enter into force 24 (twenty-four) months after its official publication.

Article 58.- Repeals.

Subsections **a)** and **b)** of Section 3, Section 4, subsection **b)** of Section 20, subsection **x)** of Section 21 of Law No. 6534/2020 "ON THE PROTECTION OF PERSONAL CREDIT DATA" are hereby repealed.

Article 59.- Regulation.

The Executive Branch shall regulate the present law before its entry into force.

Article 60.- To be communicated to the Executive Branch.

GIVEN IN THE CHAMBER OF SESSIONS OF THE HONORABLE CHAMBER OF DEPUTIES OF THE NATION, ON THE TWENTY-SEVENTH DAY OF THE MONTH OF DECEMBER.
OF THE NATION, ON THE TWENTY-SEVENTH DAY OF MAY OF THE YEAR TWO THOUSAND AND
TWENTY-FIVE.

María Constancia de Benítez
Parliamentary Secretary

Carlos María Arrechea Ortiz
First Vice President
in exercise of the Presidency
H. Chamber of Deputies

cvf