OFFICIAL GAZETTE
OF THE REPUBLIC OF PARAGUAY

"150TH ANNIVERSARY OF THE NATIONAL EPIC: 1864–1870"

Supervising Authority: Civil Cabinet of the Presidency - Government Palace - Management and Administration: Office of Official Publications - Stella Maris Ave. at Hernandarias St. - Tel.: 498 311 - ASUNCIÓN - PARAGUAY
www.gacetaoficial.gov.py

ISSUE 287 | **Asunción, November 27, 2025** | **39-PAGE EDITION**

TABLE OF CONTENTS

OFFICIAL REGISTRY SECTION

LEGISLATIVE BRANCH

Page

LAW No. 7,565.— ESTABLISHING PHYTOSANITARY MEASURES AND PROVIDING FOR OTHER RISK MITIGATION MEASURES REGARDING THE IMPORTATION OF USED AGRICULTURAL MACHINERY, EQUIPMENT, AND IMPLEMENTS INTO THE COUNTRY. **2**

LAW No. 7,593.— ON THE PROTECTION OF PERSONAL DATA IN THE REPUBLIC OF PARAGUAY. **7**

LEGISLATIVE BRANCH

"150TH ANNIVERSARY OF THE NATIONAL EPIC: 1864–1870"

LEGISLATIVE BRANCH
LAW No. 7565

ESTABLISHING PHYTOSANITARY MEASURES AND PROVIDING FOR OTHER RISK MITIGATION MEASURES REGARDING THE IMPORTATION OF USED AGRICULTURAL MACHINERY, EQUIPMENT, AND IMPLEMENTS INTO THE COUNTRY

THE CONGRESS OF THE PARAGUAYAN NATION ENACTS AS LAW

Article 1. Purpose.

The purpose of this law is to regulate the importation of used agricultural machinery, equipment, and implements in order to protect agricultural ecosystems and local biodiversity by preventing the introduction of invasive species associated with contaminated machinery, as well as to ensure crop health and sustainable agricultural production in the long term.

Article 2. Definition.

Agricultural machinery, equipment, and implements shall be considered to include all equipment used in agricultural tasks, their accessories, attachments, trailers, and carts specifically designed for the transport of agricultural machinery or parts thereof, including harvesters, tractors, planters, seeders, sprayers, and other equipment as determined by the regulations.

Article 3. Enforcement Authority.

The following entities are the enforcement authorities for this law and shall act within the scope of their respective jurisdictions:

a) The National Service for Plant and Seed Quality and Health.

b) The Ministry of Industry and Commerce.

c) The National Tax Revenue Directorate.

Article 4. Importation of Used ~~Agricultural~~ Machinery.

The free importation of used agricultural ~~machinery~~, equipment, and implements of any origin and model, no more than five years old as of their year of manufacture, that comply with the quality and ~~safety~~ requirements established in this law is hereby authorized. idad y seg

BE

that meet the quality and safety requirements established

Article 5. Registry of Importers of Used Machinery.

The Registry of Importers of Used Machinery is hereby established, under the jurisdiction of the Undersecretariat of State for Commerce of the Ministry of Industry and Commerce.

Article 6. Prior License.

A Prior Import License is hereby established for the importation of used machinery, equipment, and implements; to this end, the importer must be duly registered in the Registry of Importers of the Undersecretariat of State for Commerce and authorized for such purpose.

Article 7. Certification, Inspection, and Cleaning of Used Agricultural Machinery.

Used agricultural machinery, equipment, and implements entering the national territory must be properly sanitized and free of soil, plant matter, and pests, for which they must undergo a disinfection and cleaning process in both the country of origin and the country of destination, using methods such as high-pressure washing, steam, forced air, vacuuming, or other methods accepted by international certification bodies, with parts disassembled if necessary.

The certification, inspection, and cleaning of the machinery will be verified and carried out by the National Service for Plant and Seed Quality and Health, and a fee will be established for this purpose.

Certification at the point of origin must be issued by a body accredited by the plant protection authority of the country from which the goods are imported.

Article 8. Requirements.

The following are established as the minimum quality and safety requirements for the importation of used agricultural machinery:

a) Prior Import License.

b) Approval of a Vehicle Technical Inspection.

c) Approval of a phytosanitary inspection conducted by the National Service for Plant and Seed Quality and Health, which may include disassembly and testing.

d) A declaration of cleanliness, a treatment certificate, and a phytosanitary certificate issued in the country of origin of the used agricultural machinery in accordance with international standards.

e) A certified technical inspection by an independent and authorized company ~~in~~ the country of origin regarding the condition of the machinery, the engine, and the odometer.

f) The importation of agricultural machinery with tampered engines or odometers is prohibited; a statement of hours of use must be submitted.

g) Manufacturer's or distributor's warranty.

h) Pollutant emissions from the machinery must comply with the maximum permissible limit established by the Ministry of the Environment and Sustainable Development, in its capacity as the enforcement authority.

i) Damaged machinery, equipment, or implements may have only superficial damage that does not affect mechanical components that compromise the safety or operation of the machinery.

j) Agricultural machinery that has overturned is prohibited from entry.

k) Other requirements issued by the enforcement authority and other applicable laws.

I) Quality and safety requirements shall be regulated by the enforcement authorities.

Article 9. Responsibilities of the Importer.

The importer shall be responsible for:

a) Maintaining the validity of their Unique Importer Registration with the General Customs Administration.

b) Ensuring that their Registration as an Importer of Used Agricultural Machinery remains valid.

c) Complying with the requirements set forth in this law.

d) Bearing the costs associated with the application of phytosanitary measures determined by the National Service for Plant and Seed Quality and Health, resulting from noncompliance with the provisions of this resolution.

e) Re-export the rejected used agricultural machinery within the timeframes established by the National Service for Plant Quality and Health and Seeds.

Article 10. Biodiversity Conservation Fee.

A Biodiversity Conservation Fee is hereby established, which shall be levied on the importation of used agricultural machinery, equipment, and implements regulated by this law.

The National Service for Plant and Seed Quality and Health, in cooperation with the National Tax Revenue Directorate, shall establish the scale of values to be applied to the importation of agricultural machinery, taking into account the age, the type of engine, the engine's operating hours, the level of pollutant emissions, the condition of the tires and ~~batteries~~, and other factors with potential to cause pollution.

The funds collected shall be allocated to the National Plant and Seed Service.

BE ~~The funds~~ collected will be allocated to ~~the~~ National Plant and ~~Seed~~ Quality and Health ~~Service~~.

Vegetal y de Semillas.

BE

Article 11. Inapplicability of Tax Exemptions.

All imported used machinery, equipment, and implements that are subject to customs duties in accordance with the provisions of the MERCOSUR Common External Tariff (AEC) are not eligible for the tax exemptions identified as the Current National Tariff (ANV) due to their status as used goods.

Article 12. Vehicle Technical Inspection and Phytosanitary Inspection.

All imported used agricultural machinery must undergo a vehicle technical inspection and a phytosanitary inspection within the country as a mandatory prerequisite for customs clearance.

Article 13. Obligations of Notaries Public.

Notaries and public notaries must require the document certifying the vehicle technical inspection and the phytosanitary inspection in order to record and register deeds of transfer for imported used agricultural machinery, regardless of its period of use.

Article 14. Training and Awareness.

The National Service for Plant and Seed Quality and Health shall develop training programs for importers and farmers on the importance of phytosanitary safety and the measures to be followed to ensure it.

Article 15. Penalty System.

Any violation or failure to comply with any of the obligations established in this law, as well as with any regulatory provisions that may be issued, shall be sanctioned by the National Service for Plant and Seed Quality and Health, following an administrative investigation that guarantees the alleged violator the right to a defense.

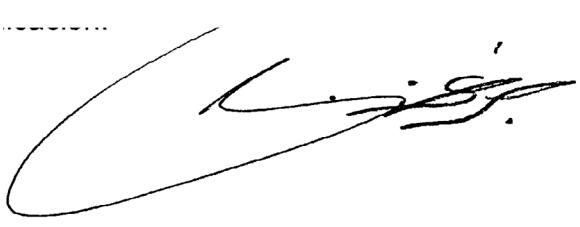
The penalties that may be imposed are: a warning, suspension or cancellation of the registration of importers and distributors of used imported agricultural machinery, equipment, and implements; confiscation; and/or a fine of up to five thousand times the minimum daily wage for various unspecified activities in the Republic.

The procedure for imposing these penalties, the circumstances surrounding the commission of the acts and/or conduct giving rise to them, their severity, and the maximum fine applicable for each violation—within the limits set forth in this law—as well as the applicability of other penalties, shall be regulated by the Executive Branch.

Article 16. Regulations.

The Executive Branch, in ~~coordination~~ with the enforcement authorities, shall issue regulations for the provisions of this law that require them within sixty days following its publication.

BE







Article 17. Effective Date.

This law shall enter into force on the day following its publication in the Official Gazette.

Article 18. Repeals.

Any provision contrary to this Act is hereby repealed.

Article 19. Transmission to the Executive Branch.

The Bill was approved by the Honorable Chamber of Deputies on the **fifteenth day of July, two thousand twenty-five**, and by the Honorable Senate on the **eighth day of October, ~~two~~ thousand twenty-five**, and is hereby enacted, in accordance with the provisions of Article **206** of the Constitution.

This is in accordance with Article **206** of the Constitution.

Raúl Luis Latorre Martínez
President
Honorable Chamber of Deputies

Basilio Gustavo Núñez
President
Honorable Chamber of Senators

Bettina Rosmary Aguilera P.
Parliamentary Secretary

Lizarellá Valiente
Parliamentary Secretary

Asunción, November 13, 2025

Let this be a Law of the Republic; let it be published and entered into the Official Register.

The President of the Republic

PRESIDENCY OF THE REPUBLIC OF PARAGUAY

TETÁ MBURUVICHA GUASU RENDA

~~Santiago Peña~~Palacios

~~Javier Giménez~~ García de Zuñiga
Minister of ~~Industry~~ and Commerce

"150TH ANNIVERSARY OF THE NATIONAL EPIC: 1864–1870"

LEGISLATIVE BRANCH
LAW No. 7593

ON THE PROTECTION OF PERSONAL DATA IN THE REPUBLIC OF PARAGUAY

THE CONGRESS OF THE PARAGUAYAN NATION ENACTS AS LAW

TITLE I
GENERAL PROVISIONS

Chapter I
Purpose 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. This law applies to any processing of personal data, whether fully or partially automated, as well as to non-automated processing when such personal data forms part of a file or is intended to do so, carried out by natural or legal persons, regardless of the medium, the country of their headquarters, or the country where the data is located, in the following cases:

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

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

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

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

   iii. when data processing ~~activities~~ are related to the monitoring of ~~the behavior~~ of natural persons, to the extent that such monitoring takes place within the ~~territory~~ of the Republic of Paraguay.

BC

the territory of the Republic of Paraguay.

2. This law shall not apply in the following cases:

a) The processing of personal data when such data is intended exclusively for activities within the context of a natural person's family or domestic life, and is not intended for commercial disclosure or use;

b) In the processing of data for the purposes of public safety, immigration matters, defense, national security, and activities related to criminal matters, criminal investigations, and the prosecution of crimes. In such cases, the processing must at all times respect fundamental rights and freedoms and be carried out in a manner that is necessary and proportionate to the intended purpose, in accordance with the general principles of personal data protection, as well as the minimum safeguards established in this law, to the extent that they are compatible with the nature of the processing.

Article 3. Definitions.

For the purposes of this law, the following definitions apply:

1. **Anonymization:** The application of measures of any nature intended to prevent or hinder the identification or re-identification of a natural person;

2. **Data blocking:** The identification and restriction of personal data, through technical and organizational measures, to prevent its processing—including its viewing—except when making the data available to judges and courts, the public prosecutor's office, and other competent public authorities, in the manner and under the conditions established by applicable regulations;

3. **Consent:** Any free, express, specific, informed, and unambiguous manifestation of will by which a natural person accepts and authorizes—whether through a statement or a clear affirmative action in writing or by electronic means, or by any equivalent means permitted by technology—the processing of their own personal data or that of the person they represent;

4. **Biometric data:** Personal data obtained through a specific technical process, relating to a person's physical and/or physiological characteristics, that enables or confirms the unique identification of that person, such as facial images, iris recognition, or fingerprint data;

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

6. **Personal data:** Information of any kind relating to identified or identifiable natural persons. An identifiable person is one who can be identified, directly or indirectly, by means of an identifier or by one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural, or social identity;

E & M
New
Y#

BC

7. **Sensitive personal data:** Data relating to racial or ethnic origin; religious, philosophical, or moral beliefs or convictions; union or political affiliation; data relating to health, sexual preference, or sexual orientation; genetic data; or biometric data intended to uniquely identify an individual; and any other data whose misuse could give rise to discrimination or pose a serious risk to the data subject;

8. **Profiling:** The result of the processing of personal data carried out in an automated or semi-automated manner to evaluate certain aspects of a natural person, to analyze or predict matters relating to professional or work performance, economic status, health, personal preferences, behaviors, interests, and other matters that may be covered by the Regulations;

9. **Data processor:** The natural or legal person, whether public or private, that processes personal data on behalf of and under the instructions of the data controller;

10. **Data Protection Impact Assessment:** A prior analysis of data processing operations that may pose a risk to the rights and freedoms of individuals;

11. **Personal data security incident:** An incident that results in the accidental or unlawful destruction, loss, or alteration of personal data that has been transmitted, stored, or otherwise processed, or the unauthorized disclosure of or access to such data;

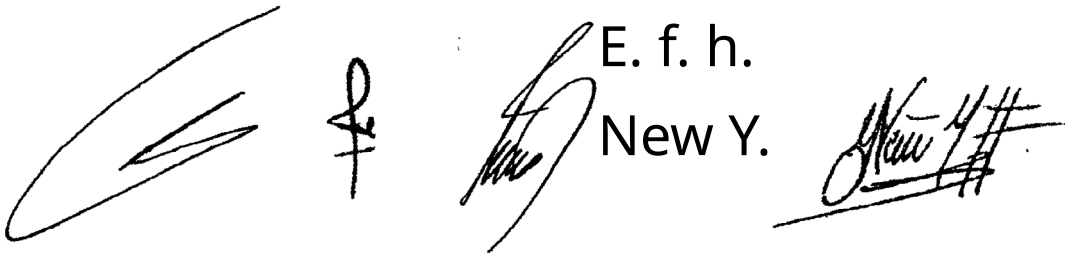
12. **Data controller:** A natural or legal person, public or private, or any other body that, alone or jointly with others, determines the purposes and means of data processing;

13. **Third Party:** A natural or legal person, whether domestic or foreign, public or private, other than the data subject, the data controller, the data processor, and those persons who, under the direct authority of the data controller or the data processor, are authorized to process personal data:

14. **Data subject:** A natural person to whom the personal data refers or to whom the personal data pertains;

15. **International data transfer:** The transfer**of** personal data between two or more entities, whether data controllers or data processors, when at least one of them is headquartered in a jurisdiction outside the Republic of Paraguay;

16. **Processing:** Any operation or set of operations performed on personal data by manual, automated, or partially automated means, including, but not limited to, the collection, access, gathering, recording, organization, structuring, adaptation, indexing, modification, extraction, consultation, storage, retention, blocking, processing, transfer, disclosure, dissemination, possession, utilization, and, in general, any use or disposition of personal data.



BC

Article 4. General Principles of Personal Data Protection.

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

a) **Principle of Data Accuracy:** Data shall be accurate. The accuracy of data provided by the data subject is presumed. Processed data must accurately reflect the information provided by the data subject. Data controllers and processors must take all reasonable measures to ensure that data is kept up to date and that inaccurate data is deleted or corrected without delay;

b) Principle of lawfulness: Personal data must be processed lawfully and fairly, in accordance with the provisions and principles established by law. The data controller must be able to demonstrate the lawfulness of the personal data processing it carries out;

c) **Principle of Purpose Limitation:** 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 distinct from those purposes.

Further processing for archival and public interest purposes, scientific and historical research purposes, or statistical purposes shall not be considered incompatible with the original purposes, provided that measures are taken to ensure compliance with the principle of data minimization:

d) **Principle of data minimization or proportionality:** The personal data processed must be strictly limited to that which is necessary, appropriate, and relevant to the purposes of the processing and may be retained only for the period of time necessary to fulfill the purposes of the processing. Regulations shall determine the cases in which, by way of exception and in consideration of historical, statistical, scientific, or judicial administration values, personal data may be retained even when such necessity or relevance has ceased to exist;

e) **Principle of Limitation of Retention Period:** Data may not be retained or maintained for longer than is necessary for the purposes of processing. The supervisory authority shall establish the time limits for deletion and/or periodic review.

The further processing of personal data for archival and public interest purposes, scientific and historical research purposes, or statistical purposes shall not be considered incompatible with the original purposes, provided that the data has been anonymized or pseudonymized;

f) **Principle of fairness and transparency:** Personal data must be processed fairly and transparently with respect to the data subject.

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



BC

g) **Principle of Balancing Public Transparency and Protection:** The obligation to disclose acts of State Agencies and Entities must take into account the principles of personal data protection established in this law and, in particular, the principle of data minimization. The publication and dissemination of personal data shall be permitted only to the extent that its inclusion is necessary and proportionate to the purpose of transparency sought through disclosure in the specific case. Personal data that exceeds that purpose, or whose publication is not necessary, must be excluded or redacted from the acts or documents to be published. The publication of sensitive data is prohibited;

h) **Principle of Due Diligence:** The data controller and, where applicable, the data processor must adopt appropriate measures—including privacy by design, privacy by default, data protection impact assessments, and the appointment of a data protection officer, among others—to ensure the proper processing of personal data and demonstrate their effective implementation;

i) **Principle of Security:** When processing personal data, technical and organizational measures must be adopted to ensure data security, with the aim of preventing accidental alteration, loss, destruction, or damage, as well as unauthorized or unlawful processing or access. In the case of data defined as sensitive, additional measures may be adopted to ensure its security, as specified in the regulations under this law;

j) **Principle of Confidentiality:** Data controllers and processors of personal data, as well as any person involved in any phase of such processing, shall be subject to a duty of confidentiality, an obligation that shall remain in effect even after the termination of their relationship with the data subject. They may be released from the duty of confidentiality by court order or legal obligation.

TITLE II
ON THE PROCESSING OF PERSONAL DATA

Chapter I
On the Legal Bases for the Processing of Personal Data.

Article 5. Conditions.

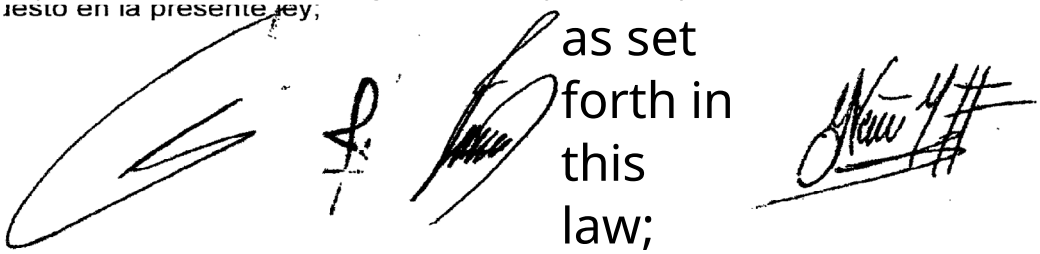
The processing of personal data may only take place if at least one of the following conditions is met:

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

2. When the processing is necessary for the data controller to comply with a legal obligation;

3. In the processing and sharing of data that is necessary and proportionate by State Agencies and Entities for the exercise of their specific functions and the implementation of public policies provided for in laws and regulations, subject to the provisions of this Act;

. lesto en la presente ley;



BC

4. When the processing of personal data is necessary for the performance of a contract or a preliminary procedure related to a contract to which the data subject is a party, at the data subject's request;

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

6. When the processing is necessary to satisfy legitimate interests pursued by the data controller or by a third party, except when the data subject's interests or fundamental rights and freedoms—which require the protection of personal data—prevail over such interests, particularly when the data subject is a child and/or adolescent. This provision shall not apply to the processing of personal data by the State within the limitations set forth in the Constitution and in this law;

7. For the protection of the life, physical or mental safety, and/or health of the data subject or a third party, exclusively in procedures carried out by health professionals, health services, or health authorities within the limits of their jurisdiction, or for the legal protection of a natural person as ordered by a competent authority in judicial proceedings. The regulations shall determine the appropriate measures according to the types of data, processing activities, and data controllers, as well as the timing for their review and update.

Article 6. Conditions for Consent.

If the legal basis for the processing of personal data is consent, such consent must be prior, freely given, informed, and unambiguous, for one or more specific purposes, whether through a statement or a clear affirmative action.

If the data subject's consent is given in the context of a written statement that also addresses other matters, the request for consent must be presented in such a way that it is clearly distinguishable from the other matters, in an intelligible and easily accessible manner, and using clear and simple language. Any statement or part thereof that violates this law shall not be binding.

The data subject shall have the right to withdraw or revoke their consent at any time and must be informed of this right before granting consent. The data controller must establish simple, streamlined, effective, and free mechanisms for exercising this right, which may not be more complex than the processes established for granting consent. The withdrawal or revocation of consent shall not affect the lawfulness of the processing carried out based on the consent given prior to its withdrawal.

In all cases, the data controller bears the burden of proving that the data subject consented to the use of their personal data.

E. F. Hickey

John H.

BC

Article 7. Consent of Children and Adolescents.

In the processing of personal data of a child or adolescent, the protection of their best interests shall prevail, in accordance with the provisions of the Constitution, the Convention on the Rights of the Child, other international legal instruments ratified by the Republic of Paraguay, and applicable legislation.

The processing of personal data of individuals under the age of sixteen, whether such data is sensitive or not, shall require the prior, express, and informed consent of the holder of parental authority, guardian, or legal custodian.

In the case of adolescents who are sixteen years of age or older and until they reach the age of majority, the processing of sensitive personal data will require the adolescent's express consent, along with the authorization of the parent or legal guardian.

In all cases, consent must be given under conditions that ensure the adolescent understands its scope, using means and language that are clear and appropriate to the age and developmental level of the child or adolescent. The information referred to in this article must be provided in a simple, clear, and accessible manner, taking into account the physical, motor, perceptual, sensory, intellectual, and mental characteristics of the data subject or of those exercising parental authority, guardianship, or legal custody, using audiovisual resources when appropriate.

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 to satisfy such interest and provided that the fundamental rights and freedoms of the data subject do not take precedence.

The processing of personal data based on legitimate interest requires that such processing take place within the framework of a relevant and appropriate relationship between the data subject and the data controller, and always in accordance with the data subject's reasonable expectations.

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

The supervisory authority may require the data controller to conduct a prior data protection impact assessment justifying its legitimate interest and the necessity of collecting or processing the data in each case, while respecting trade 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 by challenging the data controller's legitimate interest.

E & M

New H.

BC

LAW No. 7593

Chapter II
On the Obligations of the Data Controller and the 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 data subjects, the data controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with this law and its regulations. Such measures shall be reviewed and updated as necessary.

The regulations shall specify the appropriate measures based on the types of data, processing activities, and data controllers, the frequency of their review and update, as well as the measures for protection by design and by default.

Article 10. Joint Data Controllers.

When two or more data controllers jointly determine the purposes and means of processing, they shall be considered joint data controllers. The joint controllers shall determine, among themselves, in a transparent manner and by mutual agreement, their respective responsibilities in complying with the obligations imposed by this Act. Such agreements, while they may designate a common point of contact for data subjects, shall not relieve the joint controllers of their joint and several liability toward the data subject.

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

Article 11. Data Processor.

When data processing is carried out on behalf of a data controller, it may be performed only by a party that offers sufficient guarantees to implement appropriate technical and organizational measures, so that the processing complies with the requirements of this law and ensures the protection of the data subject's rights.

In such cases, the processing shall be governed by a contract or other legal instrument authorizing such delegation in accordance with the legal system, which must establish—without prejudice to other elements—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 data controller.

The data processor may also delegate such processing to another data processor, in which case the provisions of the preceding paragraph must be complied with. Such delegation does not exempt the delegating data processor from liability to the data controller with respect to the fulfillment of the obligations of the sub-processor.

If a data processor determines the purposes and means of such processing in violation of this law, it shall be held liable with respect to that processing vis-à-vis any person or persons entitled ~~to make~~ such a claim.

BC

E. f. h. Yuan H.

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

The regulations under this law shall establish the cases and conditions under which data controllers or processors shall be required to appoint a representative.

The representative may respond to a request made by the data subject or by the supervisory authority.

Article 13. Binding Self-Regulatory Mechanisms.

The supervisory authority shall promote the development of binding self-regulatory mechanisms designed to contribute to the proper implementation of this Act.

Binding self-regulatory mechanisms may consist of codes of conduct, codes of best practices, binding corporate rules, trust seals, certifications, or other mechanisms that contribute to the stated objectives; the regulations may establish the necessary requirements for their approval by the supervisory authority.

Codes of conduct may include mechanisms for out-of-court dispute resolution, but the use of such mechanisms must not impose additional costs on the data subject or require the data subject to travel disproportionately far from their place of residence.

Article 14. Impact Assessment.

Prior to implementing data processing operations that, due to their nature, scope, context, or purposes, may pose significant risks to the rights of data subjects, the data controller must conduct an assessment of the impact of such operations on the protection of personal data.

A data protection impact assessment is mandatory in the following cases:

a) A systematic and comprehensive evaluation of personal aspects of data subjects based on automated data processing, including profiling, and on the basis of which decisions are made that produce legal effects for natural persons or similarly significantly affect them;

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

c) Systematic, large-scale processing for the purpose of surveillance in public places.

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

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

E & H

May 11.

BC

LAW No. 7593

Article 15. Prior Consultation.

The data controller shall consult with the supervisory authority before proceeding with data processing when an impact assessment demonstrates that the processing would pose a risk unless the data controller takes measures to mitigate it.

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

The supervisory authority shall, within thirty business days from the date of the consultation, provide written advice to the data controller or processor, in accordance with the functions established in this law. This deadline may be suspended on an exceptional basis for just cause and only until the supervisory authority has obtained the information requested for the purposes of the consultation.

Article 16. Security Measures.

The data controller and the data processor shall periodically carry out a series of actions to ensure the establishment, implementation, operation, monitoring, review, maintenance, and continuous improvement of the security measures applicable to the processing of personal data.

The supervisory authority shall regulate the minimum technical security and integrity requirements that must be applied by data controllers and processors.

Article 17. Notification of a Personal Data Processing Security Incident to the Supervisory Authority and the Data Subject.

In the event of a personal data security incident, the data controller shall notify the Supervisory Authority and, where applicable, the Data Subject, within a period not exceeding seventy-two hours from the time the incident is discovered. The conditions and requirements shall be established in the regulations under this law.

Article 18. Data Protection Officer.

The Data Protection Officer is the person designated to assist with and oversee compliance with the rules regarding the protection of personal data.

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

The data protection officer shall be appointed based on their professional qualifications and their ability to perform the duties to be established in the regulations of this law.

A corporate group may appoint a single Data Protection Officer provided that the individual meets the criteria set forth in this regulation and is easily accessible from each facility. When the data controller or data processor is a public authority or agency, a single Data Protection Officer ~~may~~ be ~~appointed~~ for several such authorities or agencies, taking into account their organizational structure and size.

BC

taking into account their organizational structure and size.

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

Regulations shall establish other aspects relating to the data protection officer.

Chapter III
International Data Transfers.

Article 19. General Rules for International Transfers of Personal Data.

Transfers of personal data outside the national territory, including onward transfers, may only take place if the destination country, territory, sector, or international organization provides an adequate level of protection, in accordance with the provisions of this law.

The adequacy assessment shall be conducted by the National Personal Data Agency, which shall determine such adequacy by means of a reasoned resolution or through the publication of an official list, in accordance with the principles, rights, and safeguards established in this Act.

If the recipient country does not provide an adequate level of protection, the data controller or processor must adopt appropriate safeguards to ensure that the processing of personal data is carried out in accordance with the provisions of this law. Such safeguards may consist, among other things, of specific or standard contractual clauses, binding corporate rules, codes of conduct, or certification mechanisms, always in accordance with the provisions of the regulations implementing this law.

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

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

2. International judicial cooperation;

3. International cooperation among intelligence agencies to combat terrorism, illicit drug trafficking, money laundering, corruption, human trafficking, and other forms of crime;

4. When personal data is necessary for the performance of a contractual relationship to which the data subject is a party, including what is necessary for activities such as user authentication, service improvement and support, monitoring of service quality, support for account maintenance and billing, and those activities required for the management of the contractual relationship;

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

6. When the cross-border transfer of personal data is carried out for the protection, prevention, diagnosis, or medical or surgical treatment of the data subject; or when necessary for ~~the~~ conduct of epidemiological or similar studies, provided that appropriate anonymization ~~procedures~~ are applied;

BC

Mash
4#

7. When the data subject has given prior, informed, express, and unambiguous consent;

8. When the data controller offers and demonstrates 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 rules;

d) Seals, certificates, and codes of conduct issued periodically.

Chapter IV
On the Processing of Certain Categories of Personal Data.

Article 20. Processing of Sensitive Data.

The processing of sensitive personal data is prohibited unless:

1. The data subject has given consent to the processing of such personal data, except where it is established that the aforementioned prohibition cannot be overcome by the data subject's consent; such consent shall have no effect if it is not freely given, informed, or unambiguous, or if the granting of consent has been directly or indirectly imposed on the data subject;

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

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

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

5. The processing is carried out, within the scope of its legitimate activities and with the necessary safeguards, by a foundation, an association, or any other nonprofit organization whose purpose is political, philosophical, religious, or labor-related, provided that the processing relates exclusively to current members of such organizations or to individuals who maintain regular contact with them in connection with their purposes, and provided that personal data are not disclosed outside of these organizations without the consent of the data subjects;

6. The processing is necessary for the establishment, exercise, or defense of legal claims, or ~~when~~ the competent judicial authorities are acting in the exercise of their judicial ~~functions~~;



BC

7. The processing is necessary for reasons of public interest in the area 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 in health care or the provision of food, medicines, medical devices, or food products; appropriate and specific measures must be established to protect the rights and freedoms of the data subject, in particular professional confidentiality;

8. The processing is necessary for the purposes of preventive or occupational medicine, the assessment of a worker's ability to work, medical diagnosis, the provision of health or social care or treatment, or the management of 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 subsection may be processed provided that such processing is carried out by a professional subject to an obligation of professional secrecy or confidentiality, or under their responsibility, or by any other person subject to an obligation of secrecy in accordance with the legal system;

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

10. The processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, which must be proportionate to the objective pursued, respect in essence the right to data protection, and establish adequate and specific measures to protect the data subject's fundamental rights and interests. The data must be effectively anonymized;

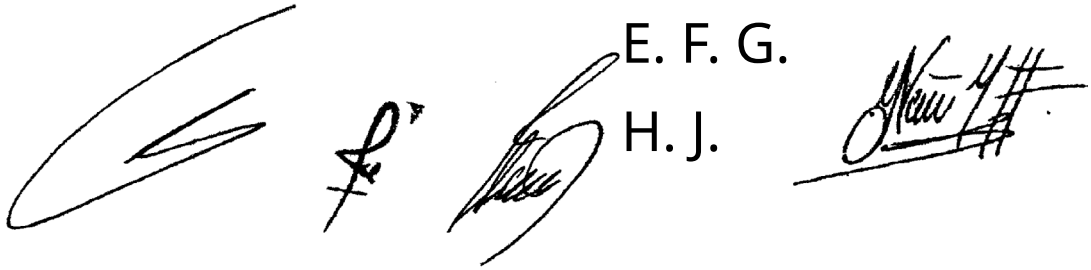
11. The processing and sharing of data that is necessary and proportionate by government authorities for the exercise of their specific functions and the implementation of public policies provided for in laws and regulations.

Article 21. Processing of Credit Information.

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

Except for the functions and powers expressly assigned to the Central Bank of Paraguay, all other functions and powers granted for the implementation of the law regulating credit data shall be exercised by the control and supervisory authority established under this law.

This law shall apply on a supplementary basis to matters not provided for in the law regulating credit data, provided that such matters are consistent with the nature of said information.



Article 22. Processing for Video Surveillance Purposes.

Natural or legal persons, whether public or private, may process images and sounds through camera or video camera systems for the purpose of ensuring the safety of persons and property, as well as that of their facilities.

Images and sounds may be captured on public streets only to the extent that it is essential for the purpose mentioned in the preceding paragraph.

However, the capture of images and sounds from public streets may extend beyond this scope when necessary to ensure the security of strategic property or facilities or transportation infrastructure, provided that under no circumstances may this involve the capture of images and sounds from inside a private residence.

Any data that must be retained to substantiate the commission of acts that threaten the safety of persons, property, 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 seventy-two hours from the time the existence of the recording became known, without prejudice to the investigative powers of the competent authorities within the framework of an ongoing investigation.

The processing by a natural person of images and sound that capture only the interior of their own residence is considered excluded from the scope of this article.

This exclusion does not apply to processing carried out by a private security entity that has been contracted to monitor a residence and has access to such recordings.

Article 23. Processing of Criminal Data, Penalties, and Administrative Offenses.

The processing of personal data relating to criminal offenses, as well as to related proceedings and precautionary and security measures, shall be governed by the applicable law.

The processing of data relating to administrative violations and penalties shall be governed by the applicable law.

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

Chapter V
On Data Processing in the Public Sector.

Article 24. Access to Public Information and Data Protection.

The right of access to information contained in public sources may be denied or restricted when such a measure is necessary to prevent specific harm to the protection of one of the private interests inherent in the protection of personal data, in accordance with the rules and principles established in this law and in accordance with the procedure set forth in this article.

An exception to access to public ~~information~~ shall apply only when the harm caused to the protected interest ~~outweighs~~ the public interest in obtaining access to the information.

BC

& Wu
Wu
Y#

The established exception shall not apply when:

a) The individual has expressly consented to the disclosure of their personal data;

b) The circumstances of the case clearly show that the information was provided to the obligated party as part of the information that must be subject to the disclosure regime;

c) The information is available from publicly accessible sources, without prejudice to the provisions of special laws;

d) The information is public in nature in accordance with the legislation in force at the time of access;

e) There is a court order issued by a competent authority requiring or authorizing its publication;

f) Publication is required for reasons of national security and public health;

g) It is transmitted between public-law entities and between such entities and subjects of international law, in accordance with treaties and inter-institutional agreements, provided that the information is provided for the sole purpose of being used in the exercise of their respective powers.

If the government agency or entity to which the request for access to information is addressed determines that such access could interfere with the right to personal data protection, it must notify the data subject concerned within no more than three business days of receiving the request.

The data subject shall have five business days to file a reasoned objection to the request for access to the personal data concerning him or her. If the data subject files an objection based on the right to the protection of their personal data within the statutory time limit, the government agency or entity receiving the request for access must seek a non-binding opinion from the supervisory authority regarding the compatibility of the request for access to information with an adequate level of personal data protection. The supervisory authority must issue its opinion within five business days.

In the event of an objection, State Agencies and Entities shall have five business days to resolve the request for access to information, counting from the receipt of the opinion from the supervisory authority or from the expiration of the statutory deadline for the supervisory authority to issue it.

If the request for access is deemed valid despite the data subject's objection, the government agency or entity shall notify the data subject and the requester of the requested data or documents within three business days. In cases of total or partial denial of access or failure to respond within the timeframe indicated above, the requester may promptly file a lawsuit, in accordance with Title V of Law No. 5282/2014, "ON CITIZENS' FREE ACCESS TO PUBLIC INFORMATION AND GOVERNMENT TRANSPARENCY."

E & Co.
New
York

Article 25. Exchange of Personal Data Among Public Institutions.

The disclosure of personal data between public institutions shall be lawful provided that:

1. The public institution responsible for the database has obtained the data in the exercise of its legally assigned 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 falls within the scope of its authority;

3. The data involved are appropriate, proportionate, and do not exceed what is necessary in relation to this latter purpose;

4. The data subject has given consent, or the exceptions set forth in Article 20 of this law apply.

TITLE III
RIGHTS RELATED TO PERSONAL DATA

Sole Chapter
On the Rights of Data Subjects.

Article 26. General Provisions on the Exercise of Rights.

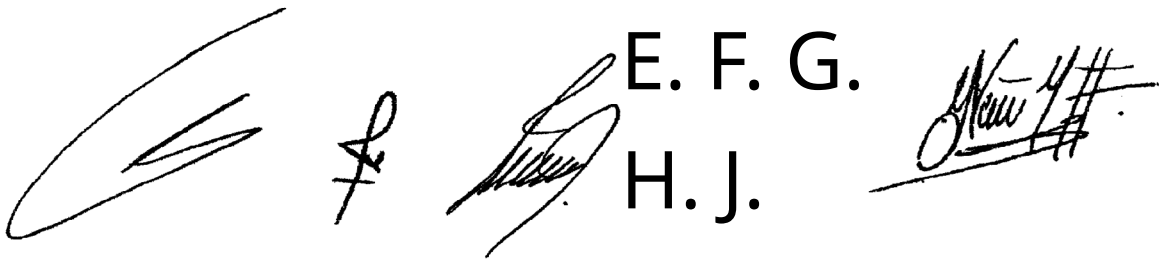
Without prejudice to the other rights arising from the provisions of this Act, the data subject or his or her representative may, at any time, request from the data controller or processor access to, rectification of, erasure of, objection to, and portability of the personal data concerning him or her.

The exercise of any of the aforementioned rights is not a prerequisite for, nor does it preclude, the exercise of another.

The data controller must establish simple, expeditious, accessible, and free means and procedures that allow the data subject to exercise their rights. The data subject's request must be addressed by the data processor or data controller within a maximum period of thirty calendar days from the date the request is submitted, unless the regulations under this law provide for a shorter period.

If the deadline expires without the request being granted or if, in the data subject's opinion, the response is insufficient, the data subject may file a complaint with the supervisory authority or, if applicable, may file a habeas data action.

If the data subject chooses to file a habeas data action, or has previously done so, he or she may not initiate proceedings before the supervisory authority. The exercise of the rights provided for in this Chapter is inalienable.



BC

LAW No. 7593

Article 27. Right to Information.

The data subject has the right to receive sufficient and easily accessible information, in clear, simple, and easily understandable language—particularly if it is intended for children, adolescents, or persons with disabilities—regarding how their personal data is processed, whether or not they provided it directly.

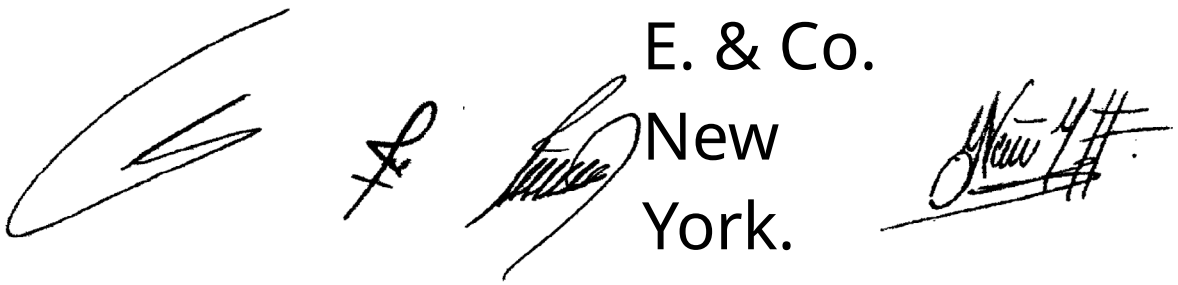
The data controller shall provide the data subject, at the time the data is collected, with at least the following information:

1. The categories of personal data that will be processed;
2. The identity and contact information, which shall include, at a minimum, the legal address, telephone number, and email address or equivalent channel;
3. The legal basis and purposes of the processing to which their personal data will be subject;
4. Any international transfers of personal data that the data controller intends to carry out, including the recipients or categories of recipients and the purposes for which such transfers are made;
5. The existence, form, and mechanisms or procedures through which you may exercise your rights of access, rectification, objection, erasure, and portability;
6. The retention period for personal data, or, failing that, the criteria used to determine the retention period;
7. The existence of automated decision-making, including profiling, and, at least in such cases, meaningful information about the logic involved, without this affecting the intellectual property rights of the data controller;
8. Where applicable, the source of the personal data when the data controller has not obtained it directly from the data subject;
9. The right to lodge a complaint with the supervisory authority.

The information provided, as well as any communication or action taken, must be provided free of charge. When requests are manifestly unfounded or excessive, particularly due to their repetitive nature, the data controller may: a) charge a reasonable fee based on the administrative costs incurred to provide the information or communication or to carry out the requested action, or b) refuse to act on the request.

The data controller bears the burden of proving that the request is manifestly unfounded or excessive.

The data controller must keep detailed records of denied requests and the reasons for such denial.



BC

Article 28. Right of Access.

The data subject shall have the right to request and obtain access to their personal data held by the data controller or processor and/or a copy thereof, upon verification of their identity. The information must be provided in a clear, intelligible manner, free of encryption, and, if necessary, accompanied by an explanation of the terms used, in language understandable to the data subject.

Under no circumstances may the report disclose data belonging to third parties, even if such data is related to the data subject, unless it has been provided by the data subject.

Article 29. Right to Rectification.

The data subject shall have the right to obtain from the data controller the rectification of their personal data when such data is false, erroneous, incomplete, or out of date.

In the event of an international transfer of erroneous or outdated data, the data controller must notify the recipient of the rectification within five business days of becoming aware of the falsity, error, inaccuracy, or outdated nature of the data.

During the process of verifying and rectifying the error, inaccuracy, falsity, or outdated nature of the information in question, the data controller must block the data or, when providing information regarding it, indicate that it is under review due to such circumstances.

Article 30. Right to Object.

The data subject shall have the right to object, at any time, for reasons related to their particular situation, to the processing of personal data concerning them, including profiling based on such provisions.

When the data subject objects to the processing of their personal data, such processing shall cease within ten business days of the submission of the objection request, unless the data controller demonstrates compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or the processing is necessary for the recognition, exercise, or defense of a right in legal proceedings.

When the data subject objects to processing for direct marketing purposes, including profiling to the extent that it is related to such marketing, their personal data shall no longer be processed for those purposes within fifteen business days of the submission of the objection request.

Article 31. Right to Erasure.

The data subject has the right to obtain from the data controller the erasure of their personal data without undue delay, so that the data controller ceases to process such data, in the following cases:

1. When the ~~personal data~~ has been processed unlawfully;
2. When ~~the~~ personal data is no longer necessary in relation to the purpose for which it was ~~collected~~ or processed;

BC

in relation to
the purpose for

3. When the retention period for personal data has expired:

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

5. When the data subject 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 to comply with a legal obligation.

Deletion shall not take place when it could prejudice the right to information and freedom of expression or the duly verified legitimate interests of third parties; when duly substantiated reasons of public interest for the processing of the data in question prevail; or when the personal data must be retained for the periods provided for in the applicable mandatory legal provisions.

Article 32. Right to Data Portability.

When personal data is processed electronically or by automated means, the data subject may request that their personal data be transferred directly from one data controller to another in accordance with technical regulations.

This right shall not apply when:

1. Exercising this right imposes a duly demonstrated excessive or unreasonable financial or technical burden on the data controller or processor;

2. It infringes upon the privacy of another data subject;

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

4. The data in question has already been anonymized by the data controller.

Article 33. Rights Regarding Automated or Semi-Automated Individual Decisions.

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

The data controller must provide, upon request, clear, complete, and adequate information regarding the criteria and procedures used for the automated decision, while respecting the data subject's trade and industrial secrets or those that the data subject is legally or contractually obligated to keep confidential.

The data controller must take appropriate ~~measures~~ to safeguard the data subject's rights. This right does not ~~preclude~~ or replace the exercise of any other rights that may apply.

BC & John New York

LAW No. 7593

TITLE IV
ON THE CONTROL AND SUPERVISION AUTHORITY AND ITS POWERS

Chapter I
On the Control and Supervision Authority.

Article 34. Control and Supervision Authority. Legal Status.

The National Agency for the Protection of Personal Data is hereby established as a decentralized unit within the organizational structure of the Ministry of Information and Communication Technologies, with the status of a National Directorate, and shall serve as the control and supervisory authority for this law.

The National Agency for the Protection of Personal Data shall enjoy functional autonomy and independence and shall have sufficient powers of decision-making, action, regulation, supervision, control, sanctioning, and all other functions necessary for the enforcement of this Act, acting in accordance with the principles established therein.

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

The organizational and administrative structure of the National Agency for the Protection of Personal Data shall be established in the regulatory decree implementing this law and shall include, at a minimum, the Director General as the highest authority and a deputy director.

The National Agency for the Protection of Personal Data shall have broad authority to issue the internal regulations necessary to supplement the regulatory provisions expressly mentioned in this Act.

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 established as the supervisory authority under this law and shall have sufficient powers and authority to act, make decisions, issue resolutions, regulate, promote, investigate, supervise, inspect, control, impose sanctions, and take any other actions necessary to ensure its effective enforcement, as well as the effective exercise and respect for 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. To supervise, monitor, and evaluate the activities carried out by the data controller and data processor;

2. To assist and advise individuals who request it regarding the scope of this law and the legal means available to them for the defense of their rights;

3. To issue the rules, regulations, guidelines, and guiding criteria that must be observed in the performance of the activities covered by this law;

BC

4. Process any complaints and/or allegations filed, take preliminary actions, and, if deemed appropriate, initiate administrative proceedings for alleged violations of this law and its implementing regulations;

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

6. To request information relevant to its area of jurisdiction from public and private institutions, which must respond within the timeframe established for that purpose;

7. Impose administrative sanctions, following an investigation, for violations of the provisions of this law and its regulations;

8. Approve binding self-regulatory mechanisms or codes of conduct and oversee compliance with them;

9. Issue standard data protection clauses;

10. Develop and maintain a list regarding the requirement for data protection impact assessments;

11. Establish data protection certification mechanisms to provide the required safeguards;

12. Assess the adequacy of the receiving country or entity in international data transfers;

13. Request information from data protection officers, under the terms set forth in this law and its implementing regulations;

14. Promote cooperation with personal data protection authorities in other countries, including the ability to enter into international administrative and non-regulatory agreements on the matter;

15. Issue non-binding technical opinions when, in administrative or judicial proceedings, the right of access to public information and the right to personal data protection must be weighed against one another, where there are doubts regarding their application;

16. Prepare annual management reports on its activities;

17. Collaborate with State Agencies and Entities on matters within its jurisdiction;

18. To exercise the functions and powers required for the proper implementation of the provisions in force set forth in Law No. 6534/2020 "ON THE PROTECTION OF PERSONAL CREDIT DATA," or any law that may replace it, with the exception of those expressly assigned to the Central Bank of Paraguay and falling within its jurisdiction.

19. Any other functions assigned to it by this law or its implementing decree, as well as those ~~necessary~~ to ensure its effective implementation and compliance.

Compliance
C
F. M.
Juan Y.

BC

LAW No. 7593

Article 36. 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 consist of:

1. The funds allocated to it annually in the General National Budget, which shall be incorporated into the budget of the Ministry of Information and Communication Technologies and must be fully itemized therein;

2. Revenues derived from fines imposed in the exercise of its sanctioning powers established in this law; and,

3. Funds derived from agreements and/or arrangements, grants, loans, financing, contributions, donations, bequests, or any other source, whether domestic or international, provided that such funds do not involve a conflict of interest.

The revenues listed in paragraph 2 shall be deposited into a special account of the Ministry of Information and Communication Technologies designated exclusively for the resources of the National Agency for the Protection of Personal Data.

Under no circumstances may the aforementioned resources be used for any purpose other than that established in this law and its regulations.

Chapter II
On the Management 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 Director, to whom he or she may delegate functions in the manner and under the conditions established in this law and its regulations.

The Director General and the Deputy Director General shall be appointed by decree of the Executive Branch, based on a shortlist of three candidates proposed by the Ministry of Information and Communication Technologies, following a public competitive selection process.

The Agency shall exercise its functions exclusively, independently, and objectively; the hierarchical authority of the highest official of the Ministry of Information and Communication Technologies shall be limited to matters not related to the functions falling under the exclusive jurisdiction of the National Agency for the Protection of Personal Data, except in cases of administrative proceedings.

Article 38. Powers and Duties of the Director General of the National Agency for the Protection of Personal Data.

The powers and duties of the Director General of the National Agency for the Protection of Personal Data are as follows:

1. To comply ~~with~~ and ensure compliance ~~with~~ this law and its regulatory provisions;

2. ~~To exercise~~ regulatory authority in accordance with the terms set forth in this law;

esta ley

BC

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

4. To represent the National Agency for the Protection of Personal Data, with the authority to sign documents and grant general and special powers of attorney for judicial and administrative proceedings on behalf of the Agency;

5. To appoint, remove, or transfer Agency personnel and to establish office hours and work shifts, in accordance with the provisions of the relevant regulations;

6. Enter into contracts and agreements with national, binational, and international institutions and agencies, whether public or private, in coordination with the Ministry of Foreign Affairs when appropriate, to fulfill the objectives and purposes of the Agency and this law;

7. Order technical or administrative inspections and/or audits of entities subject to this law;

8. Order the initiation of administrative proceedings and the imposition of sanctions when such actions are warranted as a result of such proceedings;

9. Appear annually before the Committee on Science, Technology, Innovation, and the Future of the Honorable Senate and before the Committee on Science and Technology of the Honorable Chamber of Deputies to report on its management and present its plans and priorities for the future;

10. Perform any other function related to the protection of personal data within the framework of this Act.

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

The requirements for holding the position of Director General and Deputy Director General of the National Agency for the Protection of Personal Data are as follows:

1. Be a Paraguayan national, at least thirty years of age;

2. Hold a bachelor's degree;

3. Demonstrate proven qualifications, competence, and experience in the field of personal data protection, ensuring independence of judgment, efficiency, objectivity, and impartiality in the performance of their duties;

4. Be of good repute;

5. Not have been convicted of any criminal offense under national law, for the duration of the sentence; or, if the candidate has availed themselves of alternative methods of concluding criminal proceedings or of a probationary suspension of the sentence, for the duration of the suspension of the proceedings or the sentence;

6. Not have been disqualified from holding public office, for the duration of the disqualification.

BC

eligibility.
G
&
M
Nau Y#

Article 40. Term of Office and Removal.

The Director General of the National Agency for the Protection of Personal Data and the Deputy Director General shall serve a three-year term and may be reappointed for subsequent terms.

Furthermore, they shall be removed from office prior to the expiration of their term under the following circumstances:

a) Removal due to poor performance of their duties. The administrative proceeding to verify the grounds for removal shall be conducted in accordance with the provisions of the law governing the civil service;

b) Resignation submitted to the President of the Republic;

c) Supervening inability to perform their duties;

d) A final conviction for the commission of a criminal offense punishable by imprisonment. Under no circumstances shall the positions of Director General or Deputy Director General of the National Agency for the Protection of Personal Data be considered positions of trust or subject to free appointment.

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

TITLE V
ADMINISTRATIVE REMEDIES

Chapter I
Misconduct and Its Consequences.

Article 41. Administrative Remedies.

Without prejudice to the constitutional guarantee of habeas data, the data subject may file complaints or reports with the Agency to enforce their rights, in the manner and under the conditions set forth in this law and its regulations.

The Agency may initiate proceedings to verify compliance with the provisions of this Act at the request of the data subject, their legal or authorized representative, a third party with a legitimate interest, or on its own initiative.

In such proceedings, the provisions of this law, its implementing regulations, and the provisions of Law No. 6715/2021 "ON ADMINISTRATIVE PROCEEDINGS" or any law that may replace it shall apply, to the extent applicable. Without prejudice to administrative remedies, the data subject may seek judicial relief to obtain compensation when he or she has suffered damages as a result of a violation of his or her rights to the protection of personal data, in accordance with the provisions of this Act.

E & M New H.

BC

Article 42. Corrective Measures.

In the event of noncompliance with the provisions set forth in this law, without prejudice to any administrative penalty that may be imposed, the Agency may issue corrective measures with the aim of eliminating, preventing, or halting the effects of the violations, as well as deterring repeat offenses.

Corrective measures may consist of, among other things:

1. The cessation or suspension of processing, under certain conditions or for specific periods;
2. The deletion of the data;
3. The imposition of technical, legal, and organizational measures to ensure the proper processing of personal data.

An appeal against corrective measures shall not have suspensive effect on their enforcement.

Article 43. Conduct Constituting Misconduct.

Any action or omission that constitutes a breach of the provisions set forth in this law and its implementing regulations, as well as those issued by the Agency within the scope of its authority to enforce them, shall be considered a violation.

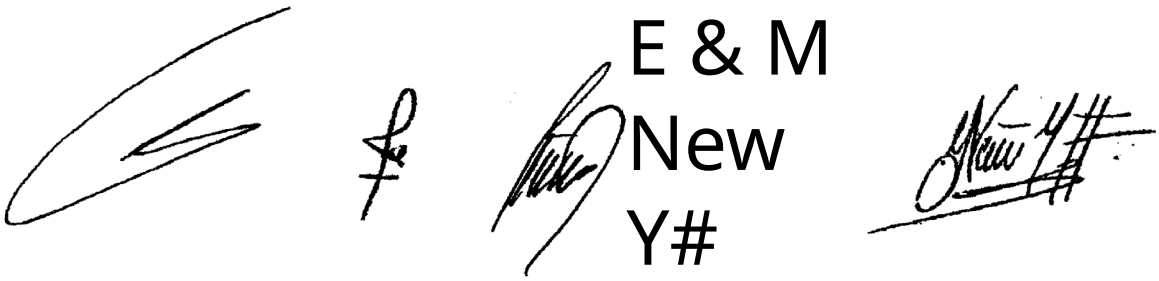
Misconduct is classified as minor or serious.

The administrative actions and measures taken as a result of the aforementioned conduct are independent of any actions or measures taken in court in cases where such conduct simultaneously gives rise to civil or criminal liability; the same applies to any remedies, penalties, or convictions that may be imposed in each case.

Article 44. Minor Offenses.

The following violations are considered minor offenses and shall be subject to a one-year statute of limitations:

1. Collecting personal data for use in a database without providing the data subject with sufficient and comprehensive information, in accordance with the technical specifications set forth in the regulations implementing this law;
2. Collecting, storing, and transmitting personal data of third parties through insecure mechanisms or those that in any way fail to guarantee the security and integrity of the data;
3. Failing to honor the rights of access, rectification, erasure, restriction of processing, or data portability in processing operations where the identification of the data subject is not required, when the data subject, in order to exercise those rights, has provided additional information that allows for their identification;



BC

4. Failure by the data processor to comply with the provisions set forth in the contract or legal instrument governing the processing or with the instructions of the data controller, unless the data processor is legally obligated to do so under other laws of the Republic of Paraguay and this Act, or in cases where such failure was necessary to prevent a violation of data protection laws and the data controller or data processor had been notified thereof;

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

6. Unjustifiably refusing to grant a data subject access to their data contained in files and databases, for the purpose of verifying the quality, collection, storage, and use of such data in accordance with this law;

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

8. Failing to make available personal data protection policies related to the processing of personal data;

9. Failure to comply with legal or regulatory obligations, provided that such failures have not been classified as serious violations.

Article 45. Serious Offenses.

The following violations are considered serious offenses and shall be subject to a two-year statute of limitations:

1. Transferring personal data to other individuals or companies in violation of the rules established in this law:

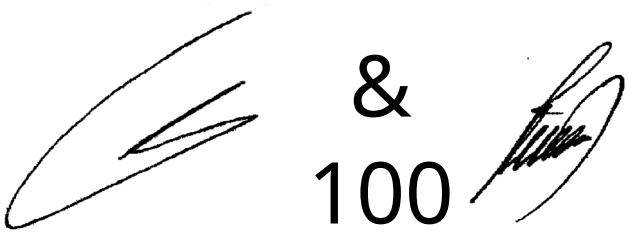
2. Repeatedly and unjustifiably refusing to grant a data subject access to their data contained in files and databases, for the purpose of verifying the quality, collection, storage, and use of such data in accordance with this Act;

3. Unjustifiably refusing to delete or correct the data of a person who has requested such action in a clear and unambiguous manner:

4. Processing the personal data of a minor without obtaining the minor's consent, when the minor has the capacity to do so, or the consent of the minor's legal guardian or custodian;

5. Failing to demonstrate that reasonable efforts were made to verify the validity of the consent provided by a minor or by the holder of parental authority, guardianship, or custody over the minor;

6. Preventing, obstructing, or repeatedly failing to address the rights of access, rectification, erasure, or data portability in processing operations where the identification of the data subject is not required, when the data subject, in order to exercise those rights, has provided additional information that allows for their identification;



Mou Y#

LAW No. 7593

7. Failure to adopt the technical and organizational measures appropriate for the effective application of the principles of data protection by design, as well as failure to implement the necessary safeguards in the processing;

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

9. Failure to adopt appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the processing;

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

11. Failure to comply with the obligation to designate a representative of the data controller or processor not established in the Republic of Paraguay, as provided for in Article 12 of this law;

12. Entrusting data processing to a third party without first entering into a contract or other formally appropriate written legal instrument, as required by this law;

13. Subcontracting data processors without the prior authorization of the data controller or without informing the data controller of changes in the subcontracting arrangement when such notification is legally required;

14. Failure to comply with the data processor's duty to notify the data controller of any security breaches of which it 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. Processing personal data without having conducted an assessment of the impact of processing operations on the protection of personal data in cases where such an assessment is required;

17. The processing of personal data without first consulting the supervisory authority in cases where the law establishes the obligation to conduct such a consultation;

18. Failure to comply with the obligation to appoint a data protection officer when such appointment is required in accordance with the provisions of this Act and its implementing regulations;

19. Failing to enable the effective participation of the data protection officer in all matters relating to the protection of personal data, failing to provide due cooperation, or interfering with the performance of the data protection officer's duties;

20. The use of a false national or international seal or certification regarding data protection, or the use of such seals or certifications after their validity has expired;

BC

& time
New
4#

LAW No. 7593

21. Collecting, storing, and transmitting personal data of third parties through insecure mechanisms or those that in any way fail to guarantee the security and integrity of the data;

22. Failure by data controllers or processors to comply with the notification obligation regarding the rectification or erasure of personal data required by this law;

23. Failure to comply with the requirements of this Act regarding the validity of consent;

24. Failure to fulfill the duty to inform the data subject about the processing of their personal data in accordance with the provisions of Article 27 of this law;

25. Requiring the payment of a fee for the exercise of any of the rights established in Title III, Sole Chapter: "Rights of Data Subjects" of this law;

26. The collection, storage, transmission, or any other use of sensitive data by private individuals or legal entities without meeting one of the legal requirements established in current legislation;

27. Obtaining, from data subjects or third parties, a person's personal data through deception, violence, or threats;

28. To disclose information contained in a personal database that the discloser is legally obligated to keep confidential;

29. Knowingly providing a third party with false or inaccurate information contained in a data file;

30. Transferring personal information of Paraguayan residents or foreigners located in the country to databases in third countries without the consent of the data subjects when such consent is required;

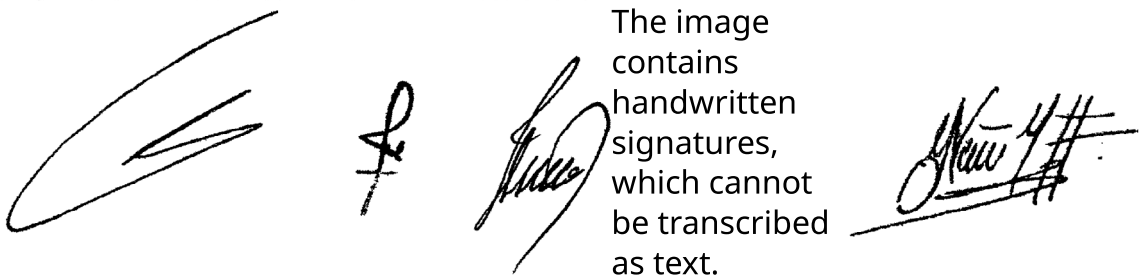
31. Processing personal data relating to criminal convictions, offenses, or related security measures outside the cases permitted by current legislation;

32. Violating the principle of confidentiality established in this law;

33. Failing to provide the supervisory authority with access to the personal data, information, premises, equipment, and processing resources required by that authority to exercise its investigative powers;

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

35. Deliberately reversing an anonymization or pseudonymization process in order to allow for the re-identification of data subjects;



BC

36. Collecting, storing, transmitting, or otherwise using personal data without meeting one of the legal requirements established in this law;

37. Failure to conduct an impact assessment prior to the implementation of data processing operations that may pose significant risks to the rights of data subjects, as provided for in this Act.

Article 46. Administrative Sanctions.

The sanctions to be imposed by the Agency for proven violations may consist of:

1. A warning, specifying the deadline and manner for taking corrective measures, if applicable;

2. Fines ranging from twenty to two thousand five hundred minimum daily wages for various unspecified 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 to up to five thousand minimum daily wages for various unspecified activities in the Republic of Paraguay.

   2.2. In the case of violations committed in the processing of sensitive data of children and adolescents, the amounts of the penalties may be increased to up to ten thousand minimum daily wages for various unspecified activities in the Republic of Paraguay.

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

The various types of penalties may be applied individually or cumulatively.

The Agency is authorized to issue supplementary and/or clarifying regulations regarding this article.

Article 47. Criteria for the Imposition of Administrative Penalties.

Administrative penalties shall be determined based on the following criteria:

1. The severity and nature of the violations and the harm or danger to the legal interests protected under this law;

2. The good faith of the offender or the express acknowledgment or acceptance by the person under investigation of having committed the violation prior to the imposition of the applicable sanction;

3. The degree of the offender's liability, as well as whether the violation was committed intentionally or through negligence;

4. The economic advantage or ~~benefit~~ obtained or sought by the offender as a result of committing ~~the violation~~;

& [Signature] New Y#

BC

5. The offender's financial situation;

6. Whether the conduct is a repeat offense;

7. The offender's cooperation with the supervisory authority's investigation;

8. The repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing harm, aimed at the secure and appropriate processing of data;

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

10. The prompt adoption of corrective measures;

11. Other factors that the supervisory authority may consider, depending on the nature of the case.

Article 48. Statute of Limitations on the Enforcement of Sanctions.

The statute of limitations for the enforcement of sanctions shall be two years from the date the decision imposing the sanction becomes final.

Article 49. Payment of Fines.

The amount of the fines must be paid within thirty business days from the date of notification.

The regulations shall establish the consequences of noncompliance, including interest, as well as any other relevant aspects for the effective enforcement of the imposed sanction.

Article 50. Alleged Noncompliance by Public Institutions.

If the supervisory authority detects an alleged violation of the provisions of this law by public institutions, it shall issue a warning and a decision establishing corrective measures that must be adopted to cease or correct the effects of the violation.

The resolution ordering the implementation of such measures shall be notified to the highest authority of the public institution where the violation occurred and to the affected data subject, if any.

Notwithstanding the provisions of the preceding paragraphs, the public institution, following an analysis of the facts in question, shall take the appropriate measures with respect to those allegedly responsible, including, but not limited to, the initiation of administrative proceedings for the imposition of disciplinary sanctions in accordance with the procedure established for that purpose.

E & M
New
Y#

BC

LAW No. 7593

Chapter II
On the Filing of Complaints or Claims.

Article 51. Filing a Complaint with the Supervisory Authority.

The data subject or their legal representative may file a complaint or claim, free of charge, through any means authorized for that purpose by the supervisory authority, clearly stating the content of their request and the provisions of this law that they believe have been violated, and providing proof that they have submitted the corresponding request to the data controller or processor responsible for their data, along with the response, if any.

The complaint must be filed within fifteen business days following the date on which the data controller or processor communicated its response to the request, or at any time if the established deadline has expired without a response from the data controller or processor. The response, if any, must be attached to the complaint.

Article 52. Decision by the supervisory authority.

Upon receiving a complaint or report, the supervisory authority may, by means of a reasoned decision:

a) Dismiss the complaint or report filed;

b) If it determines that the data subject is entitled to relief, require the data controller or processor to ensure the effective exercise of the protected rights, and the data controller or processor must provide written confirmation of such compliance to the supervisory authority within fifteen business days of its completion;

c) If a violation is verified, impose the sanctions provided for in this law.

Chapter III
On the Investigation of Offenses and the Imposition of Administrative Sanctions.

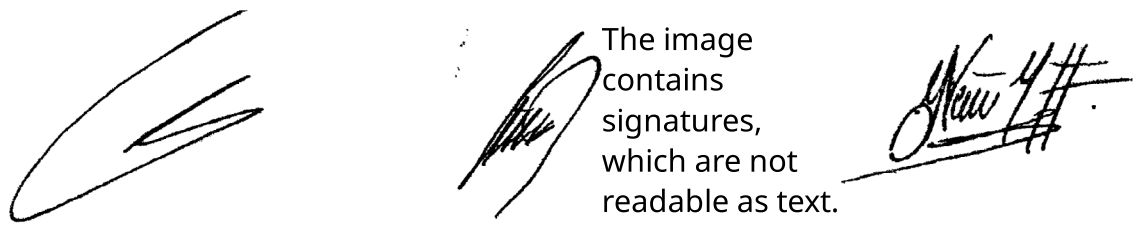
Article 53. Procedure for the Verification of Violations and the Imposition of Sanctions.

Violations of the provisions of this law and its regulations must be proven in an administrative proceeding.

The initiation of the proceedings shall be ordered by resolution of the Director General of the Agency and shall contain a complete account of the facts, acts, or omissions attributed to the alleged offender, as well as the appointment of the Investigating Judge from among those serving in the supervisory authority.

The regulations shall establish the procedure and time limits to be followed, including the timeframe within which the Investigating Judge must submit his or her final opinion to the Director General and the timeframe for issuing the corresponding resolution. All other aspects of the procedure shall be governed by the provisions of Law No. 6715/2021 "ON ADMINISTRATIVE PROCEDURES" or any law ~~that~~ may replace it.

BC



Article 54. Administrative Precautionary Measures.

Once disciplinary proceedings have been initiated, a reasoned decision may order the adoption of provisional measures to ensure the effectiveness of the final decision that may result from such proceedings.

Article 55. Motion for Reconsideration.

An appeal for reconsideration may be filed against any non-regulatory administrative decision or act issued by the Agency; such appeal must be filed with the Agency's Director General.

The administrative remedy is exhausted with the decision of the Director General of the Personal Data Protection Agency. The Ministry of Information and Communication Technologies shall have no jurisdiction to process requests or other proceedings related to personal data protection rights or other matters within the Agency's jurisdiction.

Article 56. Administrative Litigation.

Administrative litigation may be filed with the Court of Auditors within the time limit established by Law No. 6715/2021 "ON ADMINISTRATIVE PROCEDURES" or any law that may replace it.

The motion for reconsideration and the administrative lawsuit shall have suspensive effect in cases where they are filed against decisions imposing administrative sanctions; however, they shall not suspend any administrative injunctions that have been issued or any corrective measures intended to prevent harm from occurring.

TITLE VI
FINAL AND TRANSITIONAL PROVISIONS

Article 57. Entry into Force.

This law shall enter into force twenty-four months after its official publication.

Article 58. Assumption of Functions and Powers.

Any reference in Law No. 6534/2020 "ON THE PROTECTION OF PERSONAL CREDIT DATA" to the Secretariat for Consumer and User Protection shall, as of the effective date of this law, be understood as a reference to the National Agency for the Protection of Personal Data.

Article 59. Repeals.

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

OS".
G & M
New Y#

BC

Article 60. Regulations.

The Executive Branch shall issue regulations for this law within twenty-four months from the date of its publication in the Official Gazette.

Article 61. Forward to the Executive Branch.

The Bill was approved by the Honorable Chamber of Deputies on the **fourteenth day of October, two thousand twenty-five**, and by the Honorable Senate on the **fifth day of November, two thousand twenty-five**, and is hereby enacted, in accordance with the provisions of Article ~~207~~, paragraph 2) of the Constitution.

Pursuant to Article 207, paragraph 2) of the Constitution.
Raúl Luis Latorre Martínez
President
Honorable Chamber of Deputies
Basilio Gustavo Núñez
President
Honorable Chamber of Senators
María Constanza de Benítez
Parliamentary Secretary
Hermelinda Alvarenga de Ortega
Parliamentary Secretary

Asunción, November 27, 2025.
Let this be a Law of the Republic; let it be published and entered into the Official Register.
The President of the Republic

PRESIDENCY OF THE REPUBLIC OF PARAGUAY
TETÃ MBURUVICHA GUASU RENDA

Santiago Peña Palacios

Gustavo Emigdio Villate Samaniego
Minister of Information and Communication Technologies