DIARIO OFICIAL DEL BICENTENARIO

El Peruano 199 años

SATURDAY,
November 30, 2024

Founded on October 22, 1825 by the liberator Simon Bolivar

MINISTRY OF
JUSTICE AND HUMAN RIGHTS

SUPREME DECREE No. 016-2024-JUS

SUPREME DECREE THAT APPROVES THE REGULATION OF LAW No. 29733, LAW DATA PROTECTION PERSONAL

LEGAL RULES

SPECIAL SEPARATE

SUPREME DECREE THAT APPROVES THE REGULATION OF LAW Nº 29733, LAW OF PROTECTION OF PERSONAL DATA

SUPREME DECREE Nº 016-2024-JUS

THE PRESIDENT OF THE REPUBLIC

CONSIDERING:

That, numeral 6 of article 2 of the Constitution Peruvian policy states that every person has the right to have information services, whether computerized or not, public or private, not provide information that affects personal and family privacy;

That, Article 1 of Law No. 29733, the Personal Data Protection Law, states that the purpose of said Law is to guarantee the fundamental right to the protection of personal data, provided for in paragraph 6 of Article 2 of the Political Constitution of Peru, through its adequate treatment, within a framework of respect for the other fundamental rights recognized therein;

That, Article 32 of the aforementioned Law, provides that the Ministry of Justice and Human Rights exercises the National Authority for the Protection of Personal Data;

That, by Supreme Decree No. 003-2013-JUS, the Regulation of Law No. 29733, the Personal Data Protection Law, is approved, which in its article 1 states that its purpose is to develop the aforementioned Law, in order **to guarantee the fundamental right to the protection of personal data, regulating adequate treatment, both by public entities and by institutions belonging to the private sector;**

That, Legislative Decree No. 1353, Legislative Decree that creates the National Authority for Transparency and Access to Public Information, Strengthens the Personal Data Protection Regime and the Regulation of Interest Management, through its third complementary modifying provision, reformed some provisions of Law No. 29733, Personal Data Protection Law;

That, literal a) of paragraph 4.2 of article 4 of Emergency Decree No. 007-2020, Emergency Decree that approves the Digital Trust Framework and provides measures for its strengthening, establishes that one of the areas of digital trust in the digital environment is the protection of personal data and transparency, being the Ministry of Justice and Human Rights, who exercises the National Authorities of Transparency, Access to Public Information and Protection of Personal Data, and within the framework of its functions and powers, regulates, directs, supervises and evaluates the matter of transparency and protection of personal data;

That, by Legislative Decree No. 1412, Legislative Decree that approves the Digital Government Law, in its paragraphs 5.3 and 5.10 of article 5, the principle of privacy by design is established as the guiding principles of the digital government governance framework, by which, in the design and configuration of digital services, preventive measures of a technological, organizational, human and procedural nature are adopted; as well as the principle of adequate level of protection for personal data, by which the processing of personal data must be carried out in accordance with the provisions of the Personal Data Protection Law and its Regulations;

That, due to changes in the regulatory framework and the contemporary challenges posed by the emergence of new digital technologies, it is necessary to approve a new Regulation of Law No. 29733, the Personal Data Protection Law, which will allow the country to have a modern and solid regulatory framework that guarantees adequate protection of citizens' rights against the risks generated for personal data by the use of new digital technologies;

That, by Ministerial Resolution No. 0270-2023-JUS, published on August 26, 2023 in the Diario Official **El Peruano, the publication of the Draft Regulation of Law No. 29733, Law on the Protection of Personal Data and the Statement of Reasons that supports it, was arranged for a period of thirty (30) calendar days, in** order **to receive suggestions, comments or recommendations from public entities, private institutions, civil society organizations, as well as natural persons in general.**

That the General Directorate of Transparency, Access to Public Information and Protection of Personal Data received, processed and systematized the suggestions, comments and/or recommendations submitted by citizens and various institutions, both private and public;

In accordance with the provisions of section 6 of article 2 and section 8 of article 118 of the Political Constitution of Peru; Law No. 29733, the Personal Data Protection Law; Law No. 29158, the Organic Law of the Executive Branch; Emergency Decree No. 007-2020, the Emergency Decree that approves the Digital Trust Framework and provides measures for its strengthening; Law No. 29809, the Law on the Organization and Functions of the Ministry of Justice and Human Rights; the Regulations on the Organization and Functions of the Ministry of Justice and Human Rights, approved by Supreme Decree No. 013-2017-JUS; and the Regulations of the Framework Law for the Production and Systematization of Legislation, approved by Supreme Decree No. 007-2022-JUS;

With the approving vote of the Council of Ministers;

DECREE:

Article 1. Approval

The Regulation of Law No. 29733, Personal Data Protection Law, is approved, the text of which is composed of one (1) Preliminary Title, three (3) Titles, one hundred thirty-five (135) articles, six (6) Final Complementary Provisions and two (2) Transitional Complementary Provisions, which form an integral part of this Supreme Decree.

Article 2. Publication

This Supreme Decree and the Regulation approved in article 1 are published on the Single Digital Platform of the Peruvian State for Citizen Guidance (www.gob.pe) and on the digital headquarters of the Ministry of Justice and Human Rights and the Presidency of the Council of Ministers, on the same day of publication of this regulation in the Official Gazette **El Peruano.**

Article 3. Financing

The implementation of the provisions of this Supreme Decree and the Regulations approved in Article 1 are subject to the budgetary availability of the involved documents, without requiring additional resources from the Public Treasury.

Article 4. Endorsement

This Supreme Decree is countersigned by the Minister of Justice and Human Rights.

SUPPLEMENTARY PROVISION
REPEAL

Sole. Repeal

Supreme Decree No. 003-2013-JUS, which approves the Regulations of Law No. 29733, the Personal Data Protection Law, is hereby repealed.

Given at the Government House, in Lima, on the twenty-ninth day of the month of November of the year two thousand twenty-four.

Dina Ercilia Boluarte Zegarra
President of the Republic

Eduardo Melchor Arana Ysa
Minister of Justice and Human Rights

REGULATION OF LAW Nº 29733, PERSONAL DATA PROTECTION LAW

PRELIMINARY TITLE

Article I. Purpose

The purpose of this Regulation is to establish provisions for the proper application of Law No. 29733, the Personal Data Protection Law, hereinafter the Law, in order to guarantee the fundamental right to the protection of personal data, regulating adequate processing by natural persons, public entities and institutions belonging to the private sector, particularly in the digital environment.

Article II. Purpose

The purpose of this Regulation is to guarantee adequate protection of the fundamental right to the protection of personal data established in paragraph 6 of article 2 of the Political Constitution of Peru and Law No. 29733, the Personal Data Protection Law, against the risks that may arise from the use of new digital technologies.

Article III. Definitions

For the application of this Regulation, without prejudice to the definitions contained in the Law, the following definitions must be understood in addition :

1. Personal data bank: It is the set of data of natural persons, computerized or not, and structured according to specific criteria , which allows access without disproportionate effort to personal data, whether centralized, decentralized or distributed functionally or geographically .

2. Blocking: This is the measure that consists of the identification and reservation of personal data by adopting technical and organizational measures to prevent its processing, including its visualization, during the period in which any request for update, inclusion, rectification or deletion is being processed, in accordance with the provisions of the third paragraph of article 20 of the Law.

It is also provided as a preliminary step to cancellation for the time necessary to determine potential liabilities in relation to the processing during the legal or contractual limitation period.

3. Cancellation: It is the action or measure that in the Law is described as deletion, when it refers to personal data, which consists of eliminating or suppressing personal data.

4. Personal data: This is numerical, alphabetical, graphic , photographic , acoustic, personal habits, location, online identifiers, or any other type of information concerning the physical, economic, cultural, or social aspects of natural persons that identifies them or makes them identifiable . Identifiable information is considered to be information that can be verified directly or indirectly by combining data through means that can be reasonably used.

5. Personal data related to health: This is information concerning a person's past, present, or expected physical or mental health, including information derived from a medical procedure, the degree of disability, and genetic information.

6. Sensitive data: This is information relating to genetic or biometric data of a natural person, neuronal data, moral or emotional data, facts or circumstances of their emotional or family life, personal habits that correspond to the most intimate sphere, information relating to union membership , physical or mental health or other similar information that affects their privacy.

7. Deindexing: This is the process by which a specific URL or content on a website is removed or excluded from search engine results. This procedure, depending on the specific situation and circumstances , may be carried out by the website owner or the search engine.

8. Days: Business days.

9. General Directorate of Transparency, Access to Public Information and Protection of Personal Data: It is the body responsible for exercising the National Authority for the Protection of Personal Data referred to in Article 32 of the Law, and any of these names may be used interchangeably in this Regulation.

10. Person in charge of processing personal data: It is the natural person, legal entity under private law, or public entity that processes data on behalf of or on behalf of the data controller or owner of the personal data bank.

11. Profiling: It is the form of automated processing of personal data that allows evaluating aspects of a natural person, in a specific and continuous manner, to analyze or predict aspects related to their professional performance, economic situation, health, personal preferences, interests, reliability , behaviors or habits, location or movements.

12. Issuer or exporter of personal data: The owner of the personal data bank or the person responsible for processing said data, located within the national territory and who transfers personal data to another country, in accordance with the provisions of this Regulation.

13. Personal data protection impact assessment: This is a proactive accountability mechanism whereby the owner of the personal data bank or data controller carries out, prior to processing, an analysis or assessment of the impact or risks involved in processing such data.

14. Transit purposes: This implies that the means are not used for the specific purpose of processing personal data, such as processing, storing, downloading, displaying and/or similar, but exclusively to pass personal data from one place to another.

15. Cross-border flow of personal data: A cross-border flow or international transfer of personal data refers to the transfer of personal data to a recipient located in a country other than the country of origin of the personal data, regardless of the medium.

in which they are located, the means by which the transfer was carried out or the treatment they receive.

16. Personal data security incident: Any breach of security that results in the destruction, loss, unlawful alteration of personal data, or unauthorized communication or exposure of such data.

17. Personal Data Officer: The person designated by the data controller or person in charge of processing personal data for the verification , advice and implementation of compliance with the legal regime on personal data protection.

18. Recipient or importer of personal data: Any natural person or legal entity under private law, including branches, subsidiaries , affiliates or similar or public entities, who receives the data in the event of an international transfer, either as the owner of the personal data bank or as the person in charge of processing it.

19. Rectification: This is an action intended to affect or modify personal data, either to update it or correct it with exact data.

20. Representative: The natural or legal person expressly designated by the owner of the personal data bank or responsible party for the purposes of processing personal data.

21. Jurisprudence Repertoire: This is the bank of judicial or administrative resolutions, fiscal opinions , arbitration awards, resolutions of ethics committees or similar, which is found in physical or digital format, and organizes, among others, personal data as a source of consultation and is usually public.

22. Data controller: The natural person, legal entity under private law, or public entity that decides on the purpose and means of processing personal data. This definition is not restricted to the owner of the data bank, but includes any person who decides on the processing of personal data, even if they are not part of a personal data bank.

23. Processing: Any operation or set of operations, whether automated or not, performed on personal data or sets of personal data.

24. Third party: Any natural person, legal entity under private law, or public entity, other than the owner of the personal data, the owner of the database or the person responsible for the processing, the person in charge of the processing, and the persons authorized to process the data under their direct authority.

The reference to "third party" in Article 30 of the Law constitutes an exception to the meaning provided in this section.

Article IV. Scope of application

4.1 This Regulation applies to the processing of personal data, even if they are not stored in a personal data bank.

4.2 It applies to all forms of personal data processing, whether carried out by natural persons, public entities or private sector institutions, regardless of the medium on which they are stored.

4.3 The existence of particular or special rules or regimes, even when they include regulations on personal data, does not exclude public entities or private institutions to which said regimes apply within the scope of the Law and this Regulation.

4.4 The provisions of the preceding paragraph do not imply the repeal or non-application of the specific rules, as long as their application does not affect the right to the protection of personal data.

Article V. Exceptions to the scope of application

5.1 The provisions of the Law and these Regulations do not apply to the following cases:

1. The processing of personal data carried out by natural persons for exclusively domestic, personal or related purposes related to their private or family life.

2. Personal data contained or intended to be contained in personal data banks of the public administration, only insofar as the current purpose of the processing is necessary for the strict compliance with powers assigned by law to the respective public entities and provided that their purpose is:

a) National defense,
b) Public safety,
c) The development of criminal activities for the investigation and suppression of crime.

5.2 In the event that the public entities referred to in numeral 2 of paragraph 5.1 of this article carry out the processing of personal data for a purpose other than that linked to the strict fulfillment of their powers, or for archiving, administrative, historical, scientific or statistical research purposes , the provisions of the Law and of this Regulation shall apply to them as relevant.

Article VI. Scope of application in and for Peruvian territory

The provisions of the Law and this Regulation apply to the processing of personal data when:

1. It must be carried out in an establishment located in Peruvian territory corresponding to the owner of the personal data bank or the person responsible for the processing.

2. It is carried out by a data processor, regardless of its location, on behalf of a personal data bank owner established in Peruvian territory or whoever is responsible for the processing.

3. The owner of the personal data bank or the responsible party is not established in Peruvian territory, but uses means located in said territory, unless such means are used solely for transit purposes that do not involve the processing of personal data. This provision covers the following cases:

3.1. The owner of the personal data bank or the data controller is not located in Peruvian territory, but carries out activities related to the offering of goods or services to personal data owners located in Peruvian territory.

3.2. The owner of the personal data bank or the person responsible for the processing is not located in Peruvian territory, but carries out activities aimed at analyzing the behavior of personal data owners located in Peruvian territory, as well as the creation of profiles that seek to predetermine behaviors, preferences, habits, or similar.

4. The owner of the personal data bank or the person responsible for the processing is not established in

Peruvian territory, but Peruvian legislation is applicable to it, by contractual provision or international law.

Article VII. Representative of the owner of the personal data bank or person responsible for the processing of personal data

7.1 For the purposes of the provisions of paragraphs 3 and 4 of article VI, unless the processing is carried out for transit purposes , the owner of the personal data bank or whoever is responsible, located in Peruvian territory or outside of it, must provide the necessary means for the effective fulfillment of the obligations provided for in the Law and the Regulations, and designate a representative in Peruvian territory or for Peruvian territory, who is the point of contact with the National Authority for the Protection of Personal Data.

7.2 The owner of the personal data bank or whoever is responsible may designate the representative, alternatively, in the following ways:

1. You may publicly disclose this in the privacy policy of the personal data bank owner or data controller; or

2. You may report this to the National Authority for Personal Data Protection, taking into account the provisions of paragraph 7.3 below.

7.3 In the event that the appointment of the representative is communicated to the National Authority for the Protection of Personal Data, the following assumptions must be taken into account:

1. For a representative in Peruvian territory: this must be done expressly through a valid document in order to materialize his representation, in accordance with articles 53 and 115 of Law No. 27444, the General Administrative Procedure Law, or any regulation that replaces it.

2. For a representative for Peruvian territory: the designation must be communicated to the Authority through the channel established by the data controller or data processor.
This representative must be accredited to manage all communications, requests from personal data holders, claims, complaints or similar arising from administrative procedures, and must specify an email address for communications and corresponding contact for such purposes .

Article VIII. Determination of establishment

8.1. In the case of natural persons, the establishment is understood to be the premises where their main business headquarters are located or where they use to carry out their activities or their domicile.

8.2. In the case of legal entities, the establishment is understood to be the premises where the main administration of the business is located. In the case of legal entities resident abroad, it is understood to be the premises where the main administration of the business is located in Peruvian territory, or, failing that, the premises designated by them, or any permanent facility that allows the effective or actual exercise of an activity.

8.3. If it is not possible to establish the address of the establishment or home, it is considered to have an unknown address in Peruvian territory.

Article IX. Guiding Principles
The owner of the personal data bank, or where appropriate, the person responsible for the processing of personal data, must comply with the legal regime regarding the protection of personal data in accordance with the guiding principles established in the Law; and also in accordance with the following specific principles :

1. Principle of transparency: The processing of personal data must be continuously informed in a clear, easy-to-understand, and accessible manner to the data subject. This principle requires that the data subject be aware of the conditions under which their personal data are processed, as well as the rights they may assert with respect to those conditions and the other conditions established in Article 18 of the Law.

2. Principle of proactive responsibility: In the processing of personal data, legal, technical and organizational measures must be applied to ensure effective compliance with personal data regulations, and the owner of the personal data bank or whoever is responsible must be able to demonstrate such compliance.

TITLE I
PROCESSING OF PERSONAL DATA

CHAPTER I
CONSENT

Article 1. Consent for the processing of personal data

1.1 The owner of the personal data bank or whoever is responsible for the processing must obtain consent for the processing of personal data, in accordance with the provisions of the Law and these Regulations, except for the cases established in article 14 of the Law, in which section 1 includes the processing of personal data that is essential to implement interoperability between public entities.

1.2 The request for consent must refer to a specific treatment or series of treatments, with express identification of the purpose or purposes for which the data is being collected, as well as any other conditions that may exist in the treatment or treatments, without prejudice to the provisions of the following article on the characteristics of consent.

1.3 When the processing of personal data refers to purposes other than those provided for in Article 14 of the Law, consent must be obtained.

1.4 When consent is requested for a form of processing that includes or may include the national or international transfer of data, the data subject must be informed in such a way that he or she unequivocally knows this circumstance, in addition to the purpose for which his or her data is intended and the type of activity carried out by the person who will receive it.

Article 2. Characteristics of valid consent

Consent for the processing of personal data is valid if the following conditions are met:

1. Free
2. Previous
3. Express and unequivocal
4. Informed

Article 3. Free consent

3.1. The consent of the data subject is considered freely given when it is given without error, bad faith, violence, or deceit that could affect the data subject's expression of intent.

3.2. Conditioning the provision of a service or warning or threatening to deny access to benefits or services that are normally unrestricted does affect the freedom of the person who gives consent for the processing of their personal data, if the data requested are not essential for the provision of the benefits or services.

3.3. The provision of gifts or benefits to the data subject in response to their consent does not affect the data subject's freedom to grant such consent. Exceptionally, in the case of children and adolescents, where their consent is permitted, such consent granted through the provision of gifts or benefits is not considered free .

Article 4. Prior consent

Consent must be requested from the data subject prior to the collection of such data or, where appropriate, prior to processing other than that for which such data was already collected.

Article 5. Express and unequivocal consent

5.1. The consent of the data subject is considered express when it has been expressed through an action that demonstrates concrete, direct, and explicit acceptance of the processing of personal data. It may be considered express when it is expressed in the following ways:

1. Verbal, when the owner of the personal data expresses it orally in person or through the use of any technology that allows oral communication.

2. Written, when it is expressed through a document or electronic means with your handwritten, electronic or digital signature , fingerprint or any other electronic mechanism authorized by the legal system that may reflect the manifestation of express will.

3. Through digital channels, when a document is signed through electronic or digital means, or any other electronic mechanism authorized by the legal system that may reflect the express manifestation, as well as the manifestation consisting of “clicking”, “clicking” or “tapping”, “tapping”, “touching” or “pad” or other similar means.

4. By any other means in accordance with the provisions of Article 141 of the Civil Code.

5.2. Consent is considered unequivocal when it can be seen that the material actions of the personal data subject demonstrate unquestionable acceptance of a specific processing of their personal data, without generating any possibility of doubt or error.

5.3. The mere expression of will in any of the forms regulated in this article does not exempt from compliance with the other requirements of consent referring to the characteristics of free, prior and informed consent.

Article 6. Informed consent

6.1. When personal data is obtained directly from the data subject, the following information must be communicated clearly and in plain language:

1. The identity and address of the owner of the personal data bank or the data controller to whom you may contact to revoke consent or exercise your rights, and, where applicable, the representative.

2. The purpose or purposes of the treatment to which your data is submitted.

3. The identity of those who are or may be your recipients, if applicable.

4. The existence and identification of the personal data bank in which the data will be stored, where applicable.

5. The mandatory or optional nature of your responses to the questionnaire that is proposed to you, where applicable.

6. The consequences of providing your data personal and his refusal to do so.

7. Where applicable, national and international transfer of data that is carried out.

8. The existence of automated decisions, including the creation of profiles , and the transmission of information regarding the consequences for the owner of the personal data.

9. The period of retention of personal data.

10. The mechanisms for exercising the rights of Title III of the Law.

6.2. In addition to the provisions of paragraph 6.1, when the personal data have not been collected directly from the personal data subject, the data bank owner or whoever is responsible must be able to inform the personal data subject of the source of the collection of the personal data upon initial contact and request.

Article 7. Privacy Policies

The publication of privacy policies, in accordance with the second paragraph of Article 18 of the Law, is understood as a form of compliance with the duty to provide information and the principle of transparency. This does not exempt the user from the requirement to obtain the consent of the data subject for the processing of such data.

Article 8. Consent and sensitive data

In the case of sensitive data, in addition to meeting the requirements for valid consent, it must be granted in writing, through a handwritten, digital, electronic signature or any other method that guarantees the will of the owner of the personal data.

Article 9. Consent and burden of proof

For the purposes of demonstrating consent, under the terms established by the Law and these Regulations, the burden of proof in all cases falls on the owner of the personal data bank or whoever is responsible for the processing.

Article 10. Denial, revocation and scope of the consent

10.1 The data subject may revoke his or her consent to the processing of his or her personal data at any time, without prior justification and without retroactive effect. Revocation of consent is subject to the same requirements observed when it was granted, although these may be simpler if so indicated at the time.

10.2 The owner of the personal data may deny or revoke his or her consent to the processing of his or her personal data for purposes other than those that give rise to the authorized processing, without affecting the relationship that gives rise to the consent that has been granted or not revoked. In the event of revocation, it is the obligation of the person who carries out the processing of the personal data to adapt the new processing to the revocation and the processing that was in the process of being carried out, within the period resulting from diligent action, which may not exceed ten (10) days.

10.3 If the revocation affects the entire processing of personal data that was being carried out, the owner of the personal data bank, the person in charge of the processing, or, where applicable, the person responsible for the processing, applies the rules for cancellation or deletion of personal data.

10.4 The owner of the personal data bank or the person responsible for the processing must establish easily accessible, unconditional, simple, rapid, and free mechanisms to make the revocation effective.

CHAPTER II
LIMITATIONS ON CONSENT

Article 11. Processing of personal data obtained through publicly accessible sources

11.1 For the purposes of the Law and these Regulations, the following are considered sources accessible to the public, regardless of whether access requires compensation:

1. Electronic, optical, and other technological means of communication, provided that the location where the personal data is stored is designed to provide information to the public and is open to general consultation, unless a regulation determines otherwise.

2. Telephone directories, regardless of the medium on which they are available and under the terms of their specific regulation .

3. Newspapers and magazines, regardless of the medium in which they are available and under the terms of their specific regulations .

4. Social media.

5. Lists of individuals belonging to professional groups containing only their name, title, profession, activity, academic degree, postal address, telephone number, fax number, email address, and any information establishing their membership in the group. In the case of professional associations, the following information may also be included regarding their members: membership number, date of incorporation, and professional status.

6. The repertoires of jurisprudence published in accordance with law.

7. The Public Registries administered by the National Superintendence of Public Registries - SUNARP, as well as any other registry or database classified as public according to law.

8. Public Administration entities, in relation to the information that must be provided in application of Law No. 27806, the Law on Transparency and Access to Public Information.

11.2 The provisions of paragraph 8 of this article do not imply that all personal data contained in information managed by entities subject to the Law on Transparency and Access to Public Information are considered information from a source accessible to the public. The evaluation of access to personal data held by public administration entities is carried out taking into account the circumstances of each specific case, assessing the probable impact on other rights.

fundamental.

11.3 The processing of personal data obtained through publicly accessible sources must respect the principles established in the Law and in this Regulation.

CHAPTER III
TRANSFER OF PERSONAL DATA

Article 12. General aspects of the transfer of personal data

12.1 The transfer of personal data is the communication of personal data within or outside the national territory to a person other than the owner of the personal data.

12.2 The person to whom the personal data are transferred is obliged, by the mere fact of the transfer, to comply with the Law and this Regulation.

Article 13. Conditions for the transfer of personal data

13.1 Any transfer of personal data requires the consent of its owner, except for the exceptions provided for in article 14 of the Law. Such transfer must be limited to the purpose that justifies it .

13.2 In all cases, the transfer of personal data must be reported to the data subject, as established in Article 18 of the Law.

Article 14. Burden of proof in the transfer of personal data

For the purposes of demonstrating that the transfer has been carried out in accordance with the provisions of the Law and this Regulation, the burden of proof falls, in all cases, on the issuer or the person who transfers the personal data.

Article 15. Transfer within a sector or business group

In the case of transfers of personal data within a business group, affiliated or linked subsidiary companies under the common control of the same business group or those affiliated or linked to a parent company or any company in the same group as the owner of the database or data controller, the consent of the owner of the personal data must be requested unless the processing falls within one of the exceptions provided for in Article 14 of the Law, particularly when it involves an order for the processing of personal data within the framework of a prior contractual relationship.

Article 16. Recipient of personal data

The recipient of the personal data must process the personal data in compliance with the information provided by the sender to the personal data subject and respect the content of the consent granted by the personal data subject. For additional purposes , consent must be obtained where appropriate.

Article 17. Formalization of national transfers

National data transfers are formalized through mechanisms that demonstrate that the owner of the personal data bank or the data controller complies with the obligation to inform the recipient of the personal data of the conditions under which the owner of the personal data consented to the processing of the data.

Article 18. Cross-border flow of personal data

18.1 The cross-border flow of personal data must take place when the recipient or importer of the personal data is located in a country that has an adequate level of data protection in accordance with the provisions of the Law and this Regulation.

18.2 If the country does not have an adequate level of data protection, the issuer or exporter must provide appropriate guarantees to ensure the proper processing of personal data outside the national territory, except for the exceptions contemplated in Article 15 of the Law.

Article 19. Adequate level of data protection for cross-border flow

19.1 In order to determine the appropriate level of data protection for a country, the Directorate General

of Transparency, Access to Public Information and Protection of Personal Data issues a resolution to determine whether this data has protection comparable to that provided for in the Law and this Regulation.

19.2 The aforementioned evaluation considers at least and concurrently the following criteria:

1. The existence of a legal framework for the protection of personal data.
2. The existence of principles for the processing of personal data.
3. The existence of regulations that recognize and guarantee the rights of data subjects and that provide them with avenues to exercise them.
4. The existence of a personal data protection authority, or those acting in its place, to supervise and sanction violations of the regulations, where appropriate.

19.3 The assessment referred to in the previous paragraph is dispensable if the country whose adequate level of data protection is the subject of analysis has negotiated and signed common and general standards for the protection of personal data with Peru.

19.4 The resolution referred to in paragraph 19.1 is issued ex officio , at the request of a party or as a result of sectoral regulations that require sectors to obtain a technical opinion from the National Authority for the Protection of Personal Data.

Article 20. Guarantees for the cross-border flow of personal data

20.1 For the purposes of paragraph 18.2 of Article 18 of this Regulation, the issuer or exporter may rely on model contractual clauses or other legal instruments that establish at least the same obligations to which it is subject, as well as the conditions under which the data subject consented to the processing of his or her personal data.

20.2 The General Directorate of Transparency, Access to Public Information and Protection of Personal Data issues contractual clause templates so that recipients or importers assume the obligations corresponding to the owner of the database or data controller, and the rights and freedoms of the owners of personal data and the obligations of data controllers are established.

Article 21. Opinion and registration of the cross-border flow of personal data

21.1 Without prejudice to the provisions of Articles 19 and 20 of this Regulation, the owners of personal data banks or data controllers may request an opinion from the General Directorate of Transparency, Access to Public Information and Personal Data Protection regarding whether the cross-border flow of personal data they carry out complies with the Law and this Regulation. This opinion shall be issued within a maximum period of thirty (30) days.

21.2 In any case, the cross-border flow of personal data must be reported to the General Directorate of Transparency, Access to Public Information, and Personal Data Protection, including the information required for the transfer of personal data and the database registration. This communication is entered into the National Registry for the Protection of Personal Data using the form approved for this purpose.

CHAPTER IV
SPECIAL DATA PROCESSING PERSONAL

Article 22. Processing of personal data of children and adolescents

22.1 The processing of personal data of children and adolescents is considered lawful when the consent of the person or persons exercising parental authority or guardianship, as appropriate, is obtained.

22.2 Persons over the age of fourteen and under the age of eighteen, according to their capacity, may give consent for the processing of their personal data provided that the information provided has been expressed in a language they understand, in accordance with the regulations on the matter.

22.3 Under no circumstances may consent be granted for the processing of personal data of children and adolescents to enable them to access activities related to goods or services restricted for their age.

Article 23. Prohibition of data collection through children and adolescents

23.1 Personal data may not be collected from children and adolescents that would allow information to be obtained about other members of their family group, such as data relating to the professional activity of their parents, economic information, sociological data or any other information, without the consent of the owners of such data.

23.2 Identity and address data may only be collected from parents or guardians for the purpose of obtaining consent, where appropriate.

Article 24. Promotion of the protection of data of children and adolescents

It is the obligation of all personal data bank owners, especially public entities, to collaborate in promoting awareness of the right to the protection of children's and adolescents' personal data, as well as the need for their processing to be carried out with special responsibility and security.

Article 25. Processing of personal data of children and adolescents on the Internet

25.1 It is the obligation of the owners of personal data banks, or of whoever is responsible for the processing of data on children and adolescents, to guarantee the protection of the best interests of the child and their fundamental rights in the digital environment.

25.2 Within the framework of the offer of digital services for persons over fourteen and under eighteen years of age, the processing of personal data is lawful when their consent has been obtained.

25.3 Within the framework of the offer of digital services aimed at minors under fourteen years of age, the processing of personal data is lawful provided that there is consent from the person or persons exercising parental authority or guardianship, as appropriate.

25.4 The owner of the personal data bank or the person responsible for data processing on platforms or services in the digital environment makes reasonable efforts to verify , in the cases described in paragraphs 25.2 and 25.3, the identity of those who grant consent, taking into account the available technology.

Article 26. Data processing for advertising and commercial prospecting

26.1 The processing of personal data for the purposes of advertising and commercial prospecting of products and

services are lawful when consent is obtained directly from the owner of the personal data.

26.2 Consent for the processing of personal data may be obtained through an initial contact, after which, if consent has not been obtained, further contact or processing of personal data is not lawful.

26.3 For the first contact, the personal data may have been obtained from publicly accessible sources. In this case, the person responsible for processing the personal data must be able to inform, at the first contact and at the request of the personal data owner, the source of the collection of the personal data.

26.4 It is presumed that the person responsible for the processing of personal data for advertising and commercial prospecting is the person in whose interest such processing is carried out, unless proven otherwise.

26.5 In all cases, the owner of personal data has the right to refuse, revoke or oppose the processing of his or her personal data for advertising and commercial prospecting purposes , for which the data controller must provide a simple and free means to process said request, which must be attended to within a maximum period of ten (10) days. Refusing, revoking or opposing the processing of personal data for advertising and commercial prospecting purposes must not be more complex than that used to grant consent.

26.6 The data controller establishes the necessary procedures to ensure that requests submitted to a data processor are forwarded to them for timely attention.

26.7 The National Authority for the Protection of Personal Data shall issue the provisions it deems relevant regarding the provisions regulated in this article.

Article 27. Processing of personal data in the communications and telecommunications sector

27.1 Operators of communications or telecommunications services are responsible for ensuring the confidentiality , availability, proper use and integrity of the personal data they obtain from their subscribers and users in the course of their business operations.

27.2 Operators of communications or telecommunications services may not process the aforementioned personal data for purposes other than those authorized by the owner, except by court order or express legal mandate.

Article 28. Processing of data by means outsourced technology

28.1 The processing of personal data by third-party technological means, including services, applications, infrastructure, among others, refers to those in which the processing is automatic, without human intervention.

28.2 For cases where there is human intervention in the processing, Articles 32 and 33 of this Regulation apply.

28.3 The processing of personal data by third-party technological means, whether complete or partial, may be contracted by the controller of personal data provided that the execution of the same guarantees compliance with the provisions of the Law and these Regulations.

Article 29. Criteria to be considered for the processing of personal data by third-party technological means

When processing personal data through third-party technological means, the following minimum services must be considered:

1. Inform personal data subjects transparently about subcontracting that involves the information for which the service is provided.

2. Not including conditions that authorize or allow the provider to assume ownership of the personal data banks processed in the outsourcing process.

3. Guarantee the confidentiality, integrity and availability of the personal data for which the service is provided.

4. Maintain control, decisions, and responsibility over the process by which personal data is processed.

5. Guarantee and demonstrate the destruction or inability to access personal data after the service has been completed.

Article 30. Mechanisms for the provision of personal data processing services by outsourced technological means

The service provider must comply with the following mechanisms:

1. Inform the data controller of any changes to its privacy policies or the terms of the service it provides, in order to obtain consent if this means increasing its processing powers.

2. Allow the data controller to limit the type of processing of personal data for which the service is provided.

3. Establish and maintain appropriate security measures for the protection of personal data for which the service is provided.

4. Ensure and demonstrate the deletion of personal data once the service provided to the controller has concluded and the controller has been able to recover it.

5. Prevent access to personal data to those who do not have access privileges, or, if requested by the competent authority, inform the controller of this fact.

Article 31. Provision of services or treatment custom made

31.1 The person in charge of processing personal data is prohibited from transferring personal data to third parties that are the subject of processing services, unless the owner of the personal data bank or the data controller who commissioned the processing has authorized it and the owner of the personal data has given his or her consent, in cases where such consent is required by law.

31.2 The period for the retention of personal data referred to in Article 30 of the Law is a maximum of two (2) years from the completion of the last assignment. The retention of personal data for a period longer than that established may only be carried out in the case provided for in the second paragraph of Article 30 of the Law or because it is expressly provided for in a current regulatory provision, in which case the data must be returned to the data controller for retention while the legal obligation persists. The indefinite retention of personal data, as a general rule, is prohibited.

31.3 The provisions of this article shall apply, where appropriate, to the subcontracting of the provision of personal data processing services.

Article 32. Processing through subcontracting

32.1 The processing of personal data may be carried out by a third party other than the data processor, through an agreement or contract between the two parties.

32.2 For this case, prior authorization from the owner of the personal data bank or data controller is required. Such authorization is also deemed granted if it was provided for in the legal instrument formalizing the relationship between the data controller and the data processor.

32.3 The processing carried out by the subcontractor is carried out on behalf of and for the account of the data controller, but the burden of proving authorization lies with the data processor.

Article 33. Liability of the subcontracted third party

The subcontracted natural or legal person assumes the same obligations as those established for the data processor by the Law, this Regulation, and other applicable provisions. However, they assume the obligations of the personal data controller when:

1. Use or allocate personal data for a purpose other than that authorized by the database owner or data controller; or

2. Make a transfer, disregarding the instructions of the owner of the personal data bank, even if it is for the conservation of said data.

CHAPTER V
OBLIGATIONS IN THIS MATTER
TREATMENT OF
PERSONAL DATA

Article 34. Notification of the personal data security incident

34.1 In the event of a personal data security incident that generates exposure of large volumes of data, in quantity or type of data, or that may affect a large number of people or when sensitive data is involved or when damage is caused

If a breach of this law is evident to other rights or freedoms of the personal data subject, the data bank owner or the data controller must notify the National Data Protection Authority within 48 hours of becoming aware of it or becoming aware of it. If such notification is made more than 48 hours later, it must be accompanied by an indication of the reasons and/or supporting evidence for such delay. This obligation remains in place even if the personal data controller considers that the incident has been rectified or resolved internally.

34.2 The notification of the personal data security incident must indicate and describe at least the following:

1. The nature of the personal data security incident, including, where possible, the types of data and the approximate number of data subjects affected.

2. The name and contact details of the Personal Data Officer or other point of contact where further information can be obtained.

3. The possible consequences of the personal data security incident.

4. The measures adopted or proposed by the data controller or data owner to remedy the personal data security breach, including, where appropriate, measures taken to mitigate any potential negative effects.

34.3 The owner of the data bank or the person responsible for the processing who notices a personal data security incident that affects the owner of the data in other rights, you must notify the holder within 48 hours without undue delay, in simple and clear language, as well as the measures taken to mitigate its effects. If such communication is made more than 48 hours later, it must be accompanied by an indication of the reasons.

of such delay.

34.4 When the personal data security incident did not produce the impact described above and was completely overcome by the measures adopted, the obligation to communicate said incident to the owner of the personal data does not remain.

34.5 In the event that the personal data security incident develops in and/or through the digital environment, the notification is made, in addition to the National Authority for the Protection of Personal Data, to the National Center for Digital Security for its incorporation into the National Registry of Digital Security Incidents in accordance with the provisions of Emergency Decree No. 007-2020, Emergency Decree that approves the Digital Trust Framework and provides measures for its strengthening, its Regulations and complementary regulations.

34.6 Whenever it is essential for the management of personal data security incidents, the collection and transfer of such data to or between public entities, with legal authority to carry out such management, does not require consent, within the framework of the provisions of section 1 of article 14 of Law 29733, the Personal Data Protection Law.

34.6 The Secretariat of Government and Digital Transformation of the Presidency of the Council of Ministers and the National Authority for Personal Data Protection proposes and establishes protocols to ensure interoperability, collaboration and information exchange on notifications of personal data security incidents when they occur in and through the digital environment.

34.7 The National Authority for the Protection of Personal Data approves the provisions and/or guidelines necessary for the due compliance of this article.

Article 35. Documentation of security incidents

The controller of personal data must document any security incident, including the facts surrounding it, its effects, and the measures taken. This documentation allows the National Data Protection Authority to verify compliance with the obligations related to this matter.

Article 36. Obligation of the data controller

The data controller must immediately inform the owner of the personal data bank or the data controller of any personal data security incident of which they become aware.

Article 37. Appointment of the Personal Data Officer

37.1 The owner of the personal data bank or the person responsible and the person in charge of processing must appoint a Personal Data Officer when :

1. The processing is carried out by a public entity, in accordance with the provisions of paragraph 68.6 of article 68 of the Regulations of Legislative Decree No. 1412, Legislative Decree approving the Digital Government Law and establishing provisions on the conditions, requirements, and use of electronic technologies and media in administrative procedures, approved by Supreme Decree No. 029-2021-PCM.

2. The owner of the database, the data controller, or the data processor processes large volumes of personal data, in terms of quantity or type, or that may affect a large number of people, or when the data is sensitive, or when there is obvious harm to other rights or freedoms of the personal data owner.

3. The owner of the database or the data controller or the data processor carries out core or business activities that involve the processing of sensitive data.

37.2 A corporate group may appoint a single Personal Data Officer provided that he or she is easily contactable from each establishment .

37.3 Where the data controller or data controller is a public authority or body, a single Personal Data Officer may be designated for several of these authorities or bodies, taking into account their organisational structure and size .

37.4 The owner of the data bank or the person responsible for or in charge of the processing must publish the contact details of the Personal Data Officer in a visible place that allows the owners of personal data to make informed decisions .

37.5 The contact details of the designated Personal Data Officer , and any updates, must be communicated to the National Personal Data Protection Authority within 15 days of the respective designation or update.

Article 38. Profile of the Personal Data Officer

38.1 The Personal Data Officer shall be appointed on the basis of his or her professional qualities and, in particular, his or her knowledge and experience in the field of personal data protection, duly accredited, which should enable him or her to efficiently perform the functions of Article 39 of this Regulation.

38.2 The Personal Data Officer may be a person who performs other functions in the company or public entity, without it being necessary for him or her to exclusively perform the functions linked to his or her designation, and may even be a person external to the private organization.

Article 39. Functions of the Personal Data Officer

39.1 The Personal Data Officer has at least the following functions :

1. Inform and advise the owner of the personal data bank or the data controller and the employees who handle the processing of personal data regarding their obligations under the Law, this Regulation and other data protection provisions.

2. Verify and report on compliance with the provisions of the Law, this Regulation and other provisions on personal data protection, as well as compliance with the policies of the data bank owner or the data processor regarding personal data protection, including the assignment of responsibilities, awareness-raising and training of personnel involved in processing operations, and any audits carried out.

3. Cooperate, as appropriate, with the National Authority for the Protection of Personal Data in the performance of its purposes and powers.

4. Act as the point of contact for the National Data Protection Authority for matters relating to the processing of personal data.

39.2 The Personal Data Officer performs his or her duties with due regard to the risks associated with personal data processing operations, taking into account the nature, scope, context and purposes of such processing.

Article 40. Impact assessment regarding the protection of personal data

40.1 Optionally and prior to the processing of personal data, the owner of the database or the data controller may conduct a Personal Data Protection Impact Assessment, especially when it involves sensitive data, data for the purpose of creating personal profiles, data of people in particularly vulnerable situations such as children and adolescents, indigenous people in isolation and/or initial contact, or people with disabilities; or when processing large volumes of data or other situations determined by the National Personal Data Protection Authority.

40.2 The impact assessment relating to the protection of personal data may be prepared by taking as reference the guide, guidelines and procedures established in NTP-ISO/IEC 27005 and NTP-ISO 31000 in their current edition or other standards related to the analysis and assessment of risks for the protection of personal data.

40.3 The National Authority for the Protection of Personal Data shall issue the supplementary provisions that are relevant for the performance of the Impact Assessment relating to the protection of personal data.

Article 41. Dissociation procedure

41.1 Dissociation is a procedure that prevents identification or renders the data subject unidentifiable. This procedure is reversible.

41.2 The controller or processor of personal data must choose the appropriate technique when carrying out the dissociation procedure, always taking into account the type of data being processed, the number of data subjects and the risk factor (severity, probability, consequences for the controller and the subject) and those determined by the National Authority for this purpose.

41.3 The National Authority for the Protection of Personal Data approves the complementary or guiding provisions for carrying out the dissociation and anonymization procedure.

Article 42. Obligation to register

42.1 Natural or legal persons from the private sector or public entities that create, modify or cancel personal data banks are required to process the registration of said acts before the National Registry for the Protection of Personal Data.

42.2 The National Registry for the Protection of Personal Data is the storage unit intended to contain primarily information on public or private personal data banks and its purpose is to publicize the registration of said banks in such a way that it is possible to exercise the rights of access to information, rectification , cancellation, opposition and others regulated by the Law and this Regulation.

Article 43. Acts and documents that can be registered in the National Registry

43.1 The following are subject to registration in the National Registry for the Protection of Personal Data in accordance with the provisions of the Law and this title:

1. Personal data banks of the public administration, with the exceptions provided for in the Law and this Regulation.

2. Privately managed personal data banks, with the exception provided for in section 1 of article 3 of the Law.

3. Sanctions, precautionary or corrective measures imposed by the General Directorate of Transparency, Access to Public Information and Protection of Personal Data in accordance with the Law and these Regulations.

43.2 Any person may consult the information referred to in Article 34 of the Law and any other information contained in the National Registry.

43.3 The registration of the aforementioned acts in the National Registry of Personal Data Protection is free of charge, including the modification and cancellation of the registration in accordance with the provisions of this Regulation.

Article 44. Modification or cancellation of personal data banks in the National Registry of Registration of Personal Data Banks

44.1 The registration of a personal data bank of the public or private administration in the National Registry of Registration of Personal Data Banks must be kept up to date at all times.

44.3 The owners of personal data banks or those responsible for their processing shall communicate any modification or cancellation to the registration of the data bank registered with the National Registry for the Protection of Personal Data by submitting the request via the cancellation or modification form addressed to the Directorate for the Protection of Personal Data.

Article 45. Procedure

45.1 The owners of personal data banks request registration of the data banks with the National Registry of Personal Data Protection, via a form, before the Directorate of Personal Data Protection.

45.2 The registration procedure is automatically approved and is governed by the provisions established in article 31 of Law No. 27444, the General Administrative Procedure Law or any regulation that replaces it.

CHAPTER VI
SECURITY MEASURES

Article 46. Security for the processing of data through digital means

Platforms, websites, mobile applications, digital services, and IT systems used to process personal data must have the following documented and implemented:

1. Access control to personal data, which includes:

a) Access management from user registration to deletion or termination, including periodic events such as vacation periods or sporadic permits.

b) Identification and authentication procedures .
c) Management of the privileges assigned to said user, including periodic verification of the same, which must be executed periodically at a minimum interval of six months.

d) User authentication mechanisms before the system that involve the assignment of user-password use, use of digital certificates, tokens, among others.

2. Monitoring and periodic review of security measures and staff training plans, depending on their roles and responsibilities, regarding the processing of personal data they carry out.

3. The generation and maintenance of records that provide evidence of interactions with logical data, including for traceability purposes, information on user accounts with access to the system, session start and end times, and actions related to processing, viewing, modification , deletion, import, and export of personal data.

These records must be legible, timely, and have a procedure for disposal, storage, transfer, and destruction once the records are no longer useful. These records must be generated and/or executed periodically. These records must be retained for a minimum period of two (2) years.

Logical interaction logs corresponding to the traceability of the actions performed by the operators of the systems used to process personal data must be generated continuously and must be immediately available.

4. Security measures that prevent unauthorized personnel from generating copies or reproducing digital documents containing personal data.
In the case of using systems, instant messaging applications, email accounts, and/or non-institutional social networks, these must be duly approved and formally established to avoid generating risks and unauthorized transfers of personal data.

Article 47. Security Document

47.1 The controller of personal data must have a security document, which must be formally approved and have a specific date. The security document must be up-to-date and contain, at a minimum, the procedures for access management, privilege management, and periodic verification of assigned privileges related to information systems, including technology platforms, mobile applications, database engines, among others, used to process personal data. It may refer to the requirements and controls indicated in the current NTP-ISO/IEC 27001 or to a widely recognized best practice or standard in its sector. In the case of public entities, the provisions of current digital governance and digital security standards apply.

47.2 The security document is mandatory for personnel with access to information systems. The person responsible for its preparation must determine the measures necessary to ensure that personnel are adequately aware of the consequences of non-compliance and implement the necessary security measures to support their compliance.

47.3 The security document must contain internal policies for the management and processing of personal data that take into account the context and lifecycle of personal data, i.e., its collection, use, and subsequent deletion. It must also compile an inventory of personal data and the systems used for processing, specifying whether sensitive data is involved.

Article 48. Conservation, backup and recovery of personal data

48.1 In environments where information is processed, stored or transmitted, the following security controls must be designed and implemented as a minimum:

1. Controls to keep areas safe.

2. Controls to keep equipment safe inside and off-site.
3. Controls to ensure the generation of secure and continuous backup copies and verification of their integrity.

48.2 The controller of personal data may refer to the recommendations set forth in the current edition of "NTP-ISO/IEC 27001:2022 Information technology. Security techniques. Information security systems. Requirements."

Article 49. Controls to keep areas safe

49.1 Controls to keep areas safe are as follows:

1. Security perimeters that protect areas where personal data is processed.
2. Appropriate entry controls to ensure that access is allowed only to authorized personnel.
3. System against natural disasters, attack malicious or accidents.
4. Procedures for working in safe areas.
5. Control access points, dispatch areas, loading areas, and other areas where unauthorized persons may enter the premises, and if necessary, isolate information processing facilities to prevent unauthorized access.

Article 50. Controls to maintain equipment safe inside and outside the premises

50.1. Controls to keep equipment safe inside and outside the facilities are as follows:

1. Location and protection of equipment to reduce the risks of environmental threats and hazards, as well as opportunities for unauthorized access.
2. Protection of equipment against power failures and other disturbances caused by faults in supply services.
3. Protection against interception, interference and/or damage to power and telecommunications cabling carrying data or supporting information services.
4. Impossibility of removing equipment, information or software without prior authorization.
5. Ensure that equipment containing sensitive data storage media has been deleted or overwritten before disposal or reuse.
6. Ensure that computer equipment has appropriate protection in case it is left unattended by users.
7. Implement a policy of clearing desks and screens free of papers and removable storage media for information processing facilities.

Article 51. Controls to ensure the generation of secure and continuous backup copies and verification of their integrity

51.1 Backups are performed at least weekly, unless no personal data has been updated during this period. This procedure must include security measures for storage, transfer, and destruction, if applicable.

51.2 The integrity of the data stored in the backup copies must be verified , including, if applicable, complete recovery in the event of an interruption or damage that guarantees the return to the state in which they were stored.

was at the time the interruption or damage occurred.

Article 52. Logical or electronic transfer of personal data

The exchange of personal data from the processing or storage environments to any destination outside the physical facilities of the entity only proceeds with the authorization of the owner of the personal data bank and is carried out using the means of transport authorized by the same, implementing the necessary measures (among which are data encryption, use of digital signatures and certificates, verification checksum , among others) to avoid unauthorized access, loss or corruption during the transit to their destination.

Article 53. Storage of non-automated documentation

53.1 Cabinets, filing cabinets, or other items containing personal data contained in non-automated documents are protected with doors equipped with key-operated opening systems or other equivalent devices. Areas containing personal data remain locked when access to the documents is not required. All keys or opening mechanisms must be formally assigned, and, where applicable, procedures for transfer and assignment must be in place.

53.2 If, due to the characteristics of the premises available, it is not possible to keep the areas containing cabinets, filing cabinets or other elements in which non-automated documents containing personal data are stored closed, alternative measures must be adopted, in accordance with the security directives provided by the General Directorate of Transparency, Access to Public Information and Protection of Personal Data.

Article 54. Copying or reproduction of automated and non-automated documentation

54.1 The generation of copies or reproduction of documents containing personal data may only be carried out under the control of authorized personnel.

54.2 Discarded copies or reproductions must be destroyed in such a way as to prevent access to the information contained therein or its subsequent recovery.

Article 55. Access to documentation

55.1 Access to documentation is limited exclusively to authorized personnel.
55.2 Mechanisms must be established to identify the accesses made in the case of documents that can be used by multiple users.

55.3 Access by persons not included in paragraph previous must be properly recorded.

Article 56. Transfer of non-automated documentation

Whenever documentation contained in a database is physically transferred, measures must be taken to prevent unauthorized access, misuse, manipulation, and alteration of the personal data being transferred.

Article 57. Provision of services without access to personal data

57.1 The person responsible for or in charge of the information or treatment must implement the mechanisms or meas

adequate security measures to limit staff access to personal data, to the media containing them or to the resources of the information system, for the performance of work that does not involve the processing of personal data.

57.2 In the case of external personnel, the service provision contract expressly includes the prohibition of accessing personal data and the obligation of confidentiality regarding data that the personnel may have learned in connection with the provision of the service.

Article 58. Determination of the certain date of documents

The exact date of the documents submitted by the administrators as evidence must be determined according to the evidentiary assessment carried out by the competent body, for which the following alternative criteria are considered:

1. That the document has been presented before a public official or notary; or,
2. That the document has been disseminated through a public media of a specific or determinable date; or,
3. That there are other suitable technical means that generate conviction about it.

CHAPTER VII
CODES OF CONDUCT

Article 59. Scope of the Codes of Conduct

59.1 Codes of conduct are a proactive accountability mechanism that allows for demonstrating compliance with the obligations established in the Law and this Regulation for the processing of personal data. Codes of conduct are voluntary.

59.2 Sectoral codes of conduct may refer to all or part of the treatments carried out by the sector, and must be formulated by representative organizations of the sector.

59.3 Codes of conduct promoted by a company or business group must refer to all the treatments carried out by them.

59.4 The implementation of the Code of Conduct, duly accredited prior to the start of the administrative sanctioning procedure, in accordance with the requirements regulated in this Regulation, is considered a mitigating factor of liability.

Article 60. Content

60.1 Codes of conduct should be drafted in clear and accessible terms.

60.2 The codes of conduct comply with the provisions of the Law and include at least the following aspects:

1. The clear and precise delimitation of its scope of application, the activities to which the code refers and the treatments subject to it.

2. The provisions for compliance with the principles of personal data protection for processing purposes subject to the code of conduct.

3. The establishment of procedures that facilitate the exercise of the rights of information, access, rectification , cancellation and opposition of those affected.

4. The determination of the national and international transfers of personal data that, where appropriate, are planned, indicating the guarantees that must be adopted.

5. Actions to promote and disseminate personal data protection aimed at those who process it.

6. Mechanisms to ensure the confidentiality of personal data by those who process them.

7. The supervisory mechanisms through which compliance by members with the provisions of the code of conduct is guaranteed.

8. Clauses for obtaining the consent of personal data subjects for the processing or transfer of their personal data.

9. Clauses to inform data subjects personal treatment.

10. Formats for exercising the rights of information, access, rectification , cancellation and opposition.

11. In the event that personal data is processed on a contract basis, clause formats are presented for the hiring of the data processor, as established by the Law and this Regulation.

TITLE II
RIGHTS OF THE DATA HOLDER PERSONAL

CHAPTER I
GENERAL PROVISIONS

Article 61. Personal character

The rights of information, access, rectification , cancellation, opposition and objective processing of personal data may only be exercised by the owner of the personal data, without prejudice to the rules governing representation.

Article 62. Exercise of the rights of the owner of personal data

The exercise of one or more of these rights does not exclude the possibility of exercising one or more of the others, nor can it be understood as a prerequisite for exercising any of them.

Article 63. Legitimacy to exercise rights

63.1 The exercise of the rights contained in this title is carried out:

1. By the data subject, proving their identity and presenting a copy of their National Identity Document or equivalent. The use of a digital signature , in accordance with current regulations, replaces the presentation of a National Identity Document and its copy.

2. Through a legal representative accredited as such.

3. Through a representative expressly authorized to exercise the right, attaching a copy of his or her National Identity Document or equivalent document, and the title that accredits the representation.

63.2 When the owner of the personal data bank is a public entity, the representation may be accredited by any legally valid means that leaves a reliable record , in accordance with article 115 of Law No. 27444, the General Administrative Procedure Law or any other that replaces it.

63.2 If the procedure indicated in article 65 of this Regulation is chosen, the accreditation of the identity of the holder is subject to the provisions of said provision.

Article 64. Application requirements

The exercise of rights is carried out by means of a request addressed to the owner of the personal data bank or the person responsible for processing, or to the person in charge of processing, if as a result of the assignment, the contract or legal relationship establishes that they are obliged to respond to requests or if a person responsible for processing is considered to be the person responsible for managing the personal data base, which must contain:

1. Names and surnames of the holder of the right and accreditation thereof, and where applicable, of his/her representative in accordance with the preceding article.
2. Specific request that gives rise to the application.
3. Address, or address which may be electronic, to effects of the corresponding notifications.
4. Date and signature of the applicant.
5. Documents supporting the request, if applicable.

6. Payment of the consideration, in the case of public entities, provided that they have provided for it in their procedures prior to the validity of this Regulation.

Article 65. Customer service

65.1 When the owner of the personal data bank or the data controller provides services of any kind for customer service or for filing complaints related to the service provided or products offered, they may also process requests for the exercise of the rights included in this title through said services, provided that the time periods are not longer than those established in this Regulation.

65.2 In this case, the identity of the owner of personal data is considered accredited by the means established by the owner of the personal data bank or the person responsible for the processing for the identification of the latter, provided that it is accredited, in accordance with the nature of the provision of the service or product offered.

Article 66. Reception and correction of the application

66.1 All applications submitted must be received, with proof of receipt by the owner of the personal data bank or the person responsible for processing or in charge of processing, where applicable.

66.2 In the event that the application does not comply with the requirements of Article 63, the owner of the personal data bank or the person responsible for its processing, within a period of five (5) days, counting from the day following receipt of the application, shall make the observations that cannot be resolved ex officio , inviting the owner to correct them within a maximum period of five (5) days. If the indicated period elapses without any correction occurring, the application is deemed not to have been submitted.

66.3 Public entities apply Article 126 of Law No. 27444, the General Administrative Procedure Law, or any other law that replaces it, regarding observations on the documentation submitted.

66.4 When the request to exercise the right is submitted to the person in charge of processing personal data, he must transfer it within a maximum period of three (3) days to the owner of the data bank or the person responsible for the processing so that the corresponding request can be attended to.

66.5 When the request to exercise the right is submitted to the person in charge of processing personal data, who is the person who fulfills the task with the database of the owner of the data bank or the person responsible for the processing, he must receive the request and transfer it immediately so that the right of the owner of the personal data is met, as established in paragraph 65.1 of this article, and must also communicate it to the owner of the personal data.

Article 67. Facilities for the exercise of the right

67.1 The owner of the personal data bank or the person responsible for processing or in charge of processing, where applicable, is obliged to establish a simple procedure for exercising rights.

Regardless of the means or mechanisms that the Law and this Regulation establish for the exercise of the rights of the owner of personal data, the owner of the personal data bank or the person responsible for the processing or in charge of processing may offer mechanisms that facilitate the exercise of such rights for the benefit of the owner of personal data.

67.2 For the purposes of the consideration that the owner of personal data must pay for the exercise of his rights before the public administration, the provisions of the first paragraph of article 26 of the Law apply.

67.3 The exercise by personal data subjects of their rights before privately managed personal data banks is free of charge, except as established in special regulations on the subject. Under no circumstances does the exercise of these rights entail additional payment for the personal data bank holder, data controller, or data processor before whom they are exercised.

67.4 No means may be established as a means for exercising rights that involve charging an additional fee to the applicant or any other means that entails an excessive cost in the case of personal data banks of public entities.

Article 68. Form of response for the exercise of the right

68.1 The owner of the personal data bank or the person responsible for processing or in charge, where appropriate, must respond to the request in the manner and within the timeframe established in this Regulation, regardless of whether or not the personal data of the owner appear in the personal data banks that he manages.

68.2 The response to the owner of personal data must be presented in a clear, legible, understandable and easy-to-understand manr access.

68.3 If the use of keys or codes is necessary, the corresponding meanings must be provided.

68.4 The owner of the personal data bank or the data controller is responsible for proving compliance with the duty to respond and must retain the means to do so. The foregoing also applies, where relevant, to proving compliance with the provisions of the second paragraph of Article 20 of the Law.

Article 69. Response deadlines for the exercise of the right

69.1 The maximum response time of the owner of the personal data bank or the person responsible or in charge of the treatment when appropriate, before the exercise of the right to information, is eight (08) days counted from the day following the submission of the request.

69.2 The maximum period for the response of the owner of the personal data bank or the person responsible or in charge of the treatment, when appropriate, before the exercise of the right of access is twenty (20) days counted from the day following the presentation of the request by the owner of personal data.

69.3 In the case of the exercise of other rights such as rectification , cancellation or opposition, the maximum response period of the owner of the personal data bank or the person responsible or in charge of the processing, when applicable, is ten (10) days counted from the day following the submission of the request.

Article 70. Request for information or additional documentation

70.1 In the event that the information provided in the application is insufficient or erroneous in such a way that it does not allow

For your attention, the owner of the personal data bank or the person responsible for the treatment, when appropriate, may request, within seven (7) days after receiving the request, additional information or documentation from the owner of the personal data to attend to it.

70.2 Within ten (10) days of receiving the request, counting from the day following its receipt, the personal data owner must submit any additional documentation he or she deems relevant to support his or her request. Otherwise, the request will be deemed not to have been submitted.

70.3 The applicable deadline for providing the response is suspended until the personal data owner responds to the request for additional information or documentation.

Article 71. Extension of deadlines

71.1 Except for the period established for the exercise of the right to information, the periods corresponding to the response or attention to the other rights may be extended only once, and for an equal period, at most, as long as the circumstances justify it .

71.2 The justification for the extension of the period must be communicated to the owner of the personal data within the period that is intended to be extended.

Article 72. Application of specific provisions

When the provisions applicable to certain personal data banks, in accordance with the special legislation that regulates them, establish a specific procedure for the exercise of the rights regulated in this Title, such provisions are applicable to the extent that they offer equal or greater guarantees to the owner of the personal data and do not contravene the Law and this Regulation.

Article 73. Partial or total denial of the exercise of a right

A totally or partially negative response by the owner of the personal data bank or the data controller to a request for a right must be duly justified and indicate to the owner of the personal data that they may appeal to the Directorate of Personal Data Protection for a claim or to the Judiciary for the purposes of habeas data proceedings, in accordance with Article 24 of the Law.

CHAPTER II
SPECIAL PROVISIONS

Article 74. Right to information

74.1 The owner of personal data has the right, by way of access, to be provided with all the information indicated in Article 18 of the Law. The response must contain the details provided for in the aforementioned Article 18.

74.2 For the response to the exercise of the right to information, Articles 77 and 78 of this Regulation shall apply, as appropriate.

Article 75. Right of access

75.1 The owner of personal data has the right to be informed clearly, expressly and indubitably in simple language of the following:

1. Your personal data being processed;
2. The way in which your personal data was collected;
3. The reasons that motivated the collection of personal data;
4. An indication of the person at whose request the collection was made; and,
5. Transfers made or planned to be made with personal data.

75.2 Under the right of access, information or documentation may not be obtained that, although it corresponds to the owner of the personal data, does not strictly fall within the assumptions provided for in paragraph 75.1.

Article 76. Portability of personal data

76.1 As an expression of the right of access, the data subject may request the personal data about himself/herself, which he/she has provided to a controller or database owner, in a structured, commonly used and machine-readable format, and transmit them to another controller or personal data bank owner when:

1. The processing is based on consent or a contractual relationship to which the data subject is a party; or
2. The processing is carried out by automated means.

76.2 When exercising portability, the data subject has the right to have his or her data transmitted directly from one controller or data bank owner to another when it is technically possible, which does not include its exercise imposing an excessive financial , technically excessive or unreasonable burden on the controller or data processor.

76.3 The owner of the personal data bank or the person responsible for the processing who considers that he does not have the aforementioned technical possibility must be able to prove such situation in the event of a request from the National Authority for the Protection of Personal Data in within the framework of a trilateral guardianship procedure, where appropriate.

76.4 Data derived, inferred, or constructed from personal data may be subject to portability provided that the owner of the personal data bank or the data controller so determines. Derived, inferred, or constructed data is considered to be data that has undergone at least one personalization, categorization, or profiling process .

76.5 The portability that this article recognizes does not negatively affects the rights of third parties.

76.6 Portability does not apply to processing necessary for the performance of powers or functions conferred on public entities.

76.7 The National Authority for the Protection of Personal Data issues the necessary complementary provisions for the correct application of personal data portability.

Article 77. Means for compliance with the right of access

77.1 The information corresponding to the right of access, at the option of the owner of the personal data, may be provided in writing, by electronic means, telephone, image or other suitable means for this purpose .

77.2 The owner of the personal data may choose one of the following methods:

1. On-site visualization.
2. Written, copy, photocopy or facsimile.
3. Electronic transmission of the response, provided that the identity of the interested party and the security and reception of the information are guaranteed.
4. Any other form or means that is appropriate to the configuration or material implementation of the personal data bank or the nature of the processing, established by the owner of the personal data bank or the person responsible for the processing.

77.3 Whatever the form used, access must be in a clear, legible and intelligible format, without using keys or codes that require mechanical devices for proper understanding and, where appropriate, accompanied by an explanation. Access must be in a language accessible to the average knowledge of the population, of the terms that
are used.

77.4 Without prejudice to the foregoing, in order to use the most environmentally friendly means of communication available in each case, the data controller may agree with the data subject on the use of means of reproducing the information other than those established in this Regulation.

Article 78. Content of the information

The information made available to the data subject when exercising the right of access must be comprehensive and include the provisions of Article 75 of this Regulation, even if the request only covers one aspect of that information. The report may not reveal data belonging to third parties, even if they are linked to the data subject.

Article 79. Update

79.1 It is the right of the owner of personal data, by way of rectification , to update those data that have been modified at the date of exercising the right.

79.2 The update request must indicate the personal data to which it refers , as well as the modification that must be made to them, accompanying the documentation that supports the origin of the
update requested.

Article 80. Rectification

80.1 It is the right of the owner of personal data to have any data that is found to be inaccurate, erroneous or false modified.

80.2 The rectification request must indicate which personal data it refers to, as well as the correction that must be made to them, accompanying the documentation that supports the origin of the requested rectification.

Article 81. Inclusion

81.1 It is the right of the owner of personal data to have their data incorporated into a personal data bank for rectification, and to have any missing information that makes their personal data incomplete, omitted or eliminated in the processing of their personal data incorporated in light of its relevance to said processing.

81.2 The request for inclusion must indicate the personal data to which it refers , as well as the incorporation that must be carried out in them, accompanying the documentation that supports the origin and well-founded interest for the same.

Article 82. Suppression or cancellation

82.1 The owner of the personal data may request the deletion or cancellation of his or her personal data when these are no longer necessary or relevant for the purpose for which they were collected, when the period established for their processing has expired, when he or she has revoked his or her consent for the processing and in other cases in which they are not being processed in accordance with the Law and this Regulation.

82.2 The request for deletion or cancellation may refer to all of the data subject's personal data contained in a personal data bank or only to a part of them.

82.3 Within the provisions of article 20 of the Law and numeral 3 of article III of this Regulation, the presentation of the deletion request to the data controller implies the cessation of the processing of personal data by blocking them while their subsequent elimination is evaluated.

Article 83. Communication of deletion or cancellation

The owner of the personal data bank or the person responsible for the processing must document to the owner of the personal data that they have complied with the request and indicate the transfers of the deleted data, identifying to whom or to whom they were transferred, as well as the communication of the corresponding deletion.

Article 84. Inadmissibility of deletion or cancellation

Deletion is not applicable when personal data must be retained for historical, statistical or scientific reasons in accordance with applicable legislation or, where appropriate, in contractual relationships between the controller and the owner of the personal data, which justify the processing of the same.

Article 85. Protection in case of denial of
deletion or cancellation

Whenever possible, depending on the nature of the reasons for the refusal provided for in the preceding article, means of dissociation or anonymization should be used to continue processing.

Article 86. Opposition

86.1 The owner of personal data has the right to object at any time to the processing of his or her personal data not being carried out or to its cessation, if he or she has not given his or her consent for its collection because it was taken from a publicly accessible source.

86.2 Even if he or she has given consent, the owner of personal data has the right to object to the processing of his or her data, if he or she can prove the existence of well-founded and legitimate reasons related to a specific personal situation that justify the exercise of this right.

86.3 If the opposition is justified, the owner of the personal data bank or the data controller must proceed to cease the processing that gave rise to the opposition.

86.4 Unless there is a prior contractual relationship supporting such processing, where personal data are processed for advertising and commercial prospecting purposes, including profiling , the data subject may exercise his or her right to object at any time in accordance with the requirements of this Regulation.

86.5 When personal data is processed online, the exercise of the right to object may include the de-indexing of the personal data.

Article 87. Right to the objective processing of personal data

87.1 The owner of the personal data has the right not to be subject to decisions, automated or not, that produce legal effects, discrimination or significantly affect him/her, including those based on

only in automated treatments intended to evaluate, analyze or predict, without human intervention, certain personal aspects of the same, in particular, their professional performance, economic situation, health status, sexual orientation or identity, reliability or behavior, among others, considering the exceptions contemplated in article 23 of the Law.

87.2 To ensure the exercise of the right to objective processing, in accordance with the provisions of Article 23 of the Law, when personal data are processed as part of a decision-making process without the participation of the data subject, the owner of the personal data bank or the data controller must inform the data subject as soon as possible, without prejudice to the provisions for the exercise of other rights in the Law and this Regulation.

CHAPTER III
PROCEDURE FOR PROTECTION

Article 88. Direct protection procedure

88.1 The exercise of the rights regulated by the Law and this Regulation begins with the request that the owner of the personal data must address directly to the owner of the personal data bank or the data controller.

88.2 The owner of the personal data bank or data controller must respond within the timeframes provided for in this Regulation, stating the relevant details for each aspect of the request. If the deadline elapses without receiving a response, the applicant may consider their request denied.

88.3 A denial or unsatisfactory response entitles the applicant to initiate the administrative procedure before the Personal Data Protection Directorate.

Article 89. Requirements for the initiation of the trilateral protection procedure

The trilateral procedure for the protection of the rights of personal data subjects is subject to the provisions of this Regulation and Law No. 27444, the General Administrative Procedure Law, or any other law that replaces it, where applicable. Notwithstanding the foregoing, the request from the personal data subject must meet the following requirements:

1. The application to initiate the administrative procedure for protection or claim must contain the requirements in accordance with Law No. 27444, General Administrative Procedure Law, or any other law that replaces it.

2. The charge of the request that you previously sent to the owner of the personal data bank or data controller to obtain, directly, the protection of your rights.

3. The document containing the response from the owner of the personal data bank or the data controller, which, in turn, contains the denial of your request or the response you consider unsatisfactory, if you have received one.

4. Documents proving the violation of the rights of the data subject in accordance with the conditions regulated by the Law and this Regulation, where applicable.

Article 90. Response to the claim

When the Personal Data Protection Directorate has admitted the claim for processing, it is forwarded to the respondent and a period of fifteen (15) days is granted, subject to the provisions of article 223 of Law No.
27444, General Administrative Procedure Law or any other law that replaces it.

Article 91. Deadline for resolution

91.1 The maximum period in which the trilateral protection procedure must be resolved is thirty (30) days, counted from the day after receiving the response from the respondent or from the expiration of the period to formulate it, and may be extended for a maximum of thirty (30) additional days, depending on the complexity of the case.

91.2 If audit actions are carried out at the request of the Personal Data Protection Directorate, the period provided for resolution is suspended until the corresponding report is received.

Article 92. Challenge

92.1 The only recourse against the resolution of the trilateral protection procedure is the appeal in accordance with the provisions of Article 227 of Law No. 27444, the General Administrative Procedure Law, or any other law that replaces it.

92.2 The appeal is filed before the Personal Data Protection Directorate, which must issue the granting of the appeal.

Subsequently, the Directorate of Personal Data Protection must submit the administrative file to the General Directorate of Transparency, Access to Public Information and Protection of Personal Data within two (02) days of having been notified of the aforementioned concession.

92.3 The General Directorate of Transparency, Access to Public Information and Protection of Personal Data, within fifteen (15) days of receiving the administrative file, forwards the appeal to the other party, which must present its acquittal within a maximum period of fifteen (15) days.

92.4 Once the aforementioned acquittal has been received or the deadline established for such purpose has expired, the appeal shall be resolved by the General Directorate of Transparency, Access to Public Information and Protection of Personal Data within a maximum period of thirty (30) days. This resolution exhausts the administrative proce

Article 93. Precautionary measures

Precautionary measures are appropriate at any stage of the trilateral protection procedure before the Directorate of Personal Data Protection, subject to the provisions of Law No. 27444, the General Administrative Procedure Law, or any other law that replaces it, where applicable.

Article 94. Audit actions

For better resolution, the Directorate of Personal Data Protection may require the Directorate of Supervision and Instruction to carry out inspection actions , which must be carried out within five (5) days after receiving such request.

TITLE III
INFRACTIONS AND PENALTIES

CHAPTER I
INSPECTION

Article 95. Purpose

The purpose of auditing activity is to carry out a set of acts and procedures of investigation, supervision, control or inspection on compliance with obligations regarding the protection of personal data, prohibitions and other limitations required by those administered who process personal data, derived from a legal or regulatory standard, contracts with the State or other legal source, under an approach of regulatory compliance, risk prevention, risk management and protection of protected legal assets.

Article 96. Commencement of inspection activity

96.1 The inspection activity always begins with office as a result of:

1. Direct initiative of the Directorate of Supervision and Instruction; or,

2. By complaint from any public entity, natural or legal person.

96.2 In all cases, the Directorate of Supervision and Instruction requires the owner of the personal data bank, the person in charge or whoever is responsible, information related to the processing of personal data or the necessary documentation.

96.3 For the purposes of the supervisory activity , the Directorate of Supervision and Instruction is authorized to carry out the activities provided for in article 228-
B of Law No. 27444, General Administrative Procedure Law or any other that replaces it.

Article 97. Types of inspection activity
The inspection activity is classified as:

1. In Person: Inspection action carried out outside the offices of the General Directorate of Transparency, Access to Public Information and Protection of Personal Data, in the presence of the owner of the personal data bank, the person in charge or whoever is responsible or their representatives.

2. In the office: Audit action carried out from the headquarters of the General Directorate of Transparency, Access to Public Information and Protection of Personal Data and which involves access and evaluation through digital means of the activities carried out by the owner of the personal data bank, the person in charge or whoever is responsible for the processing of personal data.

Article 98. Renewal

If the complaint filed shows that it is not directed towards the objectives of an inspection , but rather towards the protection of rights, it is redirected to a claim within the framework of a trilateral protection procedure.

Article 99. Public faith

In the exercise of oversight activities , the staff of the Directorate of Oversight and Instruction is provided with public faith to verify the veracity of the facts in relation to the procedures under their charge.

Article 100. Requirements for reporting

The complaint must indicate the following:

1. Name of the complainant and address for purposes to receive notifications in accordance with the provisions of Article 20 of Law 27444.

2. Statement of the facts on which you base your complaint and the documents that support it.

3. Name and address of the person reported or, where applicable, location information.

Article 101. Form of the complaint

101.1 The complaint may be submitted in physical form or using the forms published on the Institutional Portal of the Ministry of Justice and Human Rights.

101.2 When the complaint is submitted by digital means, through the system established by the General Directorate of Transparency, Access to Public Information and Protection of Personal Data, it is understood that it is accepted that the notifications are made by said system or through other electronic means generated by it.

101.3 The complainant may request that the reservation of their identity.

Article 102. Request for information

When a complaint is filed, the Directorate of Inspection and Investigation may request the documentation that the complainant deems appropriate for the development of the inspection .

Article 103. Action of in-person inspection

103.1 In-person inspections are carried out without prior notice, except in certain circumstances and to ensure the effectiveness of the inspection . The Directorate of Inspection and Investigation, when it deems appropriate, shall notify the person being inspected of the date and time of the inspection within a reasonable period of time .

103.2 The in-person inspection action may include several visits to obtain the necessary evidence. After the first unannounced visit, if applicable, the individual being inspected is notified in advance of subsequent visits .

103.3 Inspection visits require the corresponding report to be drawn up, which records the actions taken during the visit. This report must be signed by the inspection staff , the administrator, or the staff who participated in the procedure. If the latter refuse to receive or sign the report, this is noted in the report, but does not affect its validity. The signature of the person being inspected does not imply their agreement with its content, but only their participation and acceptance of it.

103.4 The minutes are prepared in duplicate, and one copy is given to the administrator. The minutes may include any statement the participants deem appropriate to their rights.

103.5 In the event that the inspection visit is not carried out due to obstruction or hindrance by the administrator or his staff, the respective report is drawn up, recording the reason that prevented it from being carried out.

Article 104. Identification of the supervisory staff

104.1 At the beginning of the visit, the inspection staff must show a valid photo ID issued by the Inspection and Instruction Directorate that accredits them as such.

104.2 The personnel carrying out inspection visits must be provided with a written order with the official's handwritten signature , of which a copy is left, at the person's expense, to the person who attended the visit.

104.3 The order must specify the place or places where the public or private entity or natural person being inspected is located , or where the personal data banks being inspected are located , the general purpose of the visit and the legal provisions that support it.

Article 105. Content of the audit reports

The inspection reports must state:

1. Name, denomination or business name of the person inspected.

2. Time, day, month and year in which the session begins and ends supervision .

3. Data that fully identifies the place where the inspection was carried out , such as street, avenue, passage, number, district, postal code, the public or private entity where the place where the inspection was carried out is located , as well as the telephone number or other form of communication available with the person being inspected.

4. Type of inspection action .

5. Number and date of the inspection order that the reason.

6. Name and position of the person who assisted the inspectors .

7. Data and details relating to the performance.

8. Statement from the inspected party if requested.

9. Request for information made and the deadline granted for its delivery, if applicable.

10. Name and signature of those involved in the audit , including those who carried it out.

Article 106. Obstruction of inspection

If the person being audited directly refuses to cooperate or observes obstructive conduct, unreasonably delaying their cooperation, raising unreasonable questions about the audit work , ignoring the instructions of the audit officers or any other similar or equivalent conduct, this must be recorded in the minutes, specifying the obstructive act or acts and their repetition, if applicable.

Article 107. Observations in the act of inspection or subsequent

Without prejudice to the fact that those inspected may make observations during the inspection and state what is appropriate to their rights in relation to the facts contained in the minutes, they may also do so in writing within the term of five (5) days following the date of the inspection action .

Article 108. Audit report

108.1 The audit concludes with the issuance of a report that may contain:

1. Certificate of compliance with the activity carried out by the administrator.

2. The recommendation of improvements or corrections to the activity carried out by the administrator.

3. The warning of the existence of non-compliance that is not likely to warrant the determination of administrative responsibilities.

4. The recommendation to initiate a procedure in order to determine the corresponding administrative responsibilities.

5. Provision for the adoption of corrective measures, under penalty of recommending the initiation of sanctioning proceedings.

108.2 The report on the conclusion of the inspection must be prepared within a maximum period of ninety (90) days. This period begins on the date on which the Directorate of Inspection and Instruction receives the complaint or initiates the inspection proceedings ex officio . The established period may be extended only once and for up to a period of forty-five (45) days, by reasoned decision, taking into account the complexity of the case.

subject matter .

Article 109. Inadmissibility of means of appeal

No appeal may be filed against any of the forms of conclusion of the inspection activity issued by the Inspection and Instruction Directorate; any contradiction of its content and any form of defense regarding it may be asserted in the course of the administrative sanctioning procedure, if applicable.

CHAPTER II
SANCTIONING PROCEDURE

Article 110. Authorities of the sanctioning procedure

For the purposes of applying the rules on the administrative sanctioning procedure established in the Law, the authorities are the following:

1. The Directorate of Supervision and Instruction is competent to conduct and develop the investigation phase and is responsible for carrying out the actions necessary to determine the circumstances of the commission, performance of evidence, impute charges for acts contrary to the provisions of the Law and these Regulations, and issue the Final Investigation Report, as appropriate.

2. The Personal Data Protection Directorate is competent to rule in the first instance on the existence of an infringement and the imposition of sanctions, and to dictate precautionary and corrective measures aimed at the protection of personal data, as well as to resolve the appeal for reconsideration filed against its resolutions, as appropriate.

3. The General Directorate of Transparency, Access to Public Information and Protection of Personal Data acts as the second and final administrative authority in the administrative sanctioning procedure, and its decision exhausts the administrative process.

Article 111. Initiation of the sanctioning procedure

111.1 The sanctioning procedure begins with the notification of the resolution of imputation of charges to the administered, which is carried out by the Directorate of Supervision and Instruction, in accordance with the provisions of section 3 of article 234 of Law No. 27444, General Administrative Procedure Law or another that replaces it.

111.2 The complainant may appeal against the resolution declaring the dismissal or total or partial inadmissibility of his complaint.

Article 112. Content of the resolution to initiate the sanctioning procedure

112.1 The Directorate of Supervision and Instruction notifies the resolution of charges that contains the following:

1. The identification of the competent authority to impose the sanction, identifying the rule that grants said authority.

2. The facts that motivate the start of the administrative sanctioning procedure, which includes the statement of the facts attributed to the administrator and the qualification of the infractions that such facts may cause.
make up.

3. The identification of the person against whom the procedure is opened.

4. The sanction or sanctions that may be imposed.

5. The deadline for submitting defenses and evidence.

6. The rules that classify acts or omissions as administrative infractions.

112.2 Upon notification of the imputation resolution the Inspection Report is attached to the charges .

Article 113. Presentation of defenses and evidence

113.1 The administrator, within a maximum period of fifteen (15) days, counted from the day following the corresponding notification, may present his discharge, in which he may expressly pronounce himself regarding each of the facts that are expressly imputed to him, affirming them, denying them, indicating that he is unaware of them because they are not his own or explaining how they occurred, as the case may be. Likewise, he may present the corresponding evidentiary means.

113.2 In the discharges, the administrator may expressly and in writing acknowledge his responsibility, the evaluation of which is considered as a case of mitigation of responsibility for the purposes of calculating the sanction.

Article 114. Actions for the investigation of the facts

Once the period of fifteen (15) days for the presentation of the discharge has expired, with or without it, the Directorate of

The Supervision and Instruction Office carries out ex officio all the actions necessary for the examination of the facts and may order inspection visits or the presentation of evidence, if it has not done so previously, in order to gather the information that is necessary or relevant to determine, where appropriate, the existence of violations subject to sanctions.

Article 115. Final Investigation Report

115.1 The Directorate of Supervision and Instruction issues the Final Instruction Report within a maximum period of fifty (50) days. This period begins on the date on which the resolution to initiate the sanctioning procedure is notified. The established period may be extended once and for up to a period of fifty (50) days. The instruction report determines in a reasoned manner the conduct considered to constitute an infraction, the rule that provides for the imposition of the sanction, the corresponding sanction proposal or the filing of the procedure, as the case may be.

115.2 If, after the corresponding evaluation, the Directorate of Supervision and Investigation concludes that there are no violations, it must record this in the Final Investigation Report, in which it recommends that the Directorate of Personal Data Protection declare the filing of the administrative sanctioning procedure.

115.3 When the existence of administrative liability for one or more violations is determined, the Directorate of Supervision and Instruction notifies the administrator of the report, granting him a period of five (5) days, counting from the day following the notification , to present his defense to the Directorate of Personal Data Protection. The report does not constitute an appealable act.

Article 116. Resolution of the sanctioning procedure

116.1 The resolution issued by the Personal Data Protection Directorate may or may not accept the recommendation of the Final Investigation Report, and must be duly motivated and rule on the discharges and the facts imputed in order to determine the responsibility of the administrator, the applicable sanction and the corrective measures, if applicable.

116.2 The resolution of the administrative sanctioning procedure is notified to the parties of the procedure, as well as to the complainant when the procedure has originated from some inspection action due to a complaint.

Article 117. Concurrence of infractions

117.1 When the same conduct or fact qualifies as more than one infraction, the fine determined for the most serious infraction is applied, in accordance with section 6 of article 230 of Law No. 27444, General Administrative Procedure Law or another that replaces it.

117.2 When several conducts or acts qualify as independent infractions, the sum of the fines previously determined and individually shall be applied, up to a maximum of double the sanction applicable for the most serious infraction.

Article 118. Challenge

118.1 The reconsideration appeal must be supported by new evidence and is resolved by the Personal Data Protection Directorate within a period not exceeding fifteen (15) days. If the Personal Data Protection Directorate determines that the reconsideration appeal is inadmissible because it is not supported by new evidence, it must be channeled as an appeal, as appropriate.

118.2 The appeal is filed with the same body that issued the resolution being appealed, which then forwards it to the General Directorate of Transparency, Access to Public Information and Protection of Personal Data along with the file. The appeal must be resolved within a period of no more than thirty (30) days from the date of receipt of the administrative file.

118.3 Resolutions issued by the General Directorate of Transparency, Access to Public Information, and Personal Data Protection that resolve appeals exhaust the administrative process. No appeal may be filed through administrative channels, and only contentious administrative proceedings may be filed in accordance with the relevant legislation.

Article 119. Oral report hearing

119.1 Within the framework of the procedures under its jurisdiction, the Directorate of Personal Data Protection and the General Directorate of Transparency, Access to Public Information and Protection of Personal Data may, by their own decision or at the request of a party and in response to their assessment of the specific case, schedule the oral report hearing.

119.2 The oral report hearing may be in person or virtually, as determined by the competent body in light of the circumstances of each specific case.

If the hearing is virtual, the hearing must be recorded by the hearing authority, using video, audio, or any other means that allows for proof of its conduct. A copy is filed in the corresponding administrative file.

119.3 Only representatives or agents of the administrators may participate and speak at the hearing, and they must identify themselves as such before the start of the oral report hearing.

Article 120. On the confidentiality of information

120.1 Information of a confidential nature is considered to be that information which has such nature in accordance with the regime provided for in Law No. 27806, Law of Transparency and Access to Public Information, which has been presented by the parties or third parties within the framework of a procedure within the jurisdiction of the National Authority for the Protection of Personal Data, or generated by the same in the process of the investigation inherent to the exercise of the sanctioning power.

120.2 Confidential information, including but not limited to, includes banking, commercial, industrial, tax, or stock market secrets, as well as information that affects personal and family privacy.

120.3 The information must be for the exclusive use of the public officials in charge of processing the procedure. This information must not be disclosed to other parties or third parties; therefore, the National Data Protection Authority may apply dissociation and/or anonymization procedures, as appropriate.

CHAPTER III
ADMINISTRATIVE MEASURES

Article 121. Provisional and precautionary measures

121.1 Once the sanctioning procedure has been initiated, the Directorate of Personal Data Protection, at the request of the Directorate of Supervision and Instruction, may order the adoption of provisional measures to ensure the effectiveness of the final resolution that may be issued in the aforementioned procedure, in compliance with the applicable rules of Law No. 27444,

General Administrative Procedure Law or any other law that replaces it.

121.2 The Directorate of Personal Data Protection, by means of a reasoned decision, may issue a precautionary measure, based on the likelihood of the existence of an administrative violation, danger in delay and the reasonableness of the measure, in order to safeguard the right to protection of personal data.

Article 122. Corrective measures

122.1 The corrective measure is the measure dictated by the Personal Data Protection Directorate, without prejudice to the corresponding administrative sanction, intended to reverse, correct or reduce, to the extent possible, the harmful effect that the infringing conduct would have produced on the owner of the personal data.

122.2 The Directorate of Personal Data Protection may dictate the following corrective measures:

1. Cessation of processing of personal data obtained disproportionately and/or without consent.
2. Deletion of data that was obtained without the consent of the personal data owner.
3. Actions to reverse or reduce as much as possible the harmful effect of the infringing conduct on the personal data owner.
4. Immediate attention to the right requested by the owner of the personal data.
5. Others arising from current regulations regarding the protection of personal data.

CHAPTER IV
SANCTIONS

Article 123. Graduation of the amount of the sanction administrative fine

123.1 To determine the sanction to be imposed in a specific case, the principle of reasonableness of the sanctioning power recognized in section 3 of article 230 of Law No. 27444, the General Administrative Procedure Law, or any other regulation that replaces it, must be observed.

123.2 The determination of fines is carried out in accordance with the provisions of the Methodology for the calculation of fines, approved by Ministerial Resolution No. 0326-2020-JUS or any regulation that replaces it.

Article 124. Limit to the amount of the sanction administrative fine

124.1 Pursuant to the provisions of the second paragraph of Article 39 of the Law, the individual concerned may prove, in the discharge of the charges, the amount of gross annual income received in the year prior to the date on which the infraction was committed, through sworn statements from the National Superintendence of Customs and Tax Administration, financial statements or other documents of a similar nature.

124.2 If the administrator proves that he is not receiving income, he sends to the Directorate of Inspection and Instruction the necessary information so that the estimate of the income he projects to receive can be made.

Article 125. Mitigating factors of administrative liability

The following are considered mitigating factors of liability:

125.1 Express and written recognition of the infringement committed, which must be made in a clear, precise and unambiguous manner.

125.2 Collaboration with the National Authority and the adoption of amending measures that mitigate the effects of the offending conduct, after the notification of charges. Such measures must be duly substantiated.

125.3 The duly accredited implementation, prior to the start of the administrative sanctioning procedure, of the Code of Conduct, in accordance with the requirements regulated in this Regulation.

125.4 The duly accredited implementation, prior to the start of the administrative sanctioning procedure, of the Impact Assessment relating to the protection of personal data with respect to the questioned processing, in accordance with the requirements regulated in this Regulation.

Article 126. Late payment of fines

126.1 Any administrator who does not make timely payment of fines automatically incurs default; consequently, the amount of unpaid fines accrues default interest that is applied daily from the day following the due date of the fine payment period until the payment date inclusive, multiplying the amount of the unpaid fine by the current daily Default Interest Rate (TIM).

126.2 The current daily Default Interest Rate (TIM) results from dividing the current Default Interest Rate (TIM) by thirty (30).

Article 127. Benefit of prompt payment of the fine

127.1 The administrator may benefit from the early payment benefit by cancelling the fine within the period established by the Directorate of Personal Data Protection in the resolution issued in the first instance, provided that no appeal is filed against said resolution and, consequently, it is accepted.

127.2 The benefit of early payment corresponds to a 40% reduction in the amount of the fine imposed.

127.3. For the early payment benefit to take effect, the conditions mentioned in this Regulation must be met and, in addition, this circumstance must be communicated to the Personal Data Protection Directorate, attaching proof of the corresponding bank deposit.

Article 128. Coercive execution of the fine

The enforcement of the fine is governed by the law on the subject matter relating to the enforcement procedure.

Article 129. Record of sanctions, measures precautionary and corrective measures

The Directorate of Personal Data Protection is responsible for the National Registry of Personal Data Protection, which records those sanctioned for non-compliance with the Law and this Regulation, as well as precautionary and corrective measures. This registry is published on the digital site of the Ministry of Justice and Human Rights, located on the Peruvian State's Single Digital Platform for Citizen Guidance (Gob.pe).

Article 130. Application of coercive fines

130.1 In the event of non-compliance with corrective measures and precautionary measures, the Personal Data Protection Directorate imposes coercive fines, automatically and without prior request, according to the following graduation:

1. For minor infractions, the coercive fine must be of up to two (2) Tax Units.
2. For serious violations, the coercive fine must be no less than two (2) to six (6) Tax Units.

3. For very serious infractions, the coercive fine must be no less than six (6) to ten (10) Tax Units.

130.2 In the event of persistent non-compliance with any of the mandates referred to in paragraph 130.1, a new coercive fine may be imposed, successively doubling the amount of the last fine imposed up to the limit of one hundred (100) Tax Units (UIT).

130.3 The corresponding fine must be paid within a period of five (5) days, after which its coercive collection is ordered.

130.4 Against the imposition of a coercive fine no the filing of an appeal is appropriate.

130.5 The National Authority for the Protection of Personal Data approves the provisions necessary to regulate the application of coercive fines.

CHAPTER V
INFRACTIONS

Article 131. Infractions

Violations of the Law or this Regulation are classified as minor, serious and very serious, and are punishable by a fine in accordance with Article 39 of the aforementioned Law.

Article 132. Minor infractions

The following are minor infractions:

1. Process personal data that is not necessary, relevant or adequate in relation to the specific, explicit and lawful purposes for which it needs to be obtained.

2. Not to modify or rectify the personal data being processed when its inaccurate or incomplete nature is known.

3. Failure to delete personal data being processed when they are no longer necessary, relevant, or appropriate for the purpose for which they were collected, or when the processing period has expired. In these cases, the violation does not occur when an anonymization or dissociation procedure is used.

4. Failure to register or update in the National Registry of Personal Data Protection the acts established in Article 34 of the Law.

5. Incomplete reporting of two or fewer than two of the conditions for the processing of personal data indicated in Article 18 of the Law.

6. Processing personal data in violation of the security measures established in the regulations on the matter.

7. Respond late to the material exercise of the rights of the personal data owner, when legally appropriate.

8. Failure to report the cross-border flow of personal data to the Personal Data Protection Directorate of the General Directorate of Transparency, Access to Public Information and Personal Data Protection for registration in the National Registry of Personal Data Protection.

9. Failure to designate the Personal Data Officer, when appropriate .

Article 133. Serious violations

The following are serious violations:

1. Failure to attend to, impede or obstruct the exercise material of the rights of the owner of personal data.

2. Failure to comply with the obligation to inform, or incompletely informing, three or more conditions of the processing of personal data to the data subjects, in accordance with the provisions of Article 18 of the Law.

3. Processing personal data without the free, express, unequivocal, prior, and informed consent of the data subject, when such consent is required in accordance with the provisions of the Law and its Regulations.

4. Processing personal data in violation of the security measures established in the regulations on the matter, thereby causing harm to the data subject or unauthorized exposure of their personal data.

5. Processing sensitive personal data in violation of the security measures established in the regulations on the matter.

6. Process sensitive personal data that is not necessary, relevant or adequate in relation to the specific, explicit and lawful purposes for which it needs to be obtained.

7. Use personal data obtained lawfully for purposes other than those that motivated its collection, unless an anonymization or dissociation procedure is used.

8. Unjustifiably deny or delay the National Authority for the Protection of Personal Data from entering the facilities subject to inspection .

9. Unjustifiably refusing to provide the National Authority for the Protection of Personal Data the information or documentation relating to the processing of personal data that it requires within the framework of an ongoing audit or administrative procedure .

10. Obstruct the exercise of the supervisory function of the National Authority for the Protection of Personal Data.

11. Failure to comply with the confidentiality obligation established in Article 17 of the Law.

12. Failure to report a personal data security incident to the National Data Protection Authority when appropriate, as provided for in Article 34 of this Regulation.

13. Failure to register or update in the National Registry for the Protection of Personal Data the acts established in Article 34 of the Law, after having been requested to do so by the National Authority for the Protection of Personal Data.

Article 134. Very serious violations

The following are very serious violations:

1. Processing personal data through fraudulent, unfair or illegal means.

2. Providing false or inaccurate documents or information to the National Personal Data Protection Authority.

3. Failure to comply with corrective measures or precautionary measures ordered in a trilateral protection procedure, despite prior warning.

4. Processing sensitive personal data in violation of the security measures established in the regulations on the matter, thereby causing harm to the owner of the sensitive personal data or unauthorized exposure of their personal data.

sensitive.

Article 135. Recidivism

135.1 It is considered that there is a repeat offense in the commission of an offense when the same acts or omissions that gave rise to a previous offense are committed, provided that the time elapsed between the date of the sanction resolution of the acts or omissions that gave rise to the previous immediate offense becomes final , or has become final, and the date of the performance of the same acts or omissions that give rise to the commission of a new offense is equal to or less than one (1) year.

135.2 For the purposes of recidivism, violations that were not sanctioned due to a series of violations according to numeral 6 are also considered.

of Article 230 of Law No. 27444, General Administrative Procedure Law or any other law that replaces it.

135.3 Recidivism is considered a factor aggravating factor at the time of determining the fine.

SUPPLEMENTARY PROVISIONS
FINALS

First. Validity

This Regulation shall enter into force 120 calendar days after its publication in the official newspaper El Peruano.

The provisions established for the owner of the personal data bank, responsible party or person in charge of processing that are included in the assumptions provided for in numerals 2 and 3 of paragraph 37.1 of article 37 of this Regulation, referring to the designation of the Personal Data Officer , come into force progressively, according to the following schedule:

Holder of the personal data bank, responsible for or in charge of processing personal data	Effective date and mandatory nature
For companies with annual sales exceeding 2300 UIT	1 year after the date of publication of this Regulation
For medium-sized companies with annual sales exceeding 1,700 UIT and up to the maximum amount of 2,300 UIT	2 years after the date of publication of this Regulation
For small businesses with annual sales exceeding 150 UIT and up to the maximum amount of 1,700 UIT	3 years after the date of publication of this Regulation
For micro-enterprises with annual sales up to the maximum amount of 150 ITU and other equivalents	4 years after the date of publication of this Regulation

The provision set forth in Article 76, referring to the Portability of Personal Data, takes effect six months after the entry into force of this Regulation.

Second. Complementary rules

The National Data Protection Authority issues complementary regulations for the implementation of this Regulation.

The National Authority for Personal Data Protection issues a provision or guideline regarding the obligation to report personal data security incidents, for the imputation and imposition of sanctions as a result of non-compliance within the framework of an administrative sanctioning procedure.

Third. Interoperability between public entities

The definition , scope and content of interoperability, as well as the guidelines for its application and operation in accordance with personal data protection regulations, are the responsibility of the Secretariat of Government and Digital Transformation of the Presidency of the Council of Ministers, in its capacity as Governing Body of the National Digital Transformation System.

Interoperability between entities is regulated, in terms of its implementation, in accordance with the provisions established in the Digital Government Law and its Regulations, approved by Legislative Decree No. 1412 and Supreme Decree No. 029-2021-PCM, respectively; and, in the within the framework of the provisions of paragraph 76.2 of article 76 of Law No. 27444, the General Administrative Procedure Law, or any other law that replaces it.

Fourth. "I take care of my personal data" platform

The digital platform "I take care of my personal data" is created, the purpose of which is for the National Authority for the Protection of Personal Data to provide assistance to citizens, in the form of a complaint, when the exercise of the rights established in Law No. 29733, the Personal Data Protection Law, is not attended to, is partially attended to, or is denied, as well as for the filing of complaints by parties for alleged acts contrary to personal data protection regulations.

The platform is managed by the Authority National Personal Data Protection Act.

The Secretariat of Government and Digital Transformation of the Presidency of the Council of Ministers is making the capabilities of the National Digital Government Platform (PNGD) available to the National Authority for the Protection of Personal Data for the implementation of the digital platform "I take care of my personal data."

Fifth. Competencies and promotion of a culture of personal data protection in the use of digital services

The Ministry of Justice and Human Rights, through the National Authority for the Protection of Personal Data, in coordination with the Secretariat of Government and Digital Transformation, as the governing body, promotes actions to develop a culture of protecting citizens' personal data in the digital environment for accessing and using digital services.

Sixth. Resolution of queries regarding personal data protection

The National Data Protection Authority will respond to inquiries regarding personal data protection and the meaning of current regulations, under the terms set forth in Section 10 of Article 33 of the Law, within 30 days.

SUPPLEMENTARY PROVISIONS
TRANSITIONAL

FIRST. Offending conduct committed prior to upon entry into force of this Regulation

Offending conduct committed prior to the entry into force of this Regulation, in accordance with the provisions of the First Final Complementary Provision, is governed by the provisions of the Regulations of Law No. 29733, the Personal Data Protection Law approved by Supreme Decree 003-2013-JUS.

SECOND. Inspection and control activities procedures in progress

The audit activities and administrative procedures initiated upon the entry into force of this Regulation and which are in process are governed by the provisions of the Regulations of Law No. 29733, the Personal Data Protection Law approved by Supreme Decree 003-2013-JUS.

2349653-1