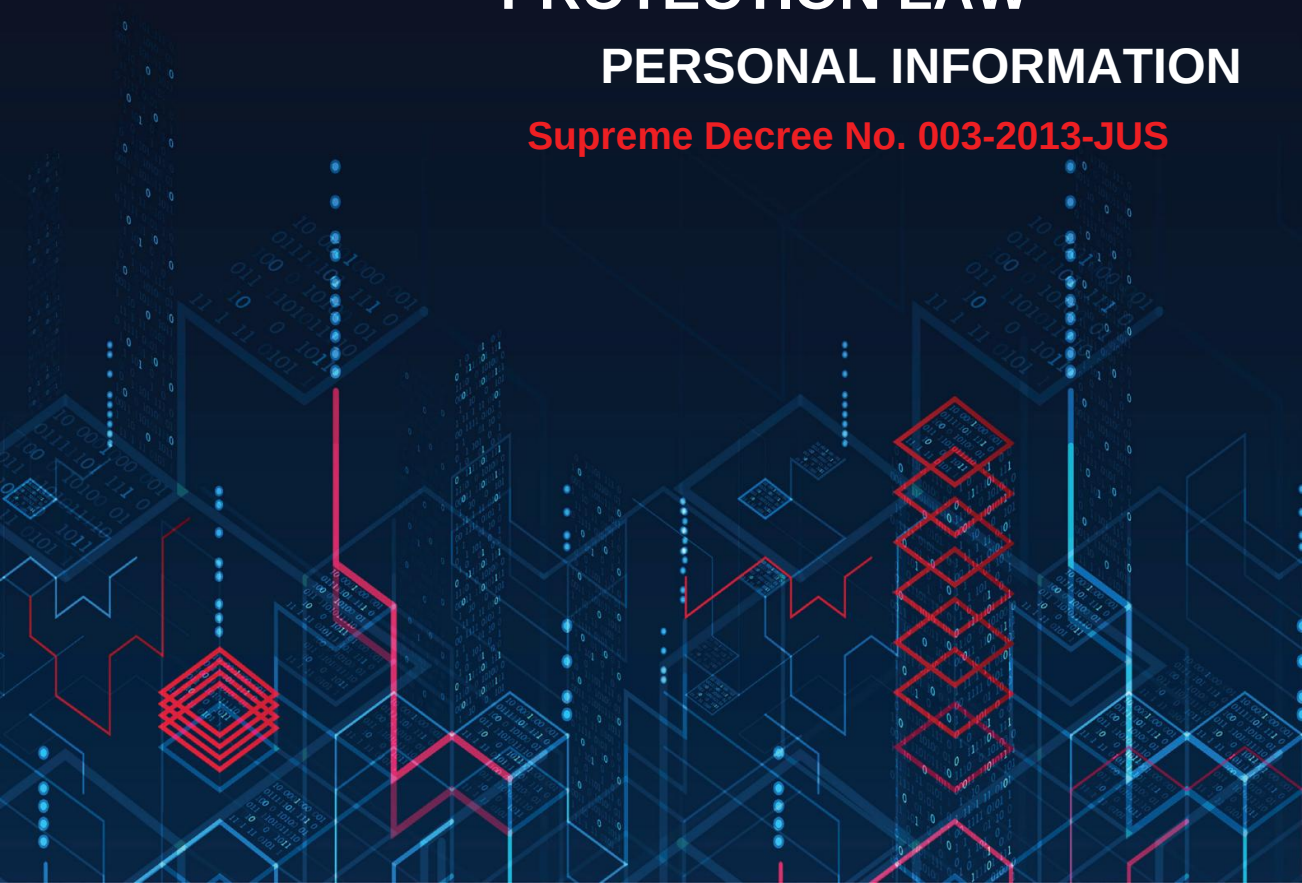
STANDARDS
LEGAL
UPDATED

Editor Peru

DIARIO OFICIAL DEL BICENTENARIO
El Peruano

PROTECTION LAW
PERSONAL INFORMATION
Law No. 29733

REGULATION OF LAW Nº 29733, PROTECTION LAW
PERSONAL INFORMATION
Supreme Decree No. 003-2013-JUS



PROTECTION LAW PERSONAL INFORMATION

LAW Nº 29733

THE PRESIDENT OF THE REPUBLIC

HOW MUCH:

The Congress of the Republic has given the following Law:

THE CONGRESS OF THE REPUBLIC;

He has given the following Law:

PROTECTION LAW PERSONAL INFORMATION

Preliminary Title: General provisions.
Title I: Guiding principles.
Title II: Processing of personal data.
Title III: Rights of the owner of personal data.
Title IV: Obligations of the owner and person in charge of the personal data bank.
Title V: Personal data banks.
Title VI: National Authority for the Protection of Personal information.
Title VII: Infringements and sanctions administrative.
Final supplementary provisions

PRELIMINARY TITLE

GENERAL DISPOSITION

Article 1. Object of the Law This Law has the objective of guaranteeing the fundamental right to the protection of personal data, provided for in article 2, paragraph 6 of the Political Constitution of Peru, through its adequate treatment, within a framework of respect for the other fundamental rights contained therein they recognize.

"Article 2. Definitions

For all purposes of this Law, it is understood as:

1. Personal data bank. Organized set of personal data, automated or not, regardless of the support, whether physical, magnetic, digital, optical or others that are created, whatever the form or modality of its creation, formation, storage, organization and access.

2. Privately administered personal data bank. Personal data bank whose ownership corresponds to a natural person or a legal entity governed by private law, as long as the bank is not strictly linked to the exercise of public law powers.

3. Public administration personal data bank. Personal data bank owned by a public entity.

4. Personal data. Any information about a natural person that identifies him or her or makes him or her identifiable through means that can reasonably be used.

5. Sensitive data. Personal data consisting of biometric data that by themselves can identify the owner; data referring to racial and ethnic origin; economic income; political, religious, philosophical or moral opinions or convictions; union membership; and information related to health or sexual life.

6 days. Business days.

7. Person in charge of processing personal data. Any natural person, legal entity governed by private law or public entity that alone or acting jointly with another carries out the processing of personal data on behalf of the owner of the personal data bank by virtue of a legal relationship that links it to it and delimits the scope of its action. Includes anyone who carries out the treatment without the existence of a bank of personal data.

8. Treatment order. Delivery by the owner of the personal data bank to a person in charge of processing personal data by virtue of a legal relationship that binds them. This legal relationship delimits the scope of action of the person in charge of processing personal data.

9. Public entity. Entity included in article I of the Preliminary Title of Law 27444, Law of General Administrative Procedure, or the one that takes its place.

10. Cross-border flow of personal data. International 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 on which they are located, the means by which the transfer was made or the treatment they receive.

11. Sources accessible to the public. Personal data banks of public or private administration, which can be consulted by any person, upon payment of the corresponding consideration, if applicable. The sources accessible to the public are determined in the regulations.

12. Sufficient level of protection for personal data. Level of protection that includes at least the recording and respect of the guiding principles of this Law, as well as technical security and confidentiality measures, appropriate according to the category of data in question.

13. Legal entity under private law. For the purposes of this Law, the legal entity not included in the scope of article I of the Preliminary Title of Law 27444, Law of General Administrative Procedure.

14. Anonymization procedure. Processing of personal data that prevents identification or does not make the owner of the data identifiable. The procedure is irreversible.

15. Dissociation procedure. Processing of personal data that prevents identification or does not make the owner of the data identifiable. The procedure is reversible.

16. Owner of personal data. Natural person to whom the personal data corresponds.

17. Owner of the personal data bank. Natural person, legal entity under private law or public entity that determines the purpose and content of the personal data bank, its processing and security measures.

18. Transfer of personal data. Any transmission, supply or manifestation of personal data, of a national or international nature, to a legal entity governed by private law, to a public entity or to a natural person other than the owner of personal data.

19. Processing of personal data. Any technical operation or procedure, automated or not, that allows the collection, recording, organization, storage, conservation, elaboration, modification, extraction, consultation, use, blocking, deletion, communication by transfer or dissemination or any other form of processing that facilitates access, correlation or interconnection of personal data."

(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.

"Article 3. Scope of application

This Law applies to personal data contained or intended to be contained in personal data banks of public administration and private administration, whose processing is carried out in the national territory.

Sensitive data are subject to special protection.

The provisions of this Law are not application to the following personal data:

1. To the contents or intended to be contained in personal data banks created by natural persons for purposes exclusively related to their private or family life.

2. To the contents or intended to be contained in public administration data banks, only insofar as their processing is necessary for strict compliance with the powers assigned by law to the respective public entities, for national defense, public security, and for the development of activities in criminal matters for the investigation and repression of crime."

(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.

TITLE I

GUIDING PRINCIPLES

Article 4. Principle of legality The processing of personal data is carried out in accordance with the provisions of the law. It is prohibited collection of personal data by fraudulent, unfair or illicit means.

Article 5. Principle of consent For the processing of personal data The consent of its owner must be obtained.

Article 6. Principle of purpose Personal data must be collected for a specific, explicit and lawful purpose.

The processing of personal data must not be extended to another purpose that has not been unequivocally established as such at the time of its collection, excluding cases of activities of historical, statistical or scientific value when a dissociation or anonymization procedure is used. .

Article 7. Principle of proportionality All processing of personal data must be adequate, relevant and not excessive to the purpose for which it was collected.

Article 8. Quality principle The personal data that will be processed must be true, accurate and, to the extent possible, updated, necessary, relevant and appropriate with respect to the purpose for which they were collected. They must be kept in a way that guarantees their security and only for the time necessary to fulfill the purpose of the treatment.

Article 9. Security principle The owner of the personal data bank and the person in charge of its processing must adopt the necessary technical, organizational and legal measures to guarantee the security of personal data. Security measures must be appropriate and consistent with the processing to be carried out and the category of personal data in question.

Article 10. Principle of disposal resource

Every owner of personal data must have the necessary administrative or jurisdictional means to claim and enforce their rights, when these are violated by the processing of their personal data.

Article 11. Principle of adequate level of protection For the cross-border flow of personal data, a sufficient level of protection must be guaranteed for the personal data to be processed or, at least, comparable to that provided for by this Law or by the international standards on the matter.

"Article 12. Value of the principles

The actions of the owners and those in charge of processing personal data and, in general, of all those involved in relation to personal data, must comply with the guiding principles referred to in this Title. This list of guiding principles is indicative.

The aforementioned guiding principles also serve as an interpretive criterion to resolve issues that may arise in the application of this Law and its regulations, as well as a parameter for the elaboration of other provisions and to fill gaps in the legislation on the matter.

(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.

TITLE II

PROCESSING OF PERSONAL DATA

Article 13. Scope of the treatment of personal information

13.1 The processing of personal data must be carried out with full respect for the fundamental rights of its owners and the rights that this Law confers on them. The same rule applies to its use by third parties.

13.2 Limitations on the exercise of the fundamental right to the protection of personal data can only be established by law, respecting its essential content and be justified by the respect of other fundamental rights or constitutionally protected assets.

13.3 Special measures are issued through regulations for the processing of personal data of children and adolescents, as well as for the protection and guarantee of their rights. To exercise the rights recognized by this Law, children and adolescents act through their legal representatives, and the regulations may determine the applicable exceptions, if applicable, taking into account the best interests of the child and adolescent. .

13.4 Communications, telecommunications, computer systems or their instruments, when they are of a private nature or private use, can only be opened, seized, intercepted or intervened by reasoned order of the judge or with the authorization of their owner, with the guarantees provided by law. . Secrecy is kept regarding matters unrelated to the fact that motivates its examination.

Personal data obtained in violation of this provision has no legal effect.

13.5 Personal data can only be processed with the consent of the owner, except by authoritative law in this regard. Consent must be prior, informed, express and unequivocal.

13.6 In the case of sensitive data, consent for the purposes of its processing must also be given in writing. Even without the consent of the owner, the processing of sensitive data can be carried out when the law authorizes it, as long as it meets important reasons of public interest.

13.7 The owner of personal data may revoke his or her consent at any time, observing the same requirements as when granting it.

13.8 The processing of personal data related to the commission of criminal offenses or Administrative actions can only be carried out by the competent public entities, unless there is a management agreement in accordance with Law 27444, Law of General Administrative Procedure, or the one that takes its place. When the cancellation of criminal, judicial, police and administrative records has occurred, these data cannot be provided unless required by the Judiciary or the Public Ministry, in accordance with the law.

13.9 The commercialization of personal data contained or intended to be contained in personal data banks is subject to the principles provided for in this Law.

"Article 14. Limitations on consent for the processing of personal data

The consent of the owner of personal data is not required for the purposes of its processing, in the following cases:

1. When personal data are collected or transferred for the exercise of the functions of public entities within the scope of their powers.

2. When it involves personal data contained or intended to be contained in sources accessible to the public.

3. When it comes to personal data related to financial and credit solvency, in accordance with the law.

4. When there is a rule for the promotion of competition in regulated markets issued in the exercise of the regulatory function by the regulatory bodies referred to in Law 27332, Framework Law of the Regulatory Bodies of Private Investment in Public Services, or whoever takes his place, as long as the information provided is not used to the detriment of the user's privacy.

5. When the personal data are necessary for the preparation, celebration and execution of a contractual relationship in which the owner of the personal data is a party, or when it is personal data that derives from a scientific or professional relationship of the owner and is necessary for its development or fulfillment.

6. When it involves personal data related to health and is necessary, in a risk circumstance, for the prevention, diagnosis and medical or surgical treatment of the owner, provided that said treatment is carried out in health establishments or by health sciences professionals. health, observing professional secrecy; or when there are reasons of public interest provided for by law or when they must be treated for reasons of public health, both reasons must be qualified as such by the Ministry of Health; or for carrying out epidemiological or similar studies, as long as appropriate dissociation procedures are applied.

7. When the processing is carried out by non-profit organizations whose purpose is political, religious or union and refers to the personal data collected from their respective members, which must be related to the

purpose to which their activities are limited, and cannot be transferred without their consent.

8. When an anonymization or dissociation procedure has been applied.

9. When the processing of personal data is necessary to safeguard the legitimate interests of the owner of personal data by the owner of personal data or by the person in charge of processing personal data.

10. When the processing is for purposes linked to the money laundering and terrorist financing prevention system or others that respond to a legal mandate.

11. In the case of economic groups made up of companies that are considered subjects obliged to report, in accordance with the rules that regulate the Financial Intelligence Unit, they may share information among themselves about their respective clients for the purposes of preventing money laundering. assets and financing of terrorism, as well as other regulatory compliance, establishing appropriate safeguards on the confidentiality and use of the information exchanged.

12. When the processing is carried out in a constitutionally valid exercise of the fundamental right to freedom of information.

13. Others that derive from the exercise of powers expressly established by Law."

(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.

"Article 15. Cross-border flow of personal data

The owner and processor of personal data must carry out the cross-border flow of personal data only if the recipient country maintains adequate levels of protection in accordance with this Law.

In the event that the recipient country does not have an adequate level of protection, the issuer of the cross-border flow of personal data must guarantee that the processing of personal data is carried out in accordance with the provisions of this Law.

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

1. Agreements within the framework of international treaties on the matter to which the Republic of Peru is a party.

2. International judicial cooperation.

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

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

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

6. When the cross-border flow of personal data is carried out for the protection, prevention, diagnosis or medical or surgical treatment of its owner; or when necessary to carry out epidemiological or similar studies, as long as appropriate dissociation procedures are applied.

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

8. Others established by the regulations of this Law, subject to the provisions of article 12." ***(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

Article 16. Security of personal data processing For the purposes of personal data processing, the owner of the personal data bank must adopt technical, organizational and legal measures that guarantee its security and prevent its alteration, loss, processing or unauthorized access.

The requirements and conditions that personal data banks must meet in terms of security are established by the National Authority for the Protection of Personal Data, except for the existence of special provisions contained in other laws.

The processing of personal data in data banks that do not meet the requirements and security conditions referred to in this article is prohibited.

Article 17. Confidentiality of personal data The owner of the personal data bank, the person in charge and those who intervene in any part of its processing are obliged to maintain confidentiality regarding them and their background. This obligation subsists even after the relationship with the owner of the personal data bank has ended.

The obligated party may be relieved of the obligation of confidentiality when there is prior, informed, express and unequivocal consent of the owner of the personal data, a consented or enforceable judicial resolution, or when there are well-founded reasons related to national defense, public security or public health. , without prejudice to the right to maintain professional secrecy.

TITLE III

RIGHTS OF THE OWNER OF PERSONAL INFORMATION

"Article 18. Right to information of the owner of personal data The owner of personal data has the right to be informed in detail,

simply, expressly, unequivocally and prior to its collection, about the purpose for which your personal data will be processed; who the recipients are or may be, the existence of the data bank in which they will be stored, as well as the identity and address of the owner and, if applicable, of the person(s) in charge of processing your personal data; the mandatory or optional nature of your responses to the proposed questionnaire, especially with regard to sensitive data; the transfer of personal data; the consequences of providing your personal data and your refusal to do so; the length of time for which your personal data is kept; and the possibility of exercising the rights that the law grants you and the means provided for this.

If personal data is collected online through electronic communications networks, the obligations of this article may be satisfied by publishing privacy policies, which must be easily accessible and identifiable.

In the event that the owner of the data bank establishes a link with a person in charge of processing after consent, the actions of the person in charge remain under the responsibility of the Owner of the Data Bank, and must establish a personalized information mechanism for the owner of the data. personal information about said new data processor.

If, after consent, the transfer of personal data occurs due to a merger, portfolio acquisition, or similar cases, the new owner of the data bank must establish an effective information mechanism for the owner of the personal data about said new data processor. ". ***(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

Article 19. Right of access of the owner of personal data The owner of personal data has the right to obtain the information about himself that is subject to processing in public or private administration data banks, the way in which his data was collected, the reasons that motivated its collection and at whose request the collection was carried out, as well as the transfers made or planned to be made.

"Article 20. Right to update, inclusion, rectification and deletion

The owner of personal data has the right to update, include, rectify and delete his or her personal data subject to processing, when they are partially or totally inaccurate, incomplete, when an omission, error or falsehood has been noticed, when they are no longer necessary. or pertinent to the purpose for which they were collected or when the period established for their processing has expired.

If your personal data has been previously transferred, the person in charge of processing of personal data must communicate the update, inclusion, rectification or deletion to those who have been transferred, in the event that the processing is maintained by the latter, who must also proceed with the update, inclusion, rectification or deletion, as appropriate.

During the process of updating, inclusion, rectification or deletion of personal data, the person in charge of processing personal data arranges for it to be blocked, preventing third parties from accessing it. Said blockade is not applicable to public entities that require such information for the proper exercise of their powers, according to law, which must inform that any of the aforementioned processes are in progress.

The deletion of personal data contained in public administration personal data banks is subject to the provisions of article 21 of the Single Ordered Text of Law 27806, Law of Transparency and Access to Public Information, or whatever replaces it. ***(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

"Article 21. Right to prevent supply

The owner of personal data has the right to prevent these from being provided, especially when this affects their fundamental rights. The right to prevent the supply does not apply to the relationship between the owner of the personal data bank and the person in charge of processing personal data for the purposes of their processing. ***(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

"Article 22. Right of opposition

Provided that the law does not provide otherwise and when consent has not been given, the owner of personal data may oppose its processing when there are well-founded and legitimate reasons related to a specific personal situation. In the event of justified opposition, the owner or person in charge of processing personal data, as appropriate, must proceed to delete it, in accordance with the law. ***(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

Article 23. Right to objective processing The owner of personal data has the right not to be subject to a decision with legal effects on him or her or that significantly affects him or her, based solely on processing of personal data intended to evaluate certain aspects of his or her personality. or conduct, unless this occurs within the framework of the negotiation, celebration or execution of a contract or in cases of evaluation for the purposes of incorporation into a public entity, in accordance with the law, without prejudice to the possibility of defending your point of view. view, to safeguard your legitimate interest.

Article 24. Right to guardianship

In the event that the owner or person in charge of the personal data bank denies the personal data owner, in whole or in part, the exercise of the rights established in this Law, the latter may appeal to the National Authority for the Protection of Personal Data by way of claim or to the Judiciary for the purposes of the corresponding habeas data action.

The procedure to be followed before the National Authority for the Protection of Personal Data is subject to the provisions of articles 219 et seq. of Law 27444, Law of General Administrative Procedure, or whatever replaces it.

The resolution of the National Authority for the Protection of Personal Data exhausts the administrative route and enables the imposition of the administrative sanctions provided for in article 39. The regulation determines the corresponding instances.

Contentious-administrative action proceeds against the resolutions of the National Authority for the Protection of Personal Data.

"Article 25. Right to be compensated

The owner of personal data who is affected as a result of non-compliance with this Law by the owner or by the person in charge of processing personal data or by third parties, has the right to obtain the corresponding compensation, in accordance with the law. ***(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

Article 26. Consideration The consideration that the owner of personal data must pay for the exercise of the rights contemplated in articles 19, 20, 21, 22 and 23 before the public administration personal data banks is subject to the provisions set forth in the Law 27444, General Administrative Procedure Law.

In the case of privately administered personal data banks, the exercise of the aforementioned rights is subject to the provisions of the special regulations on the matter.

"Article 27. Limitations

The owners and those in charge of processing personal data of public administration may deny the exercise of the rights of access, deletion and opposition for reasons based on the protection of rights and interests of third parties or when this may hinder judicial or administrative actions in progress linked to the investigation into compliance with tax or pension obligations, to criminal investigations into the commission of misdemeanors or crimes, to the development of health and environmental control functions, to the verification of administrative infractions, or when so provided. the law". ***(*) Article modified by the Third Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

TITLE IV

"OBLIGATIONS OF THE OWNER AND THE PERSONAL DATA PROCESSOR"

(*) Denomination modified by the Fourth Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.

"Article 28. Obligations

The owner and the person in charge of processing personal data, as the case may be, have the following obligations:

1. Carry out the processing of personal data, only with prior informed, express and unequivocal consent of the owner of the personal data, except by authoritative law, with the exception of the cases set forth in article 14 of this Law.

2. Do not collect personal data by fraudulent, unfair or illicit means.

3. Collect personal data that is updated, necessary, relevant and appropriate, in relation to specific, explicit and lawful purposes for which it was obtained.

4. Do not use the personal data being processed for purposes other than those for which they were collected, unless there is an anonymization or dissociation procedure.

5. Store personal data in a way that makes it possible to exercise the rights of its owner.

6. Delete and replace or, where appropriate, complete the personal data being processed when you are aware of its inaccurate or incomplete nature, without prejudice to the rights of the owner in this regard.

7. Delete the personal data being processed when they are no longer necessary or relevant to the purpose for which they were collected or the period for their processing has expired, unless an anonymization or dissociation procedure is involved.

8. Provide the National Authority for the Protection of Personal Data with the information related to the processing of personal data that it requires and allow access to the personal data banks that it manages, for the exercise of its functions, within the framework of a procedure administrative process requested by the affected party.

9. Others established in this Law and in its regulations." ***(*) Article modified by the Fourth Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

TITLE V

PERSONAL DATA BANKS

Article 29. Creation, modification or cancellation of personal data banks

The creation, modification or cancellation of personal administration data banks

public and private administration are subject to what is established by the regulations, except for the existence of special provisions contained in other laws.
In any case, publicity about its existence, purpose, identity and the address of its owner and, if applicable, its manager is guaranteed.

Article 30. Provision of services processing of personal data When, on behalf of third parties, personal data processing services are provided, these cannot be applied or used for a purpose other than that contained in the contract or agreement concluded nor be transferred to other people, not even for their conservation.

Once the provision subject to the contract or agreement has been executed, as the case may be, the personal data processed must be deleted, unless there is express authorization from the person on whose behalf such services are provided when the possibility of subsequent orders is reasonably presumed, in which case can be kept with due security conditions, up to the period determined by the regulations of this Law. ***(*) Article modified by the Fourth Complementary Provision Modifying Legislative Decree No. 1353, published on January 7, 2017, the same that came into force the day after the publication of the Supreme Decree that approves its Regulations and the modification of the Regulations of Organization and Functions of the Ministry of Justice and Human Rights, the text of which is as follows:***

"Article 31. Codes of conduct

31.1 Entities representing the owners or those in charge of processing personal data, private administration, may develop codes of conduct that establish standards for the processing of personal data that tend to ensure and improve the operating conditions of information systems based on the principles guiding principles established in this Law."

(*) Article modified by the Fourth Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.

TITLE VI

NATIONAL PROTECTION AUTHORITY OF PERSONAL DATA

Article 32. Competent body and legal regime The Ministry of Justice, through the National Directorate of Justice, is the National Authority for the Protection of Personal Data. For the proper performance of its functions, it can create offices throughout the country.

The National Authority for the Protection of Personal Data is governed by the provisions of this Law, its regulations and the relevant articles of the Regulations of Organization and Functions of the Ministry of Justice.

It corresponds to the National Authority of Protection of Personal Data carry out all the actions necessary to comply with the object and other provisions of this Law and its regulations. For this purpose, it has sanctioning power, in accordance with Law 27444, Law of General Administrative Procedure, or the one that replaces it, as well as coercive power, in accordance with Law 26979, Law of Coercive Execution Procedure, or the one who takes his place.

The National Authority for the Protection of Personal Data must periodically submit a report on its activities to the Minister of Justice.

To carry out its functions, the National Authority for the Protection of Personal Data has the support and technical advice of the National Government Office Electronic and Information Technology (ONGEI) of the Presidency of the Council of Ministers, or whoever takes its place.

Article 33. Functions of the Authority National Personal Data Protection

The National Data Protection Authority Personnel exercises the following administrative, guiding, regulatory, decision-making, supervisory and sanctioning functions:

1. Represent the country before international bodies regarding the protection of personal data.

2. Cooperate with foreign personal data protection authorities to fulfill their powers and generate bilateral and multilateral cooperation mechanisms to assist each other and provide mutual assistance when required.

3. Manage and keep the Registry updated National Protection of Personal Data.

4. Publish, through the institutional portal, the updated list of personal data banks of public and private administration.

5. Promote dissemination and promotion campaigns on the protection of personal data.

6. Promote and strengthen a culture of protection of the personal data of children and adolescents.

7. Coordinate the inclusion of information on the importance of private life and the protection of personal data in the curricula of all educational levels and also promote the training of teachers on these topics.

8. Monitor compliance with the requirements provided for in this Law, for the cross-border flow of personal data.

9. Issue authorizations, when applicable, in accordance with the regulations of this Law.

10. Answer questions about the protection of personal data and the meaning of current regulations on the matter, particularly those that it has issued.

11. Issue a technical opinion regarding draft regulations that refer in whole or in part to personal data, which is binding.

12. Issue the corresponding directives for the best application of the provisions of this Law and

in its regulations, especially regarding the security of personal data banks, as well as supervising compliance, in coordination with the sectors involved.

13. Promote the use of self-regulation mechanisms as a complementary instrument for the protection of personal data.

14. Celebrate inter-institutional or international cooperation agreements with the purpose of ensuring the rights of people regarding the protection of personal data that are processed inside and outside the national territory.

15. Respond to requests of particular interest from the administrator or general of the community, as well as requests for information.

16. Know, instruct and resolve the claims made by the owners of personal data for the violation of the rights that concern them and dictate the precautionary or corrective measures established by the regulations.

17. Ensure compliance with legislation related to the protection of personal data and respect for its guiding principles.

18. Within the framework of an ongoing administrative procedure, requested by the affected party, obtain from the owners of the personal data banks the information it deems necessary for compliance with the rules on the protection of personal data and the performance of its functions. .

19. Supervise the subjection of the processing of personal data carried out by the owner and the person in charge of the personal data bank to the technical provisions issued by it and, in case of contravention, arrange the corresponding actions in accordance with the law.

20. Initiate inspections ex officio or by complaint from a party for alleged acts contrary to what is established in this Law and its regulations and apply the corresponding administrative sanctions, without prejudice to the precautionary or corrective measures established by the regulations.

21. The other functions assigned to it by this Law and its regulations.

"Article 34. National Protection Registry of Personal Data

The National Registry for the Protection of Personal Data is created as an administrative registry in charge of the National Authority of Protection of Personal Data, with the purpose of registering in a differentiated manner, at the national level, the following:

1. Personal data banks of public or private administration, as well as the data related to them that are necessary for the exercise of the rights that correspond to the holders of personal data, in accordance with the provisions of this Law and its regulations.

The exercise of this function does not make it possible for the National Authority for the Protection of Personal Data to know the content of the personal data banks, except in the case of an ongoing administrative procedure.

2. Communications of cross-border flow of personal data.

3. The sanctions, precautionary or corrective measures imposed by the National Authority for the Protection of Personal Data in accordance with this Law and its regulations.

"Any person can consult in the National Registry for the Protection of Personal Data the existence of personal data banks, their purposes, as well as the identity and address of their owners and, if applicable, their managers."

(*) Article modified by the Fourth Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.

Article 35. Confidentiality

The staff of the National Authority for the Protection of Personal Data are subject to the obligation to maintain confidentiality of the personal data they know due to their functions. This obligation subsists even after any relationship with said authority has ended.

national, under responsibility.

Article 36. Resources of the Authority National Personal Data Protection

They are resources of the National Authority of Protection of Personal Data the following:

1. The fees for the right to process administrative procedures and services under their jurisdiction.

2. The amounts collected as fines.

3. Resources from non-reimbursable international technical cooperation.

4. The legacies and donations you receive.

5. The resources that are transferred in accordance with the law.

The resources of the National Authority of Protection of Personal Data are intended to finance the expenses necessary for the development of its operations and for its operation.

TITLE VII

INFRINGEMENTS AND SANCTIONS ADMINISTRATIVE

Article 37. Sanctioning procedure The sanctioning procedure is initiated ex officio, by the National Authority for the Protection of Personal Data or by complaint from a party, in the event of the alleged commission of acts contrary to the provisions of this Law or its regulations, without prejudice to the procedure followed within the framework of the provisions of article 24.

The resolutions of the National Authority for the Protection of Personal Data exhaust the administrative route.

Against the resolutions of the National Authority of Personal Data Protection, contentious-administrative action proceeds.

"Article 38.- Classification of infractions

Infractions are classified as minor, serious and very serious, which are classified through regulations, in accordance with the provisions of section 4) of article 230 of Law No. 27444, Law of General Administrative Procedure, by Supreme Decree with the vote approval of the Council of Ministers.

Without prejudice to the sanctions that the competent authority imposes within the framework of its jurisdiction, it may order the implementation of one or more corrective measures, with the objective of correcting or reversing the effects that the offending conduct has caused or preventing it from occurring. again.

"The administrators objectively responsible for non-compliance with obligations derived from the regulations on the protection of personal data." ***(*) Article modified by the Fourth Complementary Modifying Provision of Legislative Decree No. 1353, published on January 7, 2017.***

Article 39. Administrative sanctions In case of violation of the rules of this Law or its regulations, the National Authority of Protection of Personal Data may apply the following fines:

1. Minor infractions are punished with a minimum fine of zero point five of one tax tax unit (UIT) up to five tax tax units (UIT).

2. Serious violations are punishable with a fine of more than five tax units (UIT) up to fifty tax units (UIT).

3. Very serious infractions are punishable with a fine of more than fifty units tax units (UIT) up to one hundred tax tax units (UIT).

In no case can the fine imposed exceed ten percent of the annual gross income that the alleged offender would have received during the previous year.

The National Data Protection Authority Personnel determines the infraction committed and the amount of the fine imposed through a duly reasoned resolution. For the grading of the amount of the fines, the criteria established in article 230, numeral 3) of Law 27444, Law of General Administrative Procedure, or whatever replaces it, are taken into account.

The imposition of the fine is carried out without prejudice to the disciplinary sanctions on the personnel of public entities in the cases of personal data banks of public administration, as well as the compensation for damages and any criminal sanctions that may apply. .

Article 40. Coercive fines In application of the provisions of article 199 of Law 27444, Procedure Law General Administrative, or whichever takes its place, the National Authority for the Protection of Personal Data may impose coercive fines for an amount that does not exceed ten tax units (UIT), in the event of non-compliance with the obligations accessory to the sanction, imposed in the sanctioning procedure. Periodic penalty payments are imposed once the compliance period has expired.

The imposition of coercive fines does not prevent the exercise of other means of forced execution, in accordance with the provisions of article 196 of Law 27444, Law of General Administrative Procedure.

The regulations of this Law regulate matters concerning the application of coercive fines.

COMPLEMENTARY PROVISIONS FINALS

First. Regulations of the Law To prepare the draft regulations, a multi-sector commission is established, which is chaired by the National Authority for the Protection of Personal Data.

The draft regulation is prepared within a maximum period of one hundred and twenty business days, from the installation of the multisector commission, which must occur within a period of no more than fifteen business days, counted from the day following the publication of this Law.

Second. Security directive The National Authority for the Protection of Personal Data prepares the information security directive managed by personal data banks within a period of no more than one hundred and twenty business days, counting from the day following the publication of this Law. .

As long as the aforementioned directive is approved and governs, the sectoral provisions on the matter remain in force.

Third. Adaptation of management documents and the Single Text of Procedures Administrative of the Ministry of Justice

Being at the creation of the National Authority for the Protection of Personal Data, within a maximum period of one hundred and twenty business days, counting from the day following the publication of this Law, the Ministry of Justice prepares the pertinent modifications in its documents of management and in its Single Text of Procedures Administrative.

Quarter. Regulatory adaptation Within a period of sixty business days, the Executive Branch sends to the Congress of the Republic a bill that contains the necessary modifications to existing laws for the purposes of their adaptation to this Law.

For lower-ranking standards, the competent public entities review the regulations

corresponding and prepare the necessary proposals for its adaptation to the provisions of this Law.

In both cases, the prior favorable technical opinion of the National Authority for the Protection of Personal Data is required, in accordance with article 33 paragraph 11.

Fifth. Pre-existing personal data banks Personal data banks created prior to
this Law and its respective regulations must adapt to this standard within the period established by the regulations. Without prejudice to this, their owners must declare them before the National Data Protection Authority.

Personal, subject to the provisions of article 29.

Sixth. Habeas data The
rules established in the Constitutional Procedural Code on the habeas data process are applied at the constitutional level, regardless of the administrative field that is the subject of this Law. The administrative procedure established in this Law does not constitute a prior means for the exercise of the right. via constitutional process.

Seventh. Powers of the National Institute for the Defense of Competition and the Protection of Intellectual Property (Indecopi)
The National Data Protection Authority
Personal is competent to safeguard the rights of the owners of the information
administered by the Private Risk Information Centers (Cepirs) or similar in accordance with the terms established in this Law.

Without prejudice to this, in matters of infringement of consumer rights in general through the provision of services and information provided by Cepirs or similar, within the framework of consumer relations, the rules on consumer protection are applicable, The Consumer Protection Commission of the National Institute being the exclusively and exclusively competent entity for supervising compliance.

of Defense of Competition and Protection of Intellectual Property (Indecopi), which must ensure the suitability of goods and services based on the information provided to consumers.

Eighth. Sensitive information For the
purposes of the provisions of Law 27489, Law that Regulates Private Risk Information Centers and Protection of the Owner of the Information, sensitive information is understood to be that defined as sensitive data by this Law.

Likewise, it is specified that the confidential information referred to in paragraph 5) of the
Article 17 of the Single Ordered Text of Law 28706, Law of Transparency and Access to Public Information, constitutes sensitive data in accordance with the scope of this Law.(*)

Ninth. Unaffected powers of the tax administration The provisions of this Law should not
be interpreted to the detriment of the powers of the tax administration with respect to the information it has and requires for its records, or for the fulfillment of its functions.

Tenth. Financing The carrying
out of the actions necessary for the application of this Law is carried out with charge to the institutional budget of the Ministry of Justice specifications and the resources referred to in article 36, without demanding additional resources from the Public Treasury.

Twelfth. Validity of the Law This Law
comes into force in accordance with the following:

1. The provisions provided for in Title II, in the first paragraph of article 32 and in the first, second, third, fourth, ninth and tenth final complementary provisions apply from the day following the publication of this Law.

2. The other provisions take effect within a period of thirty business days, counted from the publication of the regulations of this Law.

Please inform the President of the Republic for its promulgation.

In Lima, on the twenty-first day of June, two thousand and eleven.

CÉSAR ZUMAETA FLORES
President of the Congress of the Republic

ALDA LAZO RIVERS OF HORNUNG
Second Vice President of the Congress of the Republic

TO THE CONSTITUTIONAL PRESIDENT
OF THE REPUBLIC

THEREFORE:

I order it to be published and fulfilled.

Given at the Government House, in Lima, to the
two days of the month of July of the year two thousand and eleven.

ALAN GARCIA PEREZ
Constitutional President of the Republic

ROSARIO DEL PILAR FERNÁNDEZ FIGUEROA
President of the Council of Ministers and
Minister of Justice

REGULATION OF LAW Nº 29733 PROTECTION LAW PERSONAL INFORMATION

SUPREME DECREE Nº 003-2013-JUS

THE PRESIDENT OF THE REPUBLIC

CONSIDERING:

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

That, Law No. 29733, Law of Protection of Personal Data, has the purpose of guaranteeing the fundamental right to the protection of personal data, provided for in the Political Constitution of the Peru;

That, article 32 of the limited Law No. 29733, provides that the Ministry of Justice and Rights Human Rights assumes the National Authority of Personal data protection;

That, the First Complementary Provision Final of Law No. 29733, provided for the establishment of a Multisectoral Commission, chaired by the National Data Protection Authority Personal, for the preparation of the corresponding Regulation;

That, the Multisectorial Commission formed by Supreme Resolution No. 180-2011-PCM has prepared the draft Regulation of Law No. 29733, Data Protection Law Personal, which has been pre-published in accordance with law, receiving contributions from citizens and the community in general;

That, in this sense, it is appropriate to approve the Regulation of Law No. 29733, Personal Data Protection Law;

In accordance with the provisions of the Law No. 29733, Personal Data Protection Law; Law No. 29158, Organic Law of the Executive Branch; and Law No. 29809, Law of Organization and Functions of the Ministry of Justice and Human Rights;

DECREE:

Article 1.- Approval

Approve the Regulation of Law No. 29733, Personal Data Protection Law, which consists of VI Titles, one hundred and thirty-one (131) Articles, three (03) Final Complementary Provisions and three (03) Transitory Complementary Provisions, which is part member of this Supreme Decree.

Article 2.- Publication

This Supreme Decree and the Regulation of Law No. 29733, Personal Data Protection Law, approved by the preceding article, must be published on the Institutional Portal of the Ministry of Justice and Human Rights (www.minjus.gob.pe).

Article 3.- Validity

The approved Regulation will come into force within thirty (30) business days from the day following the publication of this Supreme Decree in the Official Gazette El Peruano.

Article 4.- Endorsement

This Supreme Decree will be endorsed by the Minister of Justice and Human Rights.

Given at the Government House, in Lima, on the twenty-first day of March of the year two thousand thirteen.

OLLANTA HUMALA TASSO
Constitutional President of the Republic

EDA A. RIVAS FRANCHINI
Minister of Justice and Human Rights

REGULATION OF LAW Nº 29733 PROTECTION LAW PERSONAL INFORMATION

Index

Title I General disposition.

Title II Guiding principles.

Title III Processing of personal data.

Chapter I Consent.
Chapter II Limitations on consent.

Chapter III Transfer of personal data.

Chapter IV Special processing of personal data.

Chapter V Security measures.

Title IV Rights of the owner of personal data.

Chapter I General provisions.
Chapter II Special provisions.
Chapter III Guardianship procedure.

Title V National Protection Registry of Personal Data.

Chapter I General provisions.
Chapter II Registration procedure.
Chapter III Registration procedure codes of conduct.

Title VI Infringements and sanctions.

Chapter I Inspection procedure.
Chapter II Sanctioning procedure.

Chapter III Sanctions.

Final Complementary Provisions and Transient

TITLE I

General disposition

Article 1.- Object.

The purpose of this regulation is to develop Law No. 29733, Personal Data Protection Law, hereinafter the 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. Its provisions constitute rules of public order and mandatory compliance.

Article 2.- Definitions.

For the purposes of applying this regulation, without prejudice to the definitions contained in the Law, the following definitions are additionally understood:

1. Non-automated personal data bank: Non-computerized data set of natural persons structured according to specific criteria, which allows access without disproportionate efforts to personal data, whether centralized, decentralized or distributed functionally or geographically.

2. Blocking: It is the measure by which the person in charge of the personal data bank prevents third parties from accessing the data and these cannot be processed during the period in which any request for updating, inclusion, rectification is being processed. or suppression, in accordance with the provisions of the third paragraph of article 20 of the Law.

It is also provided as a prior step to cancellation for the time necessary to determine possible responsibilities in relation to the treatments, during the legal or contractually prescribed period of prescription.

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

4. Personal data: It is that numerical, alphabetical, graphic, photographic, acoustic information, about personal habits, or any other type concerning natural persons that identifies them or makes them identifiable through means that can be reasonably used.

5. Personal data related to health: This is information concerning the past, present or predicted health, physical or mental, of a person, including the degree of disability and their genetic information.

6. Sensitive data: This is information related to personal data referring to physical, moral or emotional characteristics, facts or circumstances of your emotional or family life, personal habits that correspond to the most intimate sphere, information related to physical health. or mental or other similar things that affect your privacy.

7. Days: Business days.

8. General Directorate of Personal Data Protection: It is the body in charge of exercising the National Authority for the Protection of Personal Data referred to in article 32 of the Law, and any of said names may be used interchangeably.

9. Issuer or exporter of personal data: It is the owner of the personal data bank or the person responsible for the processing located in Peru who carries out, in accordance with the provisions of this regulation, a transfer of personal data to another country.

10. Processor: This is the person who processes the personal data, and may be the owner of the personal data bank or the person in charge of the personal data bank or another person on behalf of the owner of the personal data bank by virtue of a legal relationship that links you to it and delimits the scope of your action. It includes the person who processes personal data by order of the person responsible for the processing when this is carried out without the existence of a personal data bank.

11. Receiver or importer of personal data: Any natural or legal person under private law, including branches, subsidiaries, affiliates or similar; or public entities, which receives the data in the event of international transfer, either as the owner or manager of the personal data bank, or as a third party.

12. Rectification: It is that generic action intended to affect or modify a personal data bank, either to update it, include information in it or specifically rectify its content with exact data.

13. Repertoire of jurisprudence: It is the bank of judicial or administrative resolutions that are organized as a source of consultation and intended for public knowledge.

14. Data controller: It is the one who decides on the processing of personal data, even when it is not found in a personal data bank.

15. Third party: Any natural person, legal entity under private law or public entity, other than the owner of personal data, the owner or person in charge of the personal data bank and the person responsible for the processing, including those who process the data under the direct authority of those.

The reference to “third party” made in article 30 of the Law constitutes an exception to the meaning provided for in this section.

Article 3.- Scope of application.

This regulation applies to the processing of personal data contained in a personal data bank or intended to be contained in personal data banks.

In accordance with the provisions of paragraph 6 of article 2 of the Political Constitution of Peru and article 3 of the Law, this regulation will apply to all types of personal data processing, whether carried out by natural persons, public entities or institutions. from the private sector and regardless of the support in which they are found.

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 such regimes apply from the scope of application of the Law and this regulation.

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

Article 4.- Exceptions to the scope of application.

The provisions of this regulation will not apply to:

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

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

2.1 National defense.
2.2 Public safety and,
2.3 The development of activities in criminal matters for the investigation and suppression of crime.

Article 5.- Territorial scope of application.

The provisions of the Law and this regulation are applicable to the processing of personal data when:

1. Be carried out in an establishment located in Peruvian territory corresponding to the owner of the personal data bank or whoever is responsible for the treatment.

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

3. The owner of the personal data bank or whoever is responsible for the treatment is not established in Peruvian territory, but Peruvian legislation is applicable to him, by contractual provision or international law; and

4. The owner of the personal data bank or whoever is responsible is not established in Peruvian territory, but uses means located in said territory, unless such means are used only for transit purposes that do not involve processing.

For these purposes, the person responsible must provide the means that are necessary for the effective fulfillment of the obligations imposed by the Law and these regulations and will designate a representative or implement sufficient mechanisms to be able to comply effectively, in Peruvian territory. , with the obligations imposed by Peruvian legislation.

When the owner of the personal data bank or whoever is responsible for the treatment does not is established in Peruvian territory, but the person in charge of the treatment is, the provisions relating to the security measures contained in this regulation will be applicable to the latter.

In the case of natural persons, the establishment will be understood as the premises where the main seat of their business is located, or the one they use to carry out their activities or their domicile.

In the case of legal entities, the establishment will be understood as the location where the main administration of the business is located.
If these are legal entities residing abroad, it will be understood that it is the location where the main administration of the business is located in Peruvian territory, or failing that, the one they designate, or any stable facility that allows the effective or real exercise. of an activity.

If it is not possible to establish the address of the domicile or establishment, you will be considered to have an unknown domicile in Peruvian territory.

TITLE II

Guiding principles

Article 6.- Guiding principles.

The owner of the personal data bank, or, where applicable, whoever is responsible for the treatment, must comply with the guiding principles of the protection of personal data, in accordance with the provisions of the Law, applying the development criteria established in the present title of the regulation.

Article 7.- Principle of consent.

In accordance with the principle of consent, the processing of personal data is lawful when the owner of the personal data has given free, prior, express, informed and unequivocal consent. Forms of consent in which this is not expressed directly are not admitted, such as those in which it is required to presume, or assume the existence of a will that has not been expressed. Even the consent given with other statements must be expressed expressly and clearly.

Article 8.- Principle of purpose.

In accordance with the principle of purpose, a purpose is considered to be determined when it has been expressed clearly, without room for confusion and when the purpose of the processing of personal data is objectively specified.

In the case of a personal data bank that contains sensitive data, its creation can only be justified if its purpose, in addition to being legitimate, is specific and in accordance with the explicit activities or purposes of the owner of the personal data bank.

Professionals who process any personal data, in addition to being limited by the purpose of their services, are obliged to maintain professional secrecy.

Article 9.- Quality principle.

In accordance with the principle of quality, the data contained in a personal data bank,

They must adjust precisely to reality. It is presumed that the data directly provided by the owner is accurate.

Article 10.- Security principle.
In attention to the principle of security, in the processing of personal data, the security measures that are necessary must be adopted in order to avoid any treatment contrary to the Law or this regulation, including adulteration, loss, deviations. of information, intentional or not, whether the risks come from human action or the technical means used.

TITLE III

Processing of personal data

Chapter I

Consent

Article 11.- General provisions on consent for the processing of personal data.

The owner of the personal data bank or whoever is responsible for the treatment, must obtain consent for the processing of personal data, in accordance with the provisions of the Law and this regulation, except for the cases established in article 14 of the Law, whose section 1) includes the processing of personal data that is essential to execute interoperability between public entities.

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 collected; as well as the other conditions that occur in the treatment or treatments, without prejudice to the provisions of the following article on the characteristics of consent.

When consent is requested for a form of processing that includes or may include the national or international transfer of data, the owner of the data must be informed so that they are unequivocally aware of such circumstance, in addition to the purpose to which their data will be used. data and the type of activity carried out by the person who will receive it.

Article 12.- Characteristics of the consent.
In addition to the provisions of article 18 of the Law and the preceding article of this regulation, obtaining consent must to be:

1. Free: Without error, bad faith, violence or fraud that could affect the expression of will of the owner of the personal data.

The delivery of gifts or the granting of benefits to the owner of personal data on the occasion of his consent does not affect the condition of freedom he has to grant it, except In the case of minors, in cases where their consent is admitted, consent given through gifts or benefits will not be considered free.

The conditioning of the provision of a service, or the warning or threat to deny access to benefits or services that normally have unrestricted access, does affect the freedom of the person who grants consent for the processing of their personal data, if the data requested They are not essential for the provision of benefits or services.

2. Prior: Prior to the collection of the data or, where applicable, prior to processing other than that for which it was already collected.

3. Express and Unequivocal: When the consent has been expressed in conditions that do not admit doubts of its granting.

It is considered that express consent was given verbally when the holder expresses it orally in person or through the use of any technology that allows oral dialogue.

Written consent is considered to be that which is granted by the owner through a document with his or her handwritten signature, fingerprint or any other mechanism authorized by the legal system that remains or can be printed on a paper or similar surface.

The express condition is not limited to verbal or written manifestation.
In a restrictive sense and always in accordance with the provisions of article 7 of this regulation, express consent will be considered to be that which is manifested through the conduct of the owner that shows that he has unequivocally consented, given that otherwise his conduct would necessarily have been another.

In the case of the digital environment, the manifestation consisting of “clicking”, “clicking” or “pinch”, “tapping”, “touch” or “pad” or other similar actions is also considered express.

In this context, written consent may be granted by electronic signature, by writing that is recorded, in such a way that it can be read and printed, or that by any other established mechanism or procedure allows the owner to be identified and consent obtained, through text. written. It may also be granted through pre-established text, easily visible, legible and in simple language, which the owner can make his own, or not, through a written, graphic response or by clicking or clicking.

The mere conduct of expressing will in any of the ways regulated in this section does not eliminate, nor does it fulfill, the other requirements of consent referring to freedom, opportunity and information.

4. Informed: When the owner of the personal data is clearly, expressly and undoubtedly communicated, in simple language, at least of the following:

to. The identity and address or address of the owner of the personal data bank or the person responsible for the treatment to whom you can contact to revoke consent or exercise your rights.

b. The purpose or purposes of the treatment of
that your data will be submitted.
c. The identity of those who are or may be its recipients, if applicable.
d. The existence of the personal data bank
in which they will be stored, when applicable.
and. The mandatory or optional nature of your responses to the questionnaire proposed, when applicable.

F. The consequences of providing your personal data and your refusal to do so.
g. Where applicable, the national and international transfer of data that is carried out.

Article 13.- Privacy policies.
The publication of privacy policies, in accordance with the provisions of the second paragraph of article 18 of the Law, must be understood as a form of compliance with the duty of information that does not exempt from the requirement of obtaining the consent of the owner of the personal data.

Article 14.- Consent and sensitive data.

In the case of sensitive data, consent must be granted in writing, through a handwritten signature, digital signature or any other authentication mechanism that guarantees the unequivocal will of the owner.

Article 15.- Consent and burden of proof.

For the purposes of demonstrating that consent has been obtained in the terms established in the Law and in these regulations, the burden of proof will fall in all cases on the owner of the personal data bank or whoever is responsible for the treatment.

Article 16.- Denial, revocation and scope of consent.

The owner of the personal data may revoke his or her consent to the processing of his or her personal data at any time, without prior justification and without retroactive effects.

For the revocation of consent, the same requirements observed on the occasion of its granting will be met, and these may be simpler, if so indicated on such occasion.

The owner of the personal data may deny or revoke his consent to the processing of his personal data for purposes additional to those that give rise to his authorized processing, without affecting the relationship that gives rise to the consent that he has granted or has not revoked. . In the event of revocation, it is the obligation of the person processing the personal data to adapt the new treatments to the revocation.

and the treatments that were in the process of being carried out, within the period resulting from diligent action, which may not be longer than five (5) days.
If the revocation affects the entire processing of personal data that was being carried out, the owner or person in charge of the personal data bank, or, where applicable, the person responsible for the processing, will apply the rules for cancellation or deletion of personal data.

The owner of the personal data bank or whoever is responsible for the treatment must establish easily accessible and unconditional, simple, fast and free mechanisms to make the revocation effective.

Chapter II

Limitations on consent

Article 17.- Sources accessible to the public.
For the purposes of article 2, paragraph 9) of the Law, the following will be considered sources accessible to the public, regardless of whether access requires compensation:

1. The means of electronic, optical and other technological communication, provided that the place where the personal data is located is designed to provide information to the public and is open to general consultation.

2. Telephone directories, regardless of the medium in 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 regulation.
4. Social media.
5. Lists of people belonging to professional groups that contain only the data of name, title, profession, activity, academic degree, postal address, telephone number, fax number, email address and those that establish their membership in the group.

In the case of professional associations, the following data of their members may also be indicated: membership number, date of incorporation and union status in relation to professional practice.

6. The repertoires of jurisprudence, duly anonymized.

7. Public Registries administered by the National Superintendency of Public Registries - SUNARP, as well as any other registry or data bank qualified as public in accordance with law.
8. Public Administration entities, in relation to the information that must be delivered in application of Law No. 27806, Law of Transparency and Access to Public Information.

The provisions of the preceding paragraph do not mean that all personal data contained in information managed by entities subject to the Law on Transparency and Access to Public Information is considered accessible public information. The evaluation of access to personal data held by public administration entities will be carried out taking into account the circumstances of each specific case.

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 18.- General provisions.
The transfer of personal data involves the communication of personal data inside or outside

of the national territory made to a person other than the owner of the personal data, the person in charge of the personal data bank or the person in charge of the processing of personal data.

The transfer of personal data outside the national territory is called cross-border flow of personal data.

The person to whom the personal data is transferred is obliged, by the mere fact of the transfer, to comply with the provisions of the Law and these regulations.

Article 19.- Conditions for transfer.

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

Article 20.- Proof of compliance with the transfer obligations.

For the purposes of demonstrating that the transfer was carried out in accordance with the provisions of the Law and these regulations, the burden of proof will fall, in all cases, on the data issuer.

Article 21.- Transfer within a sector or business group and code of conduct.

In the case of transfers of personal data within business groups, subsidiary companies affiliated or linked under the common control of the same group of the owner of the personal data bank or responsible for the treatment, or to those affiliated or linked to a parent company or any company of the same group as the owner of the data bank or data controller, the processing of personal data is guaranteed if there is a code of conduct that establishes the internal rules for the protection of personal data with the content provided for in article 31 of the Law, and registered as provided for in articles 89 to 97 of these regulations.

Article 22.- Recipient of personal data.

The recipient of the personal data assumes the status of owner of the personal data bank or data controller as referred to in the Law and this regulation, and must process the personal data in compliance with the provisions of the information that the issuer gave prior consent obtained from the owner of the personal data.

Article 23.- Formalization of national transfers.

The transfer must be formalized through mechanisms that allow it to be demonstrated that the owner of the personal data bank or the person responsible for the treatment communicated to the receiving controller the conditions under which the owner of the personal data consented to the processing of the same.

Article 24.- Cross-border flow of personal data.

Cross-border flows of personal data will be possible when the recipient or importer of personal data assumes the same obligations that correspond to the owner of the personal data bank or data controller who, as issuer or exporter, transferred the personal data.

In accordance with article 15 of the Law, in addition to the cases provided for in the first and third paragraph of said article, the provisions of the second paragraph of the same do not apply when dealing with personal data that derive from a scientific or professional relationship of the owner and are necessary for its development or compliance.

Article 25.- Formalization of the cross-border flow of personal data.

For the purposes of the preceding article, the issuer or exporter may use 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 owner consented to the treatment of your personal information.

Article 26.- Participation of the General Directorate of Personal Data Protection regarding the cross-border flow of personal data.

The owners of the personal data bank or those responsible for the processing may request the opinion of the General Directorate of Personal Data Protection regarding whether the cross-border flow of personal data that they carry out or will carry out complies with the provisions of the Law and these regulations.

In any case, the cross-border flow of personal data will be brought to the attention of the General Directorate of Personal Data Protection, including the information required for the transfer of personal data and the registration of the data bank.

Chapter IV

Special processing of personal data

Article 27.- Data processing personal of minors.

For the processing of personal data of a minor, the consent of the holders of parental authority or guardians, as appropriate, will be required.

Article 28.- Exceptional consent.

The personal data of those over fourteen and under eighteen years of age may be processed with their consent, provided that the information provided has been expressed in a language understandable by them, except in cases where the law requires the assistance of the holders of parental authority or guardianship.

Under no circumstances may consent to the processing of personal data of minors be granted for them to access activities linked to goods or services that are restricted to adults.

Article 29.- Prohibition of collection.

In no case may data be collected from a minor that allows information to be obtained about the other members of his or her family group, such as data related to the professional activity of his or her parents, economic information, sociological data or any other, without consent. of the owners of such data.

The identity and address data of parents or guardians may only be collected for the purpose of obtaining the consent referred to in article 27 of these regulations.

Article 30.- Promotion of protection.

It is the obligation of all holders of personal data banks and especially public entities to collaborate with the promotion of knowledge of the right to the protection of personal data of children and adolescents, as well as the need for their processing to be carried out. with special responsibility and security.

Article 31.- Processing of personal data in the communications and telecommunications sector.

Operators of communications or telecommunications services have the responsibility of ensuring the confidentiality, security, appropriate use and integrity of the personal data they obtain from their subscribers and users, in the course of their commercial operations. In this sense, they may not process the aforementioned personal data for purposes other than those authorized by its owner, unless there is a court order or express legal mandate.

Article 32.- Confidentiality and security.

Communications or telecommunications operators must ensure the confidentiality, security and appropriate use of any personal data obtained as a result of their activity and will adopt technical, legal and organizational measures, in accordance with the provisions of the Law and these regulations, without prejudice. of the measures established in the regulations of the communications and telecommunications sector that do not oppose the provisions of the Law and these regulations.

Article 33.- Data processing by outsourced personal technological means.

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

For cases in which there is human intervention in the treatment, articles 37 and 38 apply.

The processing of personal data by outsourced technological means, whether complete or partial, may be contracted by the person responsible for the processing of personal data as long as its execution is guaranteed.

compliance with the provisions of the Law and these regulations.

Article 34.- Criteria to consider for the processing of personal data by outsourced technological means.

When processing personal data through outsourced technological means, the following must be considered as minimum services:

1. Inform with transparency of subcontracting that involves the information on which the service is provided.

2. Do not include conditions that authorize or allow the provider to assume ownership of the personal data banks processed in the outsourcing.

3. Guarantee confidentiality regarding the personal data on which the service is provided.

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

5. Guarantee the destruction or impossibility of accessing personal data after the service has been completed.

Article 35.- Mechanisms for the provision of personal data processing services through outsourced technological means.

The service provider must have the following mechanisms:

1. Make known the changes in your privacy policies or in the conditions of the service you provide to the person responsible for the treatment, to obtain consent if this would mean increasing your processing powers.

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

3. Establish and maintain adequate security measures to protect the personal data on which the service is provided.

4. Guarantee the deletion of personal data once the service provided to the controller has concluded and the latter 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 person responsible of this fact.

Article 36.- Provision of services or custom treatment.

For the purposes of the Law, the delivery of personal data from the owner of the personal data bank to the person in charge does not constitute a transfer of personal data.

The person in charge of the personal data bank is prohibited from transferring personal data for the provision of processing services to third parties, unless the owner of the personal data bank that commissioned the processing has authorized it and the owner of the personal data has provided consent, in the event that such consent is required in accordance with the Law.

The period for storing data will be two (2) years from the end of the last order made.

The provisions of this article will be applicable, where applicable, to the subcontracting of the provision of personal data processing services.

Article 37.- Treatment through subcontracting.

The processing of personal data may be carried out by a third party other than the person in charge of the processing, through an agreement or contract between these two.

In this case, prior authorization from the owner of the personal data bank or data controller will be required. Said authorization will also be understood to have been granted if it was provided for in the legal instrument through which the relationship between the person responsible for the treatment and the person in charge of it was formalized. The processing carried out by the subcontractor will be carried out in the name and on behalf of the data controller, but the burden of proving authorization falls on the data processor.

Article 38.- Responsibility of the subcontracted third party.

The subcontracted natural or legal person assumes the same obligations that are established for the data processor in the Law, this regulation and other applicable provisions. However, it will assume the obligations of the owner of the personal data bank or person in charge of processing when:

1. Allocate or use personal data for a purpose other than that authorized by the owner of the data bank or data controller; either

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

Capítulo V

Security measures

Article 39.- Security for the processing of digital information.

Computer systems that manage personal data banks must include in their operation:

1. Access control to personal data information including access management from a user's registration, management of said user's privileges, user identification to the system, including username-password, use of digital certificates, tokens, among others, and carry out a periodic verification of the assigned privileges, which must be defined through a documented procedure in order to guarantee their suitability.

2. Generate and maintain records that provide evidence about interactions with data logical, including for traceability purposes, information on user accounts with access to the system, login and logout times and relevant actions. These records must be legible, timely and have a disposal procedure, including the destination of the records, once they are no longer useful, their destruction, transfer, storage, among others.

Likewise, security measures related to authorized access to data must be established through identification and authentication procedures that guarantee the security of the processing of personal data.

Article 40.- Conservation, backup and recovery of personal data.

The environments in which information is processed, stored or transmitted must be implemented, with appropriate security controls, taking as reference the physical and environmental security recommendations recommended in the “NTP ISO/IEC 17799 EDI. Information Technology. Code of Good Practices for Information Security Management.” in the current edition.

Additionally, security backup mechanisms for the information in the personal database must be considered with a procedure that includes verification of the integrity of the data stored in the backup, including when appropriate, complete recovery in the event of an interruption or damage, guaranteeing the return to the state in which it was at the time the interruption or damage occurred.

Article 41.- 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 will only proceed with the authorization of the owner of the personal data bank and will be done using the means of transport authorized by the same, taking the necessary measures, including data encryption, digital signatures, information, verification checksums, among others, aimed at avoiding unauthorized access, loss or corruption during transit to its destination.

Article 42.- Non-automated documentation storage. of

Cabinets, filing cabinets or other elements in which non-automated documents with personal data are stored must be located in areas where access is protected with access doors equipped with opening systems using a key or other equivalent device. These areas must remain closed when access to the documents included in the data bank is not necessary.

If due to the characteristics of the premises available it is not possible to comply with the provisions

In the previous section, alternative measures will be adopted, in accordance with the directives of the General Directorate of Personal Data Protection.

Article 43. Copying or reproduction.

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

Discarded copies or reproductions must be destroyed so as to prevent access to the information contained therein or its subsequent recovery.

Article 44.- Access to documentation.

Access to documentation will be limited exclusively to authorized personnel.

Mechanisms will be established to identify the accesses made in the case of documents that can be used by multiple users.

Access by people not included in the previous paragraph must be properly recorded in accordance with the security directives issued by the General Directorate of Personal Data Protection.

Article 45.- Transfer of non-automated documentation.

Whenever the documentation contained in a data bank is physically transferred, measures must be adopted to prevent access or manipulation of the information being transferred.

Article 46.- Provision of services without access to personal data.

The person responsible or in charge of the information or processing will adopt appropriate measures to limit staff access to personal data, to the media that contains them or to the resources of the information system, to carry out work that does not involve data processing. personal.

In the case of outside personnel, the contract for the provision of services will expressly include the prohibition of access to personal data and the obligation of secrecy with respect to the data that the personnel may have known due to the provision of the service.

TITLE IV

Rights of the owner of personal data

Chapter I

General disposition

Article 47.- Personal character.

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

Article 48.- Exercise of the rights of the owner of personal data.

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

Article 49.- Legitimacy to exercise rights.

The exercise of the rights contained in the This title is made:

1. By the owner of personal data, proving their identity and presenting a copy of the National Identity Document or equivalent document.

The use of the digital signature in accordance with current regulations replaces the presentation of the 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 your National Identity Document or equivalent document, and the title that accredits representation.

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

4. If the procedure indicated in article 51 of these regulations is chosen, the accreditation of the identity of the owner will be subject to the provisions of said provision.

Article 50.- Application requirements.

The exercise of rights is carried out by means of a request addressed to the owner of the personal data bank or person responsible for the treatment, which will contain:

1. Names and surnames of the holder of the right and their accreditation, and, where appropriate, of his representative in accordance with the preceding article.
2. Specific request that gives rise to the request.
3. Address, or address that may be electronic, for the purposes of corresponding notifications.
4. Date and signature of the applicant.
5. Documents that support the request, if applicable.
6. Payment of the consideration, in the case of public entities as long as they have it provided for in their procedures dated prior to the validity of this regulation.

Article 51.- Public attention services.

When the owner of the personal data bank or data controller has services of any nature to serve its public or to exercise claims related to the service provided or products offered, it may also respond to requests for the exercise of the rights included. in this title through said services, provided that the deadlines are not longer than those established in this regulation.

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 responsible for the processing for the identification of the latter, provided that it is accredited, in accordance with the nature of the service. of the service or product offered.

Article 52.- Reception and correction of the request.

All submitted requests must be received, leaving a record of their receipt by the owner of the personal data bank or data controller. In the event that the request does not comply with the requirements indicated in the previous article, the owner of the personal data bank or person responsible for its processing, within a period of five (5) days, counted from the day following receipt of the request, formulates observations for non-compliance that cannot be resolved ex officio, inviting the owner to correct them within a maximum period of five (5) days.

If the indicated period has elapsed without the correction occurring, the application will be considered not submitted.

Public entities apply article 126 of Law No. 27444, Law of General Administrative Procedure, on observations to the documentation presented.

Article 53.- Facilities for the exercise of the right.

The owner of the personal data bank or data controller is obliged to establish a simple procedure for the exercise of rights. Without prejudice to the above and regardless of the means or mechanisms that the Law and this regulation establish for the exercise of the rights corresponding to the owner of personal data, the owner of the personal data bank or the person responsible for the treatment, may offer mechanisms that facilitate the exercise of such rights for the benefit of the owner of personal data.

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

The exercise by the owner of personal data of their rights before the privately administered personal data banks will be free of charge, except as established in special regulations on the matter. In no case will the exercise of these rights imply additional income for the owner of the personal data bank or responsible for the processing before which they are exercised.

No means may be established for the exercise of rights that involve charging an additional fee to the applicant or any other means that entails an excessive cost.

Article 54.- Form of the response.

The owner of the personal data bank or data controller must respond to the request in the manner and within the deadline established in the this regulation, regardless of whether or not personal data of the owner thereof appears in the personal data banks that it administers.

The response to the owner of personal data must refer only to those data that have been specifically indicated in their request and must be presented in a clear, legible, understandable and easily accessible manner.

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

It will be up to the owner of the personal data bank or data controller to prove compliance with the duty to respond, and must retain the means to do so. The above will be applicable, where appropriate, to prove the fulfillment of what is established in the second paragraph of article 20 of the Law.

Article 55.- Response deadlines.

1. The maximum response period of the owner of the personal data bank or data controller in response to the exercise of the right to information will be eight (08) days counted from the day following the presentation of the corresponding request.

2. The maximum period for the response of the owner of the personal data bank or data controller to the exercise of the right of access will be twenty (20) days counted from the day following the presentation of the request by the owner of personal data. .

If the request is upheld and the owner of the personal data bank or data controller does not include the requested information with their response, access will be effective within ten (10) days following said response.

3. In the case of the exercise of other rights such as those of rectification, cancellation or opposition, the maximum response period from the owner of the personal data bank or person responsible for the processing will be ten (10) days counted from the day following the presentation of the the corresponding request.

Article 56.- Requirement for additional information.

In the event that the information provided in the request is insufficient or erroneous in such a way that it does not allow attention, the owner of the personal data bank may request, within seven (7) days following receipt of the request, additional documentation from the owner of the database. personal data to serve it.

Within a period of ten (10) days of receiving the request, counted from the day after receipt thereof, the owner of personal data will attach the additional documentation that he or she deems pertinent to support his or her request. Otherwise, said request will be considered not submitted.

Article 57.- Extension of deadlines.

Except for the period established for the exercise of the right to information, the periods that

corresponding to the response or attention to other rights, may be extended only once, and for an equal period, at most, as long as the circumstances justify it.

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

Article 58.- Application of specific legislation.

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, they will be applicable as long as they offer equal or greater guarantees to the owner of the rights. personal data and do not contravene the provisions of the Law and these regulations.

Article 59.- Partial or total denial of the exercise of a right.

The totally or partially negative response by the owner of the personal data bank or the person responsible for the treatment to the request for a right of the owner of personal data must be duly justified and must indicate the right that the owner has to appeal to the General Directorate of Protection of Personal Data in the process of complaint, in the terms of article 24 of the Law and this regulation.

Chapter II

Special provisions

Article 60.- Right to information.

The owner of personal data has the right, upon access, to be provided with all the information indicated in article 18 of the Law and paragraph 4 of article 12 of these regulations.

The response will contain the details provided for in the articles cited in the previous paragraph, unless the owner has requested the information referring only to some of them.

The provisions established in articles 62 and 63 of these regulations will apply to the response to the exercise of the right to information, where applicable.

Article 61.- Right of access.

Without prejudice to what is stated in article 19 of the Law, the owner of the personal data has the right to obtain from the owner of the personal data bank or the person responsible for the treatment the information related to his or her personal data, as well as all the conditions and generalities. of their treatment.

Article 62.- Means for compliance with the right of access.

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, telephone, image or other means suitable for this purpose.

The owner of the personal data may choose through one or more of the following ways:

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 confidentiality, integrity 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 data controller.

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. Likewise, access must be in a language accessible to the average knowledge of the population, of the terms used. Without prejudice to which, in order to use the most ecological means of communication available in each case, the person responsible for the treatment may agree with the owner on the use of means of reproduction of the information other than those established in this regulation.

Article 63.- Content of the information.

The information that is made available to the owner of the personal data on the occasion of the exercise of the right of access must be extensive and include the entire record corresponding to the owner of the personal data, even when the request only includes one aspect of said data. The report may not reveal data belonging to third parties, even if they are linked to the interested party.

Article 64.- Update.

It is the right of the owner of personal data, in the process of rectification, to update those data that have been modified as of the date of exercise of the right.

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

Article 65.- Rectification.

It is the right of the owner of personal data to modify data that turns out to be inaccurate, erroneous or false.

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 66.- Inclusion.

It is the right of the owner of personal data that, in the process of rectification, their data be incorporated into a personal data bank, as well as that the missing information that makes it incomplete, omitted or eliminated is incorporated into the processing of their personal data in response to its relevance for said treatment.

The inclusion request must indicate what personal data it refers to, as well as the

incorporation that must be carried out in them, accompanying the documentation that supports the origin and well-founded interest for it.

Article 67.- Deletion or cancellation.

The owner of the personal data may request the deletion or cancellation of his or her personal data from a personal data bank when they are no longer necessary or relevant for the purpose for which they were collected, when the period established for their processing has expired. , when you have revoked your consent for the treatment and in other cases in which you are not being treated in accordance with the Law and these regulations.

The request for deletion or cancellation may refer to all the personal data of the owner contained in a personal data bank or only to some part of them.

Within the provisions of article 20 of the Law and paragraph 3) of article 2 of these regulations, the request for deletion implies the cessation of the processing of personal data by blocking them and their subsequent elimination.

Article 68.- Communication of the deletion or cancellation.

The owner of the personal data bank or data controller must document to the owner of the personal data that he or she has complied with the request and indicate the transfers of the deleted data, identifying who or who was transferred, as well as the communication of the corresponding deletion. .

Article 69.- Inadmissibility of deletion or cancellation.

The deletion will not apply when the personal data must be kept for historical, statistical or scientific reasons in accordance with the applicable legislation or, where appropriate, in the contractual relations between the person responsible and the owner of the personal data, which justify the treatment thereof.

Article 70.- Protection in case of denial of deletion or cancellation.

Whenever possible, depending on the nature of the reasons supporting the refusal provided for in the preceding paragraph, means of dissociation or anonymization must be used to continue the treatment.

Article 71.- Opposition.

The owner of personal data has the right not to have the processing of his or her personal data carried out or to stop processing it when he or she has not given his or her consent for its collection because it was taken from a publicly accessible source.

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

If the opposition is justified, the owner of the personal data bank or the person responsible for its processing must proceed to cease the processing that gave rise to the opposition.

Article 72.- Right to objective processing of personal data.

To guarantee the exercise of the right to objective treatment in accordance with the provisions of article 23 of the Law, when personal data is processed as part of a decision-making process without participation of the owner of the personal data, the owner of the bank of personal data or the person responsible for the treatment must inform you as soon as possible, without prejudice to what is regulated for the exercise of other rights in the Law and these regulations.

Chapter III

Guardianship procedure

Article 73.- Direct guardianship procedure.

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 person responsible for the treatment, according to the characteristics that are regulated in the preceding articles of this title.

The owner of the personal data bank or person responsible for the processing must respond, within the deadlines provided for in article 55 of this regulation, expressing what corresponds to each of the aspects of the request. If the deadline has elapsed without receiving a response, the applicant may consider his or her request denied.

The denial or unsatisfactory response enables the applicant to initiate the administrative procedure before the General Directorate of Personal Data Protection, in accordance with article 74 of this regulation.

Article 74. Trilateral guardianship procedure.

The administrative procedure for the protection of the rights regulated by the Law and these regulations is subject to the provisions of articles 219 to 228 of Law No. 27444, Law of General Administrative Procedure, insofar as it is applicable, and will be resolved by resolution of the General Director of Personal Data Protection. The only appeal for reconsideration is available against this resolution, which, once resolved, exhausts the administrative route.

To begin the administrative procedure referred to in this article, without prejudice to the general requirements provided for in this regulation, the owner of the personal data must submit with his or her request for protection:

1. 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.

2. The document containing the response of the owner of the personal data bank or person responsible

of the treatment that, in turn, contains the denial of your request or the response that you consider unsatisfactory, if you have received it.

The maximum period in which the request for protection of rights must be resolved will be thirty (30) days, counted from the day after receiving the response from the person complained about or from the expiration of the period to formulate it and may be extended up to a maximum of thirty (30).) additional days, taking into account the complexity of the case.

The order to carry out the inspection visit suspends the deadline set for resolution until the corresponding report is received.

Article 75.- Inspection visit.

To better resolve, the Supervision and Control Directorate may be ordered to carry out an inspection visit, which will be carried out in accordance with the provisions of articles 108 to 114 of these regulations, within five (5) days following receipt. the order.

TITLE V

National Registry of Protection of Personal information

Chapter I

General disposition

Article 76.- Registry registration.

The National Registry for the Protection of Personal Data is the storage unit intended to mainly contain information on personal data banks of public or private ownership 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 in the Law and these regulations.

Article 77.- Acts and documents that can be registered in the Registry.

They will be 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. The personal data banks of the public administration, with the exceptions provided for in the Law and these regulations.

2. Privately administered personal data banks, with the exception provided for in paragraph 1) of article 3 of the Law.

3. The codes of conduct referred to in article 31 of the Law.

4. The sanctions, precautionary or corrective measures imposed by the General Directorate of Personal Data Protection in accordance with the Law and these regulations.

5. Communications referring to the cross-border flow of personal data.

Any person can consult the information referred to in article 34 of the Law and any other information contained in the Registry.

Article 78.- Obligation to register.

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

Chapter II

Registration procedure

Article 79.- Requirements.

The owners of the personal data banks must register them in the National Registry for the Protection of Personal Data, providing the following information:

1. The name and location of the personal data bank, its purposes and intended uses.

2. The identification of the owner of the personal data bank, and, where applicable, the identification of the person in charge of the treatment.

3. Types of personal data subjected to processing in said bank.

4. Procedures for obtaining and the personal data processing system.

5. The technical description of the security measures.

6. Recipients of personal data transfers.

Article 80.- Models or forms.

The General Directorate of Personal Data Protection will publish by resolution the models or electronic forms of requests for the creation, modification or cancellation of personal data banks, which allow their presentation through telematic means or on paper, in accordance with the established procedure. in this regulation.

The models or electronic forms can be obtained free of charge on the Institutional Portal of the Ministry of Justice and Human Rights.

Article 81.- Start.

The procedure will begin with the presentation, before the Directorate of the National Registry of Personal Data Protection, of the request for the creation, modification or cancellation of the personal data bank formulated by its owner or duly accredited representative.

In the case of the registration application, it must contain the requirements demanded by this regulation; if any of the requirements are missing, the omission will be required to be corrected, in accordance with the provisions of the following article.

Likewise, in the case of the request for the modification or cancellation of a personal data bank, the registration code of the personal data bank in the National Registry for the Protection of Personal Data must be indicated.

In the application, a domicile or address must be declared, in order to send notifications related to the respective procedure.

Article 82.- Correction of defects and archiving.

If the application submitted does not comply with the requirements demanded by the regulations, the National Registry Directorate for the Protection of Personal Data will require the applicant to correct the omission within ten (10) days. Once the maximum period has expired, without the interested party having complied with correcting said omission, the application will be archived.

Article 83.- Registration resolution.

The Director of the Directorate of the National Registry for the Protection of Personal Data will issue the resolution providing for the registration of the personal data bank, provided that it complies with the requirements of the Law and these regulations.

The resolution must state:

1. The code assigned by the Registry.
2. Identification of the personal data bank.
3. The description of the purpose and intended uses.
4. The identification of the owner of the personal data bank.
5. The category of personal data it contains.
6. Obtaining procedures.
7. The personal data processing system and the indication of security measures.

Likewise, the identification of the data processor where the personal data bank is located and the recipients of the personal data and the cross-border flow will be included, where applicable.

Once the personal data bank has been registered in the National Data Protection Registry, the interested party will be notified of the decision.

The registration of a personal data bank in the National Data Protection Registry does not exempt the owner from compliance with the rest of the obligations provided for in the Law and these regulations.

Article 84.- Modification or cancellation of personal data banks.

The registration of a personal data bank must be kept updated at all times.

Any modification that affects the content of the registration must be previously communicated to the National Registry Directorate for the Protection of Personal Data for registration.

When the owner of a personal data bank decides to cancel it, he must notify the National Registry Directorate for the Protection of Personal Data, so that the registration can be canceled. The applicant will specify the destination that will be given to the data or the provisions for its destruction.

Article 85.- Duration of the procedure.

The maximum period to issue the resolution regarding registration, modification or cancellation will be thirty (30) days.

If no express resolution has been issued within said period, the personal data bank will be deemed to have been registered, modified or cancelled, for all purposes.

Article 86.- Inadmissibility or denial of registration.

The Director of the National Data Protection Registry Directorate will issue a resolution denying registration when the application does not comply with the requirements set forth in the Law and in this regulation or other provisions issued by the General Directorate of Personal Data Protection in accordance with the legal powers conferred.

The resolution must be duly motivated, with express indication of the causes that prevent registration, modification or cancellation.

Article 87.- Challenge.

Reconsideration and appeals are filed against the resolution that denies registration, in accordance with the procedure indicated in Law No. 27444, General Administrative Procedure Law.

Article 88.- The instances.

The Directorate of the National Registry for the Protection of Personal Data constitutes the first instance for the purposes of addressing administrative appeals filed against the denial of registration of a personal data bank. It will resolve appeals for reconsideration and will submit appeals to the General Directorate of Personal Data Protection, which will decide as a final administrative instance on the admissibility or inadmissibility of the registration.

Chapter III

Registration procedure for codes of conduct

Article 89.- Scope of application of the codes of conduct.

1. The codes of conduct will be voluntary.

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.

3. The codes of conduct promoted by a company or business group must refer to all the treatments carried out by them.

Article 90.- Content.

1. Codes of conduct must be written in clear and accessible terms.

2. The codes of conduct must be appropriate to what is established in the Law and include at least the following aspects:

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

2.2. The specific provisions for the application of the principles of personal data protection.

23. The establishment of homogeneous standards for compliance by those adhered to the code of the obligations established in the Law.

2.4. The establishment of procedures that facilitate the exercise by those affected of their rights to information, access, rectification, cancellation and opposition.

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

2.6. Promotion and dissemination actions regarding the protection of personal data aimed at those who process them, especially regarding their relationship with those affected.

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

3. In particular, the code must include:

3.1 Clauses for obtaining the consent of the owners of personal data to the processing or transfer of their personal data.

3.2 Clauses to inform the owners of personal data about the processing, when the data is not obtained from them.

3.3 Models for the exercise by those affected of their rights to information, access, rectification, cancellation and opposition.

3.4 If applicable, model clauses for compliance with the formal requirements for hiring a data processor.

Article 91.- Start of the procedure.

The procedure for registration of codes of conduct in the National Registry for the Protection of Personal Data will always be initiated at the request of the entity, body or association promoting the code of conduct.

The application, in addition to meeting the legally established requirements, will meet the following additional requirements:

1. Accreditation of the representation with which count the person submitting the application.

2. Content of the agreement, agreement or decision that approves in the corresponding area the content of the code of conduct presented.

3. In the event that the code of conduct comes from a sectoral agreement or a company decision, the certification referring to the adoption of the agreement and legitimation of the body that adopted it and a copy of the statutes of the association, sectoral organization or entity within whose framework the code has been approved.

4. In the case of codes of conduct presented by associations or organizations of a sectorial, documentation relating to its representativeness in the sector will be attached.

5. In the case of codes of conduct based on company decisions, a description of the treatments to which it refers will be attached.

Article 92.- Correction of defects.

Once the substantive aspects of the code of conduct have been analyzed, if it is necessary to provide new documents or modify its content, the National Registry Directorate for the Protection of Personal Data will require the applicant to make the necessary modifications within a period of ten (10) days.

Article 93.- Procedure.

After the period indicated in the previous article, the Directorate of the National Registry for the Protection of Personal Data will prepare a report on the characteristics of the draft code of conduct that will be sent to the Directorate of Regulations and Legal Assistance, so that it can report within the period of seven (07) days if it complies with the requirements of the Law and these regulations.

Article 94.- Issuance of the resolution.

Once the provisions of the preceding articles have been fulfilled, the Director of the Directorate of the National Registry for the Protection of Personal Data will issue the resolution providing for the registration of the code of conduct, provided that it complies with the requirements set forth in the Law and these regulations.

Article 95.- Duration of the procedure.

The maximum period to issue the resolution will be thirty (30) days, counted from the date of submission of the request to the National Registry Directorate for the Protection of Personal Data. If the resolution has not been issued within said period, the applicant may consider his or her application approved.

Article 96.- Inadmissibility or denial of registration.

The refusal to register the code of conduct will be resolved by resolution of the Director of the Directorate of the National Registry for the Protection of Personal Data, when said request does not comply with the requirements established in the Law, this regulation and those provisions issued by the General Directorate of Protection of Personal Data, within the framework of its legal powers. and statutory.

The resolution that denies registration is subject to reconsideration and appeal, in accordance with the procedure indicated in articles 87 and 88 of these regulations.

Article 97.- Advertising

The National Registry for the Protection of Personal Data will publicize the content of the codes of conduct using electronic or telematic means.

TITLE VI

Infringements and sanctions

Chapter I

Inspection procedure

Article 98.- Object.

The purpose of the inspection procedure will be to determine whether the circumstances exist that justify the initiation of the sanctioning procedure, with identification of the owner of the personal data bank or the person responsible for the treatment and the alleged commission of acts contrary to the Law and this regulation.

Article 99.- Beginning of the inspection procedure.

The inspection procedure begins always ex officio as a consequence of:

1. Direct initiative of the Supervision and Control Directorate or the General Director of Personal Data Protection.

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

In both cases, the Supervision and Control Directorate will require the owner of the personal data bank, the person in charge or whoever is responsible, for information related to the processing of personal data or the necessary documentation. In the case of inspection visits to the headquarters of public or private entities where the personal data banks they manage are located, the inspectors will have access to them.

Procedure 100.- Redirection of the article.

In the event that the complaint submitted can be perceived as not addressing the objectives of an inspection procedure, but rather those of the protection of rights, it will be referred to the corresponding procedure.

Article 101.- Public faith.

In the exercise of oversight functions, the personnel of the Supervision and Control Directorate will be equipped with public faith to verify the veracity of the facts in relation to the procedures under their charge.

Article 102.- Complaint requirements.

The complaint must indicate the following:

1. Name of the complainant and address for the purposes of receiving notifications.

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

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

Article 103.- Form of the complaint.

The complaint may be presented in physical format or according to the automated standard formats, which are displayed on the Institutional Portal of the Ministry of Justice and Human Rights.

When the complaint is submitted by electronic means through the system established by the General Directorate of Personal Data Protection, it will be understood that it is accepted that the notifications are made by said system or through other electronic means generated by it, unless indicated. a different medium.

Article 104.- Information requirement.

When a complaint is made, the Supervision and Control Directorate may request the documentation it deems appropriate from the complainant for the development of the procedure.

Article 105.- Development of the inspection.

The inspection procedure will have a maximum duration of ninety (90) days, this period runs from the date on which the Supervision and Control Directorate receives the complaint or initiates the procedure ex officio and will conclude with the report that will rule on the existence of elements that support or do not support the alleged commission of infractions provided for in the Law.

The established period may be extended once and for up to a period of forty-five (45) days, by reasoned decision, taking into account the complexity of the matter audited and with the knowledge of the General Director of Personal Data Protection.

Article 106.- Visiting program.

The inspection may include various visits to obtain the necessary elements of conviction, which will be carried out with a maximum period of ten (10) days between each one. After the first visit, a visit schedule will be notified to the owner of the personal data bank or to the person in charge or responsible for the treatment and, where appropriate, to the complainant.

Article 107.- Identification of inspection personnel.

At the beginning of the visit, the inspection staff must show a valid credential with a photograph, issued by the General Directorate of Personal Data Protection that accredits them as such.

Article 108.- Inspection visits.

The personnel who carry out the inspection visits must be provided with a reasoned written order with the official's handwritten signature, of which they will leave a copy, at a charge, to the person who attended the visit.

The order must specify the place or places where the public or private entity or the natural person to be inspected is located, or where the personal data banks subject to inspection are located, the generic purpose of the visit and the legal provisions. that substantiate it.

Article 109. Inspection minutes.

Inspection visits require the preparation of the corresponding minutes, which will record the actions carried out.

during the verification visit. Said minutes will be drawn up in the presence of two witnesses proposed by the person with whom the procedure was understood.
If they have refused to propose them or those proposed have not participated, the signature of the person with whom the diligence was understood or proof of their refusal to sign, if applicable, will suffice.

The minutes will be prepared in duplicate and will be signed by the audit staff and those who have participated in the procedure. The minutes may include the statement that the participants consider appropriate to their rights.

One of the originals of the inspection report will be delivered to the auditee, the other being incorporated into the proceedings.

Article 110.- Content of the inspection records.

The inspection records will state:

1. Name, name or company name of the person being audited.

2. Time, day, month and year in which it begins and conclude the audit.

3. The 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 in which the place where the inspection was carried out is located, as well as such as the telephone number or other form of communication available with the auditee.

4. Number and date of the inspection order that motivated it.

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

6. Name and address of the people who participated as witnesses.

7. Data and details related to the performance.

8. Statement from the auditee if requested.

9. Name and signature of those who participated in the inspection, including those who carried it out. If the person inspected, his legal representative or the person who assisted the inspector refuses to sign, this will not affect the validity of the record, and the inspecting personnel must state the respective reason.

The signature of the auditee will not imply his agreement with the content, but only his participation and receipt of it.

Article 111.- Obstruction of inspection.

If the auditee directly refuses to collaborate or observes obstructive behavior, unjustifiably delaying his collaboration, raising unreasonable questions about the inspection work, disregarding the instructions of the inspectors or any other similar or equivalent conduct, it will be recorded in the minutes, with precision of the obstructive act or acts and their systematic nature, if applicable.

Article 112.- Observations during the inspection or later.

Without prejudice to the fact that those audited may make observations in the act of inspection and express what is appropriate to their right in relation to the facts contained in the minutes, also They may do so in writing within a period of five (5) days following the date on which it was lifted.

Article 113.- Report.

The inspection procedure will conclude with the report issued by the Supervision and Control Directorate, in which it will preliminarily determine the circumstances that justify the establishment of the sanctioning procedure or the absence of them.

If this is the case, the measures that must be ordered to the presumed responsible will be established, in a precautionary manner. The instruction of the sanctioning procedure will be carried out in accordance with the provisions of the Law and these regulations.

The determination of the alleged responsibility for acts contrary to what is established in the Law and these regulations contained in the Report, will be notified to the auditee and the complainant, if applicable, within a period that will not exceed five (5) days.

Article 114.- Inadmissibility of means of challenge.

No appeal may be filed against the inspection report issued by the Supervision and Control Directorate; the contradiction of its content and any form of defense regarding it will be asserted in the sanctioning procedure, if applicable.

Chapter II

Sanctioning procedure

Article 115.- Authorities of the sanctioning procedure.

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

1. The Director of the Sanctions Directorate is the authority that instructs and resolves, in the first instance, on the existence of an infraction and imposition or not of sanctions and on accessory obligations aimed at the protection of personal data. Likewise, it is competent to conduct and develop the investigation phase, and is responsible for carrying out the necessary actions to determine the circumstances of the commission, or not, of acts contrary to what is established in the Law and these regulations.

2. The General Director of Personal Data Protection resolves the sanctioning procedure in the second and last instance and his decision exhausts the administrative route.

Article 116.- Beginning of the sanctioning procedure.

The sanctioning procedure will always be promoted ex officio, in response to a report from the Supervision and Control Directorate that may respond to a complaint or a reasoned decision of the Director General of Personal Data Protection.

Article 117. Liminar rejection.

The Sanctions Directorate may, by means of an express and reasoned resolution, decide to file cases that do not merit the initiation of the sanctioning procedure, despite the report of the Supervision and Control Directorate.

The complainant may appeal against this decision.

Article 118.- Precautionary and corrective measures.

Once the sanctioning procedure has begun, the Sanctions Directorate may order, through a reasoned act, the adoption of provisional measures that ensure the effectiveness of the final resolution that may fall in the aforementioned procedure, in compliance with the applicable rules of the Law. No. 27444, General Administrative Procedure Law.

Likewise, without prejudice to the administrative sanction that corresponds to a violation of the provisions contained in the Law and these regulations, corrective measures may be issued, when possible, aimed at eliminating, avoiding or stopping the effects of the violations.

Article 119.- Content of the resolution initiation of the sanctioning procedure.

1. The Sanctions Directorate notifies the resolution to initiate the sanctioning procedure that will contain:

2. The identification of the authority that issues the notification.

3. The indication of the corresponding file and the mention of the inspection report, if it is the case.

4. Identification of the public entity or private to whom the procedure is opened.

5. The decision to open sanctioning proceedings.

6. The account of the background that motivates the initiation of the sanctioning procedure, which includes the manifestation of the facts that are attributed to the administrator and the classification of the infractions that such facts may constitute.

7. The sanction or sanctions, which, if applicable, could be imposed.

8. The deadline to present defenses and evidence.

Article 120.- Presentation of defenses and evidence.

The administrator, within a maximum period of fifteen (15) days, counted from the day following the corresponding notification, will present his defense, in which he may make a specific statement regarding each of the facts that are expressly attributed to him, affirming them, denying them, pointing out that they are ignored because they are not their own or exposing how they occurred, as the case may be. Likewise, you may present the arguments by which you refute the presumed infringement and the corresponding evidence.

If expert or testimonial evidence is offered, the facts will be specified and the names and addresses of the expert will be indicated. or of the witnesses, displaying the respective questionnaire or interrogation in preparation for them. Without these requirements, said tests will be considered not offered.

Article 121.- Actions for the investigation of the facts.

Once the period of fifteen (15) days for the presentation of the defense has expired, with or without it, the Sanctions Directorate will carry out ex officio all the necessary actions to examine the facts and may arrange an inspection visit by the Directorate. of Supervision and Control, if it has not been done before, in order to collect the information that is necessary or relevant to determine, where appropriate, the existence of infractions susceptible to sanction.

Article 122.- Closing of investigation and term of the sanctioning procedure.

Once the investigative actions are concluded, the Sanctions Directorate will issue a resolution closing the investigative stage within fifty (50) days from the beginning of the procedure.

Within twenty (20) days after notification of the resolution to close the investigative stage, the Sanctions Directorate must resolve in the first instance.

An oral report may be requested within five (5) days following notification of the resolution to close the instructional stage.

When there is justified cause, the Sanctions Directorate may extend, once and for up to an equal period, the period of fifty (50) days referred to in this article.

The resolution that resolves the sanctioning procedure will be notified to all parties involved in the procedure.

Article 123.- Challenge.

Appeals for reconsideration or appeal may be filed against the resolution that resolves the sanctioning procedure within fifteen (15) days of notification of the resolution to the administrator.

The appeal for reconsideration will be supported by new evidence and will be resolved by the Sanctions Directorate within a period that will not exceed thirty (30) days.

The appeal will be resolved by the General Director of Personal Data Protection, and must be addressed to the same authority that issued the act that is challenged, so that it can elevate the action. The appeal must be resolved within a period of no more than thirty (30) days.

Chapter III

Sanctions

Article 124.- Determination of the sanction administrative fine.

The fines are determined based on the Tax Unit in force on the date on which the infraction was committed and when it is not possible to establish such date, the one that was in force on the date on which the General Directorate of Personal Data Protection detected the infraction. .

Article 125.- Graduation of the amount of the administrative sanction of fine.

To graduate the sanction to be imposed, the principle of reasonableness of the sanctioning power recognized in paragraph 3 of article 230 of Law No. 27444, Law of General Administrative Procedure, as well as the condition of the sanctioned repeat offender and the procedural conduct of the offender, must be observed.

In the event that the infractions continue, after having been sanctioned, a greater sanction than the one previously imposed must be imposed in accordance with the terms established in paragraph 7 of article 230 of Law No. 27444, Law of General Administrative Procedure.

Article 126.- Mitigating agents.

Collaboration with the actions of the authority and the spontaneous recognition of infractions accompanied by amending actions will be considered mitigating factors. Taking into account the opportunity of recognition and the amendment formulas, the mitigation will even allow the reasoned reduction of the sanction below the range provided for in the Law.

Article 127.- Default in the payment of fines.

The administrator who does not make the timely payment of the fines incurs automatic default, consequently the amount of the unpaid fines will accrue default interest that will be applied daily from the day following the expiration date of the fine cancellation period until the date of payment inclusive, multiplying the amount of the unpaid fine by the current daily Default Interest Rate (TIM). The current daily Default Interest Rate (TIM) results from dividing the current Default Interest Rate (TIM) by thirty (30).

Article 128.- Incentives for paying the fine.

It will be considered that the sanctioned person has complied with paying the fine if, before the expiration of the period granted to pay the fine, he deposits sixty percent (60%) of the amount in the bank account determined by the General Directorate of Personal Data Protection. its amount. For said benefit to take effect, you must communicate this fact to the General Directorate of Personal Data Protection, attaching proof of the corresponding bank deposit. After this period, payment will only be accepted for the entire fine imposed.

Article 129.- Execution of the fine sanction.

The execution of the fine sanction is governed by the law of the matter referring to the coercive execution procedure.

Article 130.- Registry of sanctions, precautionary and corrective measures.

The Directorate of the National Registry for the Protection of Personal Data will be in charge of the Registry of Those Sanctioned for Noncompliance with the Law and this regulation, the Registry of Measures Precautionary Measures and the Registry of Corrective Measures, which will be published on the Institutional Portal of the Ministry of Justice and Human Rights.

Article 131.- Application of coercive fines

In case of non-compliance with accessory obligations to the fine imposed for violation of the Law and these regulations, the Sanctions Directorate may impose coercive fines according to the following grading:

1. For non-compliance with accessory obligations to the fine imposed for minor infractions, the coercive fine will be from zero points two to two Tax Tax Units (0.2 to 2 UIT).

2. For non-compliance with accessory obligations to the fine imposed for serious infractions, the coercive fine will be two to six Tax Tax Units (2 to 6 UIT).

3. For non-compliance with accessory obligations to the fine imposed for very serious infractions, the coercive fine will be six to ten Tax Tax Units (6 to 10 UIT).

"Chapter IV

Violations

Article 132.- Violations

Violations of Law No. 29733, Personal Data Protection Law, or its Regulations are classified as minor, serious and very serious and are punishable with a fine in accordance with article 39 of the aforementioned Law.

1. They are minor infractions

a) Process personal data in breach of the security measures established in the regulations on the matter.

b) Collect personal data that is not necessary, relevant or appropriate in relation to the specific, explicit and lawful purposes for which it needs to be obtained.

c) Not modify or rectify the personal data being processed when it is known to be inaccurate or incomplete.

d) Do not delete the personal data being processed when they are no longer necessary, relevant or appropriate for the purpose for which they were collected or when the period for their processing has expired. In these cases, the infringement is not established when the anonymization or dissociation procedure is carried out.

e) Failure to register or update in the National Registry the acts established in article 34 of the Law.

f) Process personal data in violation of the provisions of the Law and its Regulations.

2. These are serious infractions:

a) Not addressing, preventing or hindering the exercise of the rights of the owner of personal data of

in accordance with the provisions of Title III of Law No. 29733 and its Regulations.

b) Process personal data without the free, express, unequivocal, prior and informed consent of the owner, when it is necessary in accordance with the provisions of Law No. 29733 and its Regulations.

c) Process sensitive personal data in breach of the security measures established in the regulations on the matter.

d) Collect sensitive personal data that is not necessary, relevant or appropriate in relation to the specific, explicit and lawful purposes for which it needs to be obtained.

e) Use lawfully obtained personal data for purposes other than those for which it was collected, unless anonymization or dissociation procedure is involved.

f) Obstruct the exercise of the Authority's supervisory function.

g) Breach the obligation of confidentiality established in article 17 of Law No. 29733.

h) Failure to register or update in the National Registry the acts established in article 34 of Law No. 29733, despite having been required to do so by the Authority within the framework of a sanctioning procedure.

3. They are very serious infractions:

a) Process personal data in contravention of the obligations contained in Law No. 29733 and its Regulations, when this prevents or attacks the exercise of other fundamental rights.

b) Collect personal data through fraudulent, unfair or illicit means.

c) Provide false documents or information to the Authority.

d) Not cease the improper processing of personal data when there is a prior request from the Authority as a result of a sanctioning procedure or a trilateral protection procedure.

e) Failure to comply with the corrective measures established by the Authority as a result of a trilateral protection procedure.

Article 133.- Graduation in case of recidivism

In case of recidivism in the commission of two (02) minor infractions, in the same year, the third minor infraction is sanctioned as an infraction grave.

In the event of a repeat offense in the commission of two (02) serious infractions, in the same year, the third serious infraction is punished as a very serious infraction." ***(*) Chapter IV incorporated by the Third Complementary Provision Modifying the Regulation of 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 management of interest, approved by Supreme Decree No. 019-2017-JUS, published on September 15, 2017.***

Final Complementary Provisions

First.- Interoperability between public entities.

The definition, scope and content of interoperability, referred to in the first paragraph of article 11 of this regulation, as well as the guidelines for its application and operation in accordance with the personal data protection regulations, are the responsibility of the National Office of Electronic Government and Information Technology - ONGEI of the Presidency of the Council of Ministers, in its capacity as Governing Body of the National Information Technology System. Interoperability between entities will be regulated in terms of its implementation within the framework of the provisions of section 76.2.2 of section 76.2 of article 76 of Law No. 27444, General Administrative Procedure Law.

Second.- Protection of personal data and competitiveness.

The powers established in this regulation are exercised by the National Authority for the Protection of Personal Data, in accordance with the country's competitiveness policies established by the corresponding entity.

Third.- Protection of personal data and social programs.

In accordance with the provisions of paragraph 12 of article 33 of the Law, the terms in which compliance with the Law and this Regulation must be agreed with the rules or policies of transparency and supervision that govern the administration of data banks linked to The Social Programs and the Household Targeting System will be developed by directive and in coordination with the Ministry of Development and Social Inclusion - MIDIS.

Transitional Complementary Provisions

First.- Adaptation of personal data banks.

Within a period of two (2) years from the entry into force of this regulation, the existing personal data banks must adapt to what is established by the Law and this regulation, without prejudice to the registration referred to in the Fifth Provision. Final Complementary Law No. 29733, Personal Data Protection Law.

Second.- Sanctioning power.

The sanctioning power of the General Directorate of Personal Data Protection, in relation to the personal data banks existing on the date of entry into force of this regulation, is suspended until the expiration of the adaptation period established in the First Transitory Complementary Provision. .

Third.- Formats.

The General Directorate of Data Protection Personales will create the standard formats necessary for the processing of the procedures regulated in these regulations within a period that will not exceed sixty (60) days from the entry into force of these regulations.