of the National Superintendence of Migrations - MIGRACIONES, since their participation will help, among other aspects, to share knowledge in order to make the movement of people between the two countries more viable; That, the expenses for land tickets and per diem will be assumed by the Executing Unit 001: General Office of Administration of Sheet 007, Ministry of the Interior; That, the penultimate paragraph of numeral 10.1 of article 10 of Law No. 29951, Public Sector Budget Law for Fiscal Year 2013 establishes, with respect to trips abroad by public servants or officials and representatives of the State charged to public resources , that the requirement of additional exceptions to those indicated in the literals of said numeral, in the case of entities of the Executive Branch, must be channeled through the Presidency of the Council of Ministers and is authorized by supreme resolution endorsed by the President of the Council of Ministers;

With the approval of the General Advisory Office Legal Department of the Ministry of the Interior; Y,

In accordance with the provisions of Law No. 27619, Law that regulates the authorization of travel abroad for servers and officials and its Regulations approved by Supreme Decree No. 047-2002-PCM; the law No. 29951, Public Sector Budget Law for Fiscal Year 2013; Legislative Decree No. 1130 that creates the National Superintendence of Migrations – MIGRATION; Legislative Decree No. 1135, which approves the Law on the Organization and Functions of the Ministry of the Interior and the Regulations on the Organization and Functions of the Ministry of the Interior approved by Decree Supreme N° 002-2012-IN;

RESOLVED:

Article 1.- Authorize the trip abroad, in Commission of Services, of Miss Janneth Capacoila Grimaldos, Inspector of Migrations of the National Superintendence of Migrations - MIGRATION, from March 25 to 26, 2013, to the city of Copacabana - State Plurinational of Bolivia, to participate in the First Meeting of the Peru-Bolivia Highland Border Committee.

Article 2.- Expenses for travel expenses and land tickets caused by the trip referred to in the preceding article, will be charged to the Executing Unit 001: General Administration Office of Sheet 007, Ministry of the Interior, according to to the following detail:

Land Tickets: S/. 108.06 Travel expenses (for 2 days) : S/. 1,080.00

Article 3.- Within fifteen (15) calendar days of the trip, the designated servant must present a detailed report to the Sector Holder describing the actions carried out and the results obtained during the authorized trip; as well as duly documented accountability.

Article 4.- This Supreme Resolution will not give the right to exoneration or release of taxes of any kind or denomination.

Article 5.- This Supreme Resolution will be endorsed by the President of the Council of Ministers and by the Minister of the Interior.

Sign up, communicate and get published.

OLLANTA HUMALA TASSO
Constitutional President of the Republic

JUAN F. JIMÉNEZ MAYOR
President of the Council of Ministers

WILFREDO PEDRAZA SIERRA
Minister of the Interior

915560-3

JUSTICE AND RIGHTS HUMANS

Regulations of the Law are approved No. 29733, Data Protection Law personal

SUPREME DECREE
Nº 003-2013-JUS

THE PRESIDENT OF THE REPUBLIC

CONSIDERING:

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

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

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

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

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

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

In accordance with the provisions of Law No. 29733, Personal Data Protection Law; Law No. 29158, Organic Law of the Executive Power; and Law No. 29809, Law on 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 thirty-one (131) Articles, three (03) Final Complementary Provisions and three (03) Complementary Provisions Temporary, which forms an integral part 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 shall enter 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.- Countersignature This Supreme Decree will be countersigned by the Minister of Justice and Human Rights.

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

OLLANTA HUMALA TASSO
Constitutional President of the Republic

EDA A. RIVAS FRANCHINI
Minister of Justice and Human Rights

REGULATION OF LAW Nº 29733 PERSONAL DATA PROTECTION LAW

Index

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 these regulations, without prejudice to the definitions contained in the Law, in addition, the following definitions are understood:

1. **Non-automated personal data bank:** Non-computerized dataset of natural persons and 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-party access to the data and these cannot be processed, during the period in which any request for updating, inclusion, rectification is being processed. cation or deletion, in accordance with the provisions of the third paragraph of article 20 of the Law.
It is also provided as a step prior to cancellation for the time necessary to determine possible responsibilities in relation to the treatments, during the legal prescription period or contractually provided.

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

4. **Personal data:** It is that numerical, alphabetical, graphic, photographic, acoustic information, about personal habits, or of 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:** It is that 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:** It is that information related to personal data referring to the physical, moral or emotional characteristics, facts or circumstances of your affective or family life, personal habits that correspond to the most intimate sphere, information related to physical health or mental or other similar ones that affect your privacy.

7. **Days:** Business days.

8. **General Directorate for the Protection of Personal Data:** 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 denominations may be used indistinctly.

9. **Issuer or exporter of personal data:** It is the owner of the personal data bank or the person responsible for the treatment located in Peru that carries out, in accordance with the provisions of these regulations, a transfer of personal data to another country.

10. **Person in charge of the treatment:** It is the person who carries out the processing of 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 binds him to it and delimits the scope of his action. It includes whoever processes personal data by order of the person responsible for the treatment when it is carried out without the existence of a personal data bank.

11. **Recipient or importer of personal data:** It is any natural or legal person under private law, including branches, affiliates, 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 data.
exact.

13. **Directory 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. **Responsible for the treatment:** It is the one who decides on the processing of personal data, even when they are not in a personal data bank.

15. **Third party:** It is any natural person, legal person 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 data controller, 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 in this numeral.

Article 3.- Scope of application.
This regulation is applicable to the processing of personal data contained in a database

personal or intended to be contained in personal data banks.

In accordance with the provisions of numeral 6 of article 2 of the Political Constitution of Peru and article 3 of the Law, these regulations will apply to all modalities 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.

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

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

Article 4.- Exceptions to the scope of application.
The provisions of this regulation shall not apply to:

1. The processing of personal data carried out by natural persons for exclusively domestic, personal purposes or those related to their private or family life.
2. The contents or intended to be contained in personal data banks of the public administration, only as long as their treatment is necessary for strict compliance with the powers assigned by law to the respective public entities, provided that their purpose is:

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

Article 5.- Scope of territorial application.
The provisions of the Law and these regulations are applicable to the processing of personal data when:

1. It is 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 them, 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 solely for transit purposes that do not imply treatment.

For these purposes, the person in charge must provide the necessary means 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 the territory Peruvian, with the obligations imposed by Peruvian legislation.

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

In the case of natural persons, the establishment shall be understood as the place where the main seat of their businesses is located, or the one they use for the performance of their activities or their domicile.
In the case of legal persons, the establishment shall be understood as the premises where the main administration of the business is located. If it's about of legal persons residing abroad, it will be understood that it is the place 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, it will be considered with an unknown domicile in Peruvian territory.

TITLE II

guiding principles

Article 6.- Guiding principles.
The owner of the personal data bank, or where appropriate, 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.
Pursuant to the principle of consent, the processing of personal data is lawful when the owner of the personal data has given his free, prior, express, informed and unequivocal consent. Consent formulas in which it is not directly expressed 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 declarations must be stated expressly and clearly.

Article 8.- Principle of finality.
In attention to the principle of finality, it is considered that a finality is determined when it has been expressed clearly, without 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 activities or explicit purposes of the owner of the personal data bank.
The professionals who carry out the treatment of any personal data, in addition to being limited by the purpose of their services, are obliged to keep professional secrecy.

Article 9.- Principle of quality.
In attention to the principle of quality, the data contained in a personal data bank must accurately adjust to reality. It is presumed that the data directly provided by the owner thereof are 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 to these regulations, including adulteration, loss, deviations of information, intentional or not, whether the risks come from human action or from 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 treatment of personal data, in accordance with the provisions of the Law and these regulations, except in the cases established in article 14 of the Law, in which numeral 1) is included the treatment of personal data that

It 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 treatment 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 for which they will be used. your data and the type of activity carried out by the person who will receive them.

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

1. Free: Without error, bad faith, violence or fraud that may 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 the personal data on the occasion of their consent does not affect the condition of freedom they have to grant it, except in the case of minors, in the cases in which their consent is admitted. , in which the consent granted 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 are normally unrestricted access, does affect the freedom of the person who grants consent for the processing of their personal data, if the data requested are not essential for the provision of benefits or services.

2. Prior: Prior to the collection of the data or, where appropriate, prior to the treatment other than that for which they were already collected.

3. Express and Unequivocal: When the consent has been expressed in conditions that do not admit doubts about its granting.
It is considered that the express consent was given orally when the owner expresses it orally in person or through the use of any technology that allows oral communication.

Written consent is considered to be that granted by the owner through a document with his autograph 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 these regulations, 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, necessarily, it would have been another
In the case of the digital environment, the manifestation consisting of "clicking", "clicking" or "puncture", "touching", "touch" or "pad" or other similar is also considered express.
In this context, written consent may be granted by means of an 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 his consent obtained, through of written text. It may also be granted by pre-established text, easily visible, legible and in simple language, which the holder can endorse, or not, by means of a written or graphic response or by clicking or clicking.
The mere conduct of expressing will in any of the forms regulated in this numeral does not eliminate, nor does it fulfill, the other consent requirements related to freedom, opportunity and information.

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

a. The identity and domicile or address of the owner of the personal data bank or the data controller to whom you can contact to revoke consent or exercise your rights. b. The purpose or purposes of the treatment to which

your data will be submitted.
c. The identity of those who are or may be their 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 answers to the questionnaire that is proposed, when applicable.
F. The consequences of providing your data personal information and your refusal to do so.
g. Where appropriate, 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 to obtain 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 user. titular.

Article 15.- Consent and burden of proof.
For the purposes of demonstrating that consent was 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 the consent.
The owner of the personal data may revoke his consent for the processing of his 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 had been indicated on such occasion.

The owner of the personal data may deny or revoke their consent to the processing of their personal data for additional purposes to those that give rise to their authorized treatment, without affecting the relationship that gives rise to the consent that has been granted or has not been granted. revoked. In the event of revocation, it is the obligation of the person who processes 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 more 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 appropriate, the data controller, 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
Consent limitations

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

1. Electronic, optical and other technological means of 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 support in which they are available and under the terms of their specific regulation.
3. Newspapers and magazines regardless of the support in which they are available and under the terms of their specific regulation.
4. Social media.
5. The 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 information of their members may also be indicated: membership number, date of incorporation and union status in relation to professional practice.
6. The jurisprudence repertoires, duly anonymized.

7. The Public Registries managed by the National Superintendence of Public Registries - SUNARP, as well as any other registry or data bank qualified as public according to 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 numeral 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 made according to 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 these regulations.

Chapter III
Transfer of personal data

Article 18.- General provisions.
The transfer of personal data implies the communication of personal data within or outside 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.

Cross-border fl ow of personal data is the transfer of personal data outside the national territory.

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 the 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 transfer obligations.
In order to demonstrate that the transfer was made 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, affiliated or related subsidiary companies under the common control of the same group as the owner of the personal data bank or data controller, or those affiliated or linked to a parent company or any company of the same group as the owner of the data bank or responsible for the treatment, it is complied with guaranteeing the processing of personal data, if there is a code of conduct that establishes the internal regulations 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 personal data assumes the status of owner of the personal data bank or person responsible for the treatment in what refers to the Law and these regulations, and must carry out the treatment of personal data complying with the provisions of the information that the The issuer gave prior consent from the owner of the personal data.

Article 23.- Formalization of national transfers.

The transfer must be formalized through mechanisms that make it possible to demonstrate that the owner of the personal data bank or the person responsible for the treatment informed the receiving person of the conditions in which the owner of the personal data consented to the transfer. treatment of them.

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 thereof do not apply when dealing with personal data derived from a scientific or professional relationship. of the owner and are necessary for its development or compliance.

Article 25.- Formalization of the cross-border fl ow 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 for the Protection of Personal Data regarding the cross-border fl ow of personal data.
The owners of the personal data bank or those responsible for the treatment may request the opinion of the General Directorate for the Protection of Personal Data regarding whether the cross-border flow of personal data that it carries 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 for the Protection of Personal Data, 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.- Treatment of personal data of minors.

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

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

Article 29.- Prohibition of compilation.
In no case may it be collected from a minor

age data that allow obtaining information about the other members of your family group, such as data related to the professional activity of their parents, economic information, sociological data or any other, without the consent of the owners of such data.

The identity and address data of the 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 the owners of personal data banks and especially of public entities to collaborate with the promotion of knowledge of the right to protection of personal data of children and adolescents, as well as the need for their treatment to be carried out with special responsibility and security.

Article 31.- Processing of personal data in the communications and telecommunications sector.
The 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, except by court order or express legal mandate.

Article 32.- Confidentiality and security.
Communications or telecommunications operators must ensure the confidentiality, security and proper 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 to 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.- Treatment of personal data by outsourced technological means.
The processing of personal data by outsourced technological means, among which are services, applications, infrastructure, among others, refers to those in which the processing is automatic, without human intervention.

For cases in which the treatment exists
human intervention, 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 compliance with the provisions of the Law and these regulations is guaranteed for its execution.

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

When carrying out the processing of personal data by outsourced technological means, the following must be considered as minimum benefits:

1. Inform with transparency the subcontracting that involves the information about the one that provides the service.

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 the confidentiality of the personal data on which the service is provided.

4. Maintain control, decisions and responsibility over the process through which the processing of personal data is carried out.

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

Article 35.- Mechanisms for the provision of the personal data processing service by outsourced technological means.

The service provider must have the following mechanisms:

1. Make known the changes in its privacy policies or in the conditions of the service it provides to the data controller, to obtain consent if this means increasing its

processing powers.

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

3. Establish and maintain adequate security measures for the protection of personal data about those who provide the service.

4. Guarantee the deletion of personal data once the service provided to the person in charge has concluded and the latter has been able to recover them.

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

Article 36.- Provision of services or treatment on request.

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 to third parties the personal data subject to the provision of treatment services, unless the owner of the personal data bank that commissioned the treatment has authorized it and the owner of the personal data have given their consent, in the cases that such consent is required by law.

The term for the conservation of the data will be two (2) years counted from the end of the last order.
accomplished.
The provisions of this article will be applicable, as appropriate, to the subcontracting of the provision of personal data processing services.

Article 37.- Treatment through subcontracting.

The processing of personal data can be carried out by a third party other than the person in charge of the treatment, through an agreement or contract between these two.
For this case, prior authorization will be required from the owner of the personal data bank or data controller. Said authorization will also be understood as 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 the treatment was formalized. The treatment carried out by the subcontractor will be carried out in the name and on behalf of the data controller, but the burden of proving the authorization rests with 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 person in charge of the treatment in the Law, these regulations and other applicable provisions. However, it will assume the obligations of the owner of the personal data bank or person in charge of the treatment 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 when it is for the conservation of said data.

Capítulo V
Security measures

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

The computer systems that manage banks of
Personal data must include in its operation:

1. Control of access to personal data information including access management from the registration of a user, the management of said user's privileges, the identification of the user before the system, among which are user-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 logical data, including for traceability purposes, information on user accounts with access to the system, logon and logoff times, and relevant actions. These records must be legible, timely and have a disposition procedure, among which are 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 personal data processing.

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

The environments in which the information is processed, stored or transmitted must be implemented, with appropriate security controls, taking as a 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, the security backup mechanisms of the personal database information must be contemplated with a procedure that contemplates the verification of the integrity of the data stored in the backup, including when pertinent, the complete recovery in the event of an interruption. or damage, guaranteeing the return to the state it was in 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 it, taking the necessary measures, among which are data encryption, digital signatures, information, verification checksum, among others, intended to prevent unauthorized access, loss or corruption during transit to its destination.

Article 42.- Storage of non-automated documentation.

The cabinets, filing cabinets or other elements in which non-automated documents with personal data are stored must be in areas where access is protected with access doors equipped with key-opening systems or another equivalent device. Said areas must remain closed when access to the documents is not necessary.

included in the data bank.

If, due to the characteristics of the premises, it is not possible to comply with the provisions of the previous section, alternative measures will be adopted, in accordance with the directives of the General Directorate for the Protection of Personal Data.

Article 43. Copying or reproduction.

Copies or reproduction of documents may only be made under the control of authorized personnel.

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

Article 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.

The access of persons not included in the previous paragraph must be properly registered in accordance with the security directives issued by the General Directorate for the Protection of Personal Data.

Article 45.- Transfer of non-automated documentation.

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

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

The person in charge or in charge of the information or treatment will adopt the appropriate measures to limit the access of the personnel to personal data, to the supports that contain them or to the resources of the information system, for the performance of works that do not imply the treatment of data. personal.

In the case of external personnel, the contract for the provision of services will expressly include the prohibition of access to personal data and the obligation of secrecy regarding the data that the personnel could 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 treatment 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 any or some of the rights does not exclude the possibility of exercising any 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 this title is carried out:

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 empowered to exercise the right, attaching a copy of their National Identity Document or equivalent document, and the title that accredits the 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 a reliable record, in accordance with article 115 of Law No. 27444, General Administrative Procedure Law.

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 through a request addressed to the owner of the personal data bank or data controller, which will contain:

1. Names and surnames of the holder of the right and accreditation of the same, and in his case of his representative in accordance with the preceding article.
2. Specific request that gives rise to the request.
3. Address, or address that can be electronic, to effects of the corresponding notifications.
4. Date and signature of the applicant.
5. Documents that support the petition, if it is the case.
6. Payment of the consideration, in the case of public entities provided that they provide for it in their procedures dated prior to the validity of these regulations.

Article 51.- Customer service.
When the owner of the personal data bank or person responsible for the treatment has services of any nature for the attention to its public or the exercise of claims related to the service provided or products offered, it may also attend to the requests for the exercise of the rights included in this title through said services, provided that the terms are not greater 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 treatment for the identification of the former, provided that it is accredited, according to the nature of the provision of the service or product offered.

Article 52.- Reception and rectification of the petition.

All applications submitted 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 meet the requirements indicated in the previous article, the owner of the personal data bank or person responsible for its treatment, within a period of five (5) days, counted from the day after receipt of the request. request, formulates the observations for non-compliance that cannot be saved ex officio, inviting the owner to correct them within a maximum period of five (5) days.

After the specified period has elapsed without the rectification, the application will be deemed not submitted.
Public entities apply article 126 of Law No. 27444, General Administrative Procedure Law, regarding observations on 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.
Notwithstanding the foregoing and regardless of the means or mechanisms that the Law and these regulations 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 processing, 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 for the exercise of their rights before the public administration, the provisions of the first paragraph of article 26 of the Law will be followed.
The exercise by the owner of personal data of their rights before the personal data banks of private administration 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 person responsible for the treatment before which they are exercised.
None may be established as means for the exercise of rights that imply charging an additional fee to the applicant or any other means that involves an excessive cost.

Article 54.- Form of the response.
The owner of the personal data bank or person responsible for the treatment must respond to the request in the manner and within the period established in these regulations, regardless of whether or not the personal data of the owner of the same in the personal data banks that it manages.

The response to the personal data holder 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 it is necessary to use keys or codes, the corresponding meanings must be provided.

Proof of compliance with the duty to respond will correspond to the owner of the personal data bank or data controller, and must retain the means to do so. What is indicated will be applicable, in what is pertinent, to prove the realization 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 person responsible for the treatment when exercising the right to information will be eight (08) days from the day after the corresponding request is submitted.

2. The maximum term for the response of the owner of the personal data bank or person responsible for the treatment before the exercise of the right of access will be twenty (20) days counted from the day after the presentation of the request by the owner of personal data. .
If the request is accepted and the owner of the personal data bank or data controller does not include the requested information with his 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 of the owner of the personal data bank or person responsible for the treatment will be ten (10) days from the day after the presentation. of the corresponding application.

Article 56.- Requirement for additional information.

In the event that the information provided in the application is insufficient or erroneous in such a way that it does not allow its attention, the owner of the personal data bank may request, within seven (7) days following receipt of the application, additional documentation to the owner. of personal data to serve you.
Within ten (10) days of receiving the request, counted from the day after it is received, the owner of personal data will attach the additional documentation that he deems pertinent to support his request. Otherwise, said application will be considered as not submitted.

Article 57.- Extension of terms.
Except for the period established for the exercise of the right to information, the corresponding periods for the response or attention to the other rights, may be extended only once, and for an equal period, at the most, as long as the circumstances justify it. who.

The justification for the extension of the term must be communicated to the holder of the personal data within the term that is 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 apply as soon as they offer the same or greater guarantees to the owner of the data. personal data and do not contravene the provisions of the Law and these regulations.

Article 59.- Partial or total refusal before 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 before the request of a right of the owner of personal data, must be duly justified and must indicate the right that assists him to

appeal to the General Directorate for the Protection of Personal Data in the form of a claim, under the terms of article 24 of the Law and these regulations.

Chapter II
special provisions

Article 60.- Right to information.

The owner of personal data has the right, in access, to be provided with all the information indicated in article 18 of the Law and numeral 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 one of them.

The provisions of Articles 62 and 63 of this regulation will be applicable to the response to the exercise of the right to information, insofar as it is pertinent.

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 data controller the information regarding their 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 suitable means for this purpose.

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

1. Visualization on site.
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 receipt 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 to the nature of the treatment, established by the owner of the personal data bank or responsible for the treatment.

Whatever the method used, access must be in a clear, legible and intelligible format, without using passwords or codes that require mechanical devices for proper understanding and, where appropriate, accompanied by an explanation. Likewise, access must be in language accessible to the average knowledge of the population, of the terms used. Notwithstanding 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 the use of means of reproduction of the information other than those established in these regulations.

Article 63.- Content of the information.

The information made available to the owner of the personal data on the occasion of the exercise of the right of access must be comprehensive 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 when linked

with 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 on the date of exercise of the right.

The update request must indicate what 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 the data that turns out to be inaccurate, erroneous or false.

The request for rectification must indicate what 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 is incorporated into a personal data bank, as well as that the processing of their personal data incorporates that missing information that makes it incomplete, omitted or eliminated in attention to its relevance for said treatment.

The request for inclusion must indicate what personal data it refers to, as well as the incorporation that has to be made in them, accompanying the documentation that supports the origin and well-founded interest for it.

Article 67.- Suppression or cancellation.

The owner of the personal data may request the deletion or cancellation of their 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 data has expired. treatment, when you have revoked your consent for treatment and in other cases in which they 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 numeral 3) of article 2 of these regulations, the request for deletion implies the cessation of the processing of personal data from a blocking thereof and its subsequent elimination.

Article 68.- Communication of the deletion or cancellation.

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

Article 69.- Inadmissibility of the deletion or cancellation.

The deletion will not proceed when the personal data must be kept by virtue of historical, statistical or scientific reasons in accordance with the applicable legislation or, where appropriate, in the contractual relations between the person in charge and the owner of the personal data, which justifies who treat them.

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

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

Article 71.- Opposition.

The owner of personal data has the right not to carry out the processing of their personal data or to cease it, when they have not given their consent for its collection because they were taken from a source of public access.

Even if consent has been given, the owner of personal data has the right to oppose the processing of their data, if they prove the existence of well-founded and legitimate reasons related to a specific personal situation that justify the exercise of this right.

In the event that the opposition is justified, the owner of the personal data bank or person responsible for its treatment must proceed to cease the treatment that has given 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 the participation of the owner of the personal data, the owner of the personal data bank or data controller must inform him as soon as possible, without prejudice to what is regulated for the exercise of the 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 these regulations begins with the request that the owner of the personal data must direct 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 treatment must respond, within the periods provided in article 55 of these regulations, expressing what corresponds to each of the extremes of the request. Once the term has elapsed without having received the response, the applicant may consider his application denied.

The refusal or unsatisfactory response enables the applicant to initiate the administrative procedure before the General Directorate for the Protection of Personal Data, in accordance with article 74 of these regulations.

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 in what is applicable, and will be resolved by Resolution of the General Director of Personal Data Protection. Against this resolution, only an appeal for reconsideration is applicable, which, once resolved, exhausts the

administrative.

To initiate the administrative procedure referred to in this article, without prejudice to the general requirements set forth in these regulations, the owner of the personal data must submit with their guardianship request:

1. The charge for the request that you previously sent to the owner of the personal data bank or data controller to obtain from him, directly, the guardianship of
Your rights.

2. The document that contains the response from the owner of the personal data bank or data controller that, in turn, contains the refusal of your request or the response that you consider unsatisfactory, if received.

The maximum term in which the request for protection of rights must be resolved will be thirty (30) days, counted from the day after receipt of the response of the claimant or from the expiration of the term to formulate it and may be extended up to a maximum of thirty (30) additional days, depending on the complexity of the case.

The order to carry out the inspection visit suspends the period established to resolve until the corresponding report is received.

Article 75. Fi scaling visit.

To better resolve, the Supervision and Control Department 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 the five (5) days following the received the order.

TITLE V

National Registry of Personal Data Protection

Chapter I
General disposition

Article 76.- Registry registration.

The National Registry for the Protection of Personal Data is the storage unit for
It mainly contains 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 by the Law and these regulations.

Article 77.- Recordable acts and documents 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 in this title:

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

2. The personal data banks of private administration, with the exception provided for in numeral 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 for the Protection of Personal Data in accordance with the Law and these regulations.

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

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

Article 78.- Registration obligation.

Natural or legal persons from the private sector or public entities that create, modify or cancel personal data banks are obliged 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 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 data bank
personal information, its purposes and intended uses.

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

3. Types of personal data processed in said bank.

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

5. The technical description of the security measures.

6. The recipients of personal data transfers.

Article 80.- Models or forms.

The General Directorate for the Protection of Personal Data will publish by means of a resolution the models or electronic forms of the 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 procedure established in these regulations.

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 for the Protection of Personal Data, of the request for the creation, modification or cancellation of the personal data bank made by its owner or duly accredited representative.

In the case of the registration application, it must contain the requirements demanded by these regulations, 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 a 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 the notifications related to the respective procedure.

Article 82.- Correction of defects and archiving.

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

Article 83.- Resolution of registration.

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

The resolution must state:

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

Also, where appropriate, the identification of the person in charge of the treatment where the personal data bank is located and the recipients of the personal data and of the cross-border flow will be included.

Once the personal data bank is 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 holder from compliance with the rest of the obligations provided for in the Law and these regulations.

Article 84.- Modifi cation 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 Directorate of the National Registry for the Protection of Personal Data for registration.

When the owner of a personal data bank decides to cancel it, he must communicate it to the Directorate of the National Registry for the Protection of Personal Data, in order to proceed with the cancellation of the registration. The applicant will specify the destination that will be given to the data or the forecasts for its destruction.

Article 85.- Duration of the procedure.

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

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

Article 86.- Inadmissibility or refusal of registration.

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

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

Article 87.- Challenge.

Appeals and reconsideration resources proceed 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 the administrative appeals filed against the refusal to register a personal data bank. It will resolve the reconsideration resources and will submit the appeals to the General Directorate for the Protection of Personal Data, which will resolve in the last administrative instance the origin or inadmissibility of the registration.

Chapter III
Registration procedure for codes of conduct

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

1. Codes of conduct will be voluntary.

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

3. The codes of conduct promoted by a company or business group must refer to all the processing 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 adequate 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 subjected to it.

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

23. The establishment of homogeneous standards for compliance by those adhering 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, if applicable, are foreseen, indicating the guarantees that must be adopted.

2.6. Actions to promote and disseminate personal data protection aimed at those who process them, especially in terms of their relationship with those affected.

2.7. The supervision mechanisms through which compliance by adherents with what is established in 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 the personal data of the treatment, 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.- Beginning of the procedure.

The procedure for registration in the National Registry for the Protection of Personal Data of the codes of conduct will always begin at the request of

the entity, body or association that promotes 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 that the person submitting the application has.
2. Content of the agreement, agreement or decision by which the content of the code of conduct presented is approved in the corresponding area.
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 legitimacy of the body that adopted it and a copy of the statutes of the association, sectoral organization will be attached. 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 sectoral nature, documentation relating to their representativeness will be attached.
in the sector.
5. In the case of codes of conduct based on company decisions, a description of the processing to which it refers will be attached.

Article 92.- Rectification of defects.

Once the substantive aspects of the code of conduct have been analyzed, if the provision of new documents or the modification of its content is necessary, the Directorate of the National Registry for the Protection of Personal Data will require the applicant to carry out the necessary procedures within ten (10) days. required modifications.

Article 93.- Procedure.

Once the period indicated in the previous article has elapsed, 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 arranging for the registration of the code of conduct, provided that it meets the requirements of the Law and these regulations.

Article 95.- Duration of the procedure.

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

Article 96.- Inadmissibility or refusal of registration.

The denial of the registration of 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 meet the requirements set forth in the Law, these regulations and those provisions issued by the Directorate. General Protection of Personal Data, within the framework of its legal and statutory powers.

The reconsideration and appeal appeals may be filed against the resolution that denies registration, in accordance with the procedure indicated in articles 87 and 88 of these regulations.

Article 97.- Publicity 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 that justify the initiation of the disciplinary 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 these regulations.

Article 99.- Initiation of the inspection procedure.

The inspection procedure is always started
officio as a consequence of:

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

2. By denunciation of any public entity, natural or legal person.

In both cases, the Directorate of Supervision and Control will require the owner of the personal data bank, the person in charge or whoever is responsible, information regarding 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.

Article 100.- Renewal of the procedure.

In the event that, from the complaint presented, it can be perceived that it is not addressed to the objectives of an inspection procedure, but to those of the protection of rights, it will be referred to the corresponding procedure.

Article 101.- Public faith.

In the exercise of control functions, the staff of the Supervision and Control Directorate will be endowed 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 purposes
to receive the 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 appropriate, data for their location.

Article 103.- Form of the complaint.

The complaint may be submitted on physical support 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 for the Protection of Personal Data, 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 otherwise indicated. point a

different medium.

Article 104.- Request for information.

When a complaint is filed, the Supervision and Control Department 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 Department 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 not, the alleged commission of offenses provided for in the Law.

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

Article 106.- Program of visits.

The audit may include various visits to obtain the necessary elements of conviction, the

which will be developed within a maximum period of ten (10) days between each one. After the first visit, a program of visits will be notified to the owner of the personal data bank or to the person in charge or to the person in charge of the treatment and, where appropriate, to the complainant.

Article 107.- Identification of inspection personnel.

At the beginning of the visit, the supervisory personnel must display a valid credential with a photograph, issued by the General Directorate for the Protection of Personal Data that accredits it as such.

Article 108.- Inspection visits.

The personnel who carry out inspection visits must be provided with a reasoned written order with the official's autograph 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 audited is located, or where the personal data banks subject to audit are located, the generic purpose of the visit and the legal provisions that support it.

Article 109. Fi scalization Act.

Inspection visits require the drawing up of the corresponding minutes, in which there will be a record of the actions carried out during the verification visit. Said record will be drawn up in the presence of two witnesses proposed by the person with whom the procedure was understood. If he had refused to propose them or those proposed had not participated, the signature of the person with whom the diligence was understood or the record of his refusal to sign, if applicable.

The minutes will be drawn up in duplicate and will be signed by the supervisory personnel and those who have participated in the procedure. The minutes may include the statement that the participants consider appropriate to their right.

One of the originals of the audit report will be delivered to the auditee, incorporating the other to the proceedings.

Article 110.- Content of audit reports.

The audit records shall state:

1. Name, denomination or trade name of the supervised.
2. Time, day, month and year in which the fiscalization.
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. audit, as well 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 attended the inspectors.
6. Name and address of the persons who participated as witnesses.
7. Data and details related to the performance.
8. Statement of the inspected if requested.
9. Name and signature of those who participated in the inspection, including those who carried it out. If the auditee, his legal representative or the person who assisted the inspector refuses to sign, this will not affect the validity of the record, and the inspector 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 auditing.

If the inspected party directly refuses to collaborate or observes obstructive conduct, unreasonably delaying their collaboration, raising unreasonable questions about the inspection work, disregarding the indications of the inspectors or any other similar or equivalent conduct, a record shall be recorded in the minutes, with precision of the act or acts obstructive and of its systematic nature, if applicable.

Article 112.- Observations in the act of inspection or later.

Without prejudice to the fact that those inspected may make observations in the act of inspection and state what is appropriate to their right in relation to the facts contained in the record, they may also do so in writing within the term of five (5) days following the date on which it was raised.

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 disciplinary procedure or the absence of them.

If this is the case, the measures that must be ordered to the alleged perpetrator will be established, in a precautionary manner. The investigation of the disciplinary procedure will be carried out in accordance with the provisions of the Law and these regulations.

The determination of the presumed 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.

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

Chapter II
disciplinary procedure

Article 115.- Authorities of the disciplinary procedure.

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

1. The Director of the Sanctions Department 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 tending to 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 the acts contrary to what is established in the Law and these regulations.

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

Article 116.- Penalty. Start of the procedure

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

Article 117. Liminar rejection.

The Sanctions Directorate may, by means of an express and reasoned resolution, decide to archive cases that do not warrant the start of the sanctioning procedure, notwithstanding the report of the Supervision and Control Directorate. The complainant may appeal against this decision.

Article 118.- Precautionary and corrective measures.

Once the disciplinary procedure has begun, the Sanctions Department 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, with observance

of the applicable norms of Law No. 27444, Law of General Administrative Procedure.

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

Article 119.- Content of the decision to start the disciplinary procedure.

1. The Sanctions Department notifies the resolution of start of the disciplinary procedure that will contain:
2. The identification of the authority issuing the notification.

3. The indication of the corresponding file and the Mention of the inspection report, if applicable.
4. The identification of the public or private entity to whom proceedings are being opened.
5. The decision to open disciplinary proceedings.
6. The account of the antecedents that motivate the initiation of the disciplinary procedure, which includes the statement of the facts that are attributed to the company and the qualification of the infractions that such facts may constitute.

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

8. The term to present the disclaimers and evidence.

Article 120.- Presentation of defenses and evidence.

The administrator, within a maximum period of fifteen (15) days, counted from the day after the corresponding notification, will present his defense, in which he will be able to pronounce specifically regarding each of the facts that are expressly imputed to him, affirmed signing them, denying them, indicating that they ignore them because they are not their own or exposing how they occurred, as the case may be. Likewise, it may present the arguments by means of which it distorts the presumed infraction and the corresponding evidence.

In case expert or testimonial evidence is offered, the facts on which they will deal will be specified and the names and addresses of the expert or of the witnesses will be indicated, exhibiting the questionnaire or the respective interrogation in preparation of the same. Without these requirements, said tests will be considered as not offered.

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

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

Article 122. Closing of instruction and term of sanctioning procedure.

Once the instructive actions have been concluded, the Sanctions Department will issue a resolution closing the instructive stage within fifty (50) days from the start of the procedure.

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

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

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

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

Article 123.- Challenge.

Against the resolution that resolves the procedure reconsideration or appeal proceed within fifteen (15) days of notification of the resolution to the administrator.

The appeal for reconsideration will be based on new evidence and will be resolved by the Sanctions Department within a period not to exceed thirty (30) days.

The appeal will be resolved by the General Director of Personal Data Protection, and must address the same authority that issued the act that is challenged, to raise the action. The appeal must be resolved within a period not exceeding thirty (30) days.

Chapter III
sanctions

Article 124.- Determination of the sanction fine administration.

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 for the Protection of Personal Data detected the infraction. .

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

In order to graduate the sanction to be imposed, the principle of reasonableness of the sanctioning power recognized in numeral 3 of article 230 of Law No.
27444, Law of General Administrative Procedure, as well as the condition of penalized recidivist and the procedural conduct of the offender.

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

Article 126.- Mitigating factors.

The collaboration with the actions of the authority and the spontaneous recognition of the infractions accompanied by actions of amendment will be considered mitigating. Taking into account the timing of the recognition and the amendment formulas, the attenuation will even allow the motivated reduction of the sanction below the range provided for in the Law.

Article 127.- Delay in the payment of fines.

The company that 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 after the expiration date of the fine cancellation period until the date payment inclusive, multiplying the amount of the unpaid fine by the current daily Moratorium Interest Rate (TIM). The current daily Moratorium Interest Rate (TIM) results from dividing the current Moratorium Interest Rate (TIM) by thirty (30).

Article 128.- Incentives for the payment of the fine.

It will be considered that the sanctioned party has complied with paying the fine if, before expiration of the term granted to pay the fine, he deposits sixty percent (60%) of its amount. In order for said benefit to take effect, you must communicate this fact to the General Directorate for the Protection of Personal Data, attaching the corresponding bank deposit receipt.

After said term, payment will only be accepted for the full amount of the imposed fine.

Article 129.- Execution of the sanction of a fine.

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

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

The Directorate of the National Registry for the Protection of Personal Data will be in charge of the Registry of

The Registry of Precautionary Measures and the Registry of Corrective Measures, which will be published on the Institutional Portal of the Ministry of Justice and Human Rights, are penalized for non-compliance with the Law and these regulations.

Article 131.- Application of coercive fines In case of non-compliance with accessory obligations to the sanction of a fine imposed for violation of the Law and these regulations, the Sanctions Department may impose coercive fines according to the following graduation:

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

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

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

SUPPLEMENTARY PROVISIONS FINALS

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 Informatics - ONGEI of the Presidency of the Council of Ministers, in its capacity as Governing Entity of the National Information System. The interoperability between entities will be regulated in terms of its implementation within the framework of the provisions of numeral 76.2.2 of subsection 76.2 of article 76 of Law No. 27444, Law of General Administrative Procedure.

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 numeral 12 of article 33 of the Law, the terms in which compliance with the Law and this Regulation must be agreed with the norms or policies of transparency and auditing that govern the administration of the linked data banks with 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.

SUPPLEMENTARY PROVISIONS TRANSIENT

FIRST.- Adequacy of personal data banks.

Within two (2) years of the entry into force of these regulations, existing personal data banks must conform to the provisions of the Law and these regulations, without prejudice to the registration referred to in the Fifth Final Complementary Provision of Law No. 29733, Personal Data Protection Law.

SECOND.- Sanctioning power.
The sanctioning power of the General Directorate for the Protection of Personal Data, in relation to the existing personal data banks 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 for the Protection of Personal Data 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.

915561-3

They approve transfers of Notaries Public holders of various Districts Notaries, to temporarily fill vacant positions

MINISTERIAL RESOLUTION
Nº 0079-2013-JUS

Lima, March 21, 2013

SEEN: Report No. 051-2013-JUS/CN, of the President of the Council of Notaries, on the temporary transfer of the notary public Mercedes Eugenia Portugal Montejo, and;

CONSIDERING:

That, the Fifth Complementary Provision Transitory of Law No. 29933 – Law that modifies article 9 of Legislative Decree No. 1049, Decree Legislative of the Notariado, on the notarial positions in the territory of the Republic, establishes that the Ministry of Justice and Human Rights, in attention to the needs of the population, can order the temporary transfers of public notaries at the national level, when there are vacancies and until they are covered by virtue of the national public contest of merits referred to in the second transitory complementary provision of the aforementioned Law; and in case it is declared void, until the places are covered by the regular public contests;

That, through Supreme Decree No. 020-2012-JUS, the Regulations for the Temporary Transfer of Notaries at the national level were approved, in accordance with the Fifth Transitory Complementary Provision of Law No. 29933 referred to above, whose article 2, literal b) establishes that temporary transfers will be approved by Ministerial Resolution, indicating the transferred notary public, the district and province of origin, the district and province of destination; adding literal c) of the aforementioned article that in order for the temporary transfer to be completed, the written acceptance of the respective notary public must be obtained; delimiting in its literal e) that the notaries public temporarily transferred maintain a direct relationship with the College of Notaries of origin; That, numeral 6.1 of Directive No. 001-2013-JUS/CN on the "Rules and Procedures that regulate the Temporary Transfer of Notaries", approved by Ministerial Resolution No. 0063-2013-JUS, provides that the Ministry of Justice and Human Rights issues the Ministerial Resolution approving the temporary transfer of the notary public at the proposal of the President of the Council; Likewise, numeral 5.6 of the aforementioned Directive establishes that the Colleges of Notaries of destination of the temporarily transferred public notaries, must refrain from intervening, supervising, controlling or carrying out any action that hinders the regular exercise of the aforementioned public notary; That, through Report No. 035-2013-JUS/CN, of the President of the Council of Notaries, the priority of filling vacant positions through temporary transfer was determined, in response to the needs of the population, while they are carried out. the National Public Merit Contest for Admission to the Notarial Function or the regular Contest, constituting a total of eighteen (18) places, of which nine (09) correspond to the Notarial District of San Martín; That, by Ministerial Resolution No. 336-2004-JUS, of July 20, 2004, the lawyer was appointed