YEAR OF NATIONAL INTEGRATION AND RECOGNITION OF OUR DIVERSITY

El Peruano

OFFICIAL GAZETTE

FOUNDED IN 1825 BY EL LIBERTADOR SIMÓN BOLÍVAR

Saturday, September 22, 2012

[seal] REPUBLIC OF PERU

PERU | Ministry of Justice and Human Rights

DRAFT REGULATION OF LAW No. 29733 PERSONAL DATA PROTECTION LAW

September - 2012

SPECIAL SEPARATA

DRAFT REGULATION OF LAW No. 29733
PERSONAL DATA PROTECTION LAW

Index

TITLE I

General provisions

Article 1.- Object
This regulation has the object of developing Law No. 29733, Personal Data Protection Law, to guarantee the fundamental right to the protection of personal data, regulating a suitable processing, both by political entities and by private sector institutions. Its provisions constitute mandatory public policy rules.

Article 2.- Definitions
For the purposes of the application of this regulation, without prejudice to the definitions contained in Law No. 29733, Personal Data Protection Law, additionally, the following definitions are given.

1. **Non-automated personal database**: Series of non-computerized data of natural persons, structured according to specific criteria, allowing to access without disproportionate effort the personal data, whether centralized, decentralized or distributed functionally or geographically.

2. **Blocking**: Measure by which the processor of the database prevents the access of third parties to the data, and these may not be processed during the period of processing of any request for update, inclusion, rectification or elimination, pursuant to the third paragraph of article 20 of the Law.
   It is also provided as a preliminary step to cancellation, for the time necessary to determine possible responsibilities related to processing, during the term of legal limitation or as contractually provided.

3. **Cancellation**: Action or measure described in the Law as elimination, when referring to personal data, consisting of eliminating or suppressing the personal data of a database.

4. **Personal data:** Numerical, alphabetical, graphic, photographic, acoustic or any other time of information concerning natural persons that identifies them or makes them identifiable through means that may be reasonably used.

5. **Health-related personal data**: Information concerning past, present or predicted physical or mental health of a person, including the degree of disability and his genetic information.

6. **Sensitive data**: Information concerning personal data referring to physical, moral or emotional characteristics, facts or circumstances of the affective or family life, personal habits, information concerning the physical or mental health and others similar, that affect a person's privacy.

7. **Days**: Business days.

8. **General Department of Personal Data Protection**: Entity in charge of exercising the National Authority for Personal Data Protection referred to in article 32 of the Law, any of said names being used indistinctly.

9. **Issuer or exporter of personal data**: Holder of the database or the person responsible for processing, located in Peru, who makes a transfer of personal data to another country, pursuant to this regulation.

10. **Data processor**: Party processing the personal data, which may be the holder of the database or the processor of the database or another person by the order of the holder of the database, pursuant to a legal relationship that binds him to it, and delimits the scope of his action. Includes the party processing personal data by order of the processor of the database, when it is done in the absence of a database.

11. **Receiver or importer of personal data**: Any private natural or legal person, including the branches, affiliates, related or similar companies, or public entities, who receive the data in the event of international transfer, be it as holder or processor of the personal database, or as third party.

12. **Rectification**: Generic action intended to affect or modify a database, either by updating, including information in it, or specifically rectifying its content with correct data.

13. **Jurisprudence repertory**: Base of judicial or administrative resolutions organized as source of consultation and intended for public information.

14. **Data controller**: Party deciding on the processing of personal data, even when they are not in a database.

15. **Third party**: Any natural person, private or public legal person other than the subject of personal data, the holder or processor of the personal database, and of the data controller, including those who process data under their direct authority.

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

Article 3.- Scope of application.
This regulation applies to the processing of personal data contained in a personal database or intended to be contained in personal database. Pursuant to section 6 article 2 of the Political Constitution of Peru and article 3 of Law No. 29733, Personal Data Protection Law, this regulation will apply to any personal data processing modality, be it done by natural persons, public entities or private sector institutions, regardless of the medium on which the data is found.

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

The provisions of the previous paragraph do not imply the derogation or non-application of special rules, provided that their application does not impair the right to the protection of personal data.

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

1. Personal data processing done by natural persons exclusively for domestic personal purposes or related to their private or family life.

2. The contents or data intended to be contents in databases of the public administration, only if their processing is necessary for strict compliance with the competence assigned by law to the respective public entities, provided they have the following objects:

   2.1 National defense.

   2.2 Public safety and,

   2.3 Development of activities in criminal matters for the investigation and repression of crime.

Article 5.- Territorial scope of application.
The provisions of the Law and this regulation apply to the processing of personal data when:

1. It is done in an establishment located in Peruvian territory, corresponding to the holder of the database or the data controller.

2. It is done by a data processor, regardless of its location, in the name of a holder of the database established in Peruvian territory, or the data controller.

3. The holder of the database or the data controller is not established in Peruvian territory, but is subject to Peruvian legislation, by contractual or international law provision; and

4. The holder of the database or the controller is not established in Peruvian territory, but uses means located in said territory, except if such means are used only for transit purposes that do not imply processing.

For these purposes, the controller must provide the means necessary for actual performance of the obligations imposed by Law and this regulation and will designate a representative or will implement sufficient mechanisms to be able to comply effectively, in Peruvian territory, with the obligations imposed on it by Peruvian law.

When the holder of the database or the data controller are not established in Peruvian territory, but the data processor is, the latter will be subject to the provisions concerning the security measures contained in this regulation.

In the case of natural persons, the establishment will be understood as the premises where the main place of its business is located, or that used for the performance of its activities or its domicile.

In case of legal persons, it will be understood as the establishment the place where the main administration of the business is located. In case of legal persons residing abroad, it will be understood that it is the premises where the main administration of the business is located in Peruvian territory, or in the absence thereof that designated by them, or any stable installation that allows the actual or real performance of an activity.

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

TITLE II

Guiding principles

Article 6.- Guiding principles.
The holder of the database, or if applicable the data controller, must comply with the guiding principles of personal data protection, pursuant to the Law, applying the development criteria established in this title of the regulation.

Article 7.- Principle of consent.
Given the principle of consent, personal data processing is legal when the data subject gave his free, prior, express, informed and unequivocal consent. Formulas of consent are not permitted in which the consent is not expressed directly, as such in which it is necessary to presume or assume the existence of a will that was not expressed. Even the consent given with other declarations must be declared expressly and clearly.

Article 8.- Principle of purpose
Given the principle of purpose, it is considered that the purpose is determined when it was expressed clearly, without room for confusion and where the object of the personal data processing is specified in an objective manner.

In the case of personal databases that contain sensitive data, their creation may be justified only if their purpose, in addition to being legitimate, is concrete and in accordance with the explicit activities or purposes of the holder of the database.

The professionals who process a personal datum, in addition to being limited by the purpose of their services, are obligated to keep professional secrecy.

Article 9.- Principle of quality.
Given the principle of quality, the data contained in a database must precisely be in line with reality. It is presumed that the data directly provided by their subject are exact.

Article 10.- Principle of security.
Given the principle of security, in the processing of personal data it is necessary to adopt the security measures necessary to avoid any processing contrary to the Law or this regulation, including the adulteration, loss, distortion of information, intentional or not, be it that the risk originate from human action or from the technical means used.

TITLE III

Personal data processing

Chapter I

Consent

Article 11.- General provisions on consent for personal data processing.
The holder of the database or the data controller must obtain the consent for the processing of personal data according to the Law and this regulation, except in the events established in article 14 of the Law.

The request for consent must refer to a determined processing or series of processing, with express identification of the purpose or purposes for which the data are collected; as well as the other conditions occurring in the processing, without prejudice to the provisions of the following article on the characteristics of consent.

When the consent is requested for a form of processing that includes or may include the national or international transfer of the data, their subject must be informed so as to be unequivocally aware of such circumstance, in addition to the purpose for which his data are intended and the type of activity carried out by the party receiving them.

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

1. **Free:** Without error, bad faith, violence or fraud that may affect the declaration of will of the data subject.

   The delivery of gifts or the granting of benefits to the data subject in connection with his consent do not affect the condition of freedom he has to grant it, except in the case of minors, in the events that their consent is admitted, since the consent granted against gifts or benefits will not be considered free.

   The conditioning of the performance of a service, or the notice or warning of threat of denying access to benefits or services that normally have unrestricted access, if it affects the freedom of the person consenting to the processing of his data.

2. **Prior**: Before recompiling the data or if applicable prior to the processing other than that for which they were already recompiled.

3. **Express or Unequivocal**: When the consent has been declared under conditions that do not admit doubts about its granting.

   It is considered that the express consent was verbally given when the subject expresses it orally, while being present, or by the use of any technology that allows oral questioning.

   It is considered written consent that granted by the subject in a document with his autograph signature, fingerprint or any other mechanism authorized by the legal system, which remains or may be printed on a surface of paper or similar.

   The express condition is not limited to the verbal or written declaration.

   Restrictively, and always in agreement with article 7 of this regulation, express consent is considered that indicated by the conduct of the subject who shows that he has consented unequivocally, since otherwise his conduct would have necessarily been different.

   In case of digital environment, it is also considered express the declaration consisting of "clicking," or "tapping," or "touch" or "pad."

   In this context, written consent may be granted by electronic signature, by printed written document, so that it may be read and a printout made, or by any other mechanism or procedure established that may identify the subject and receive his consent, by a written text. It may also be granted by pre-established text, easily visible, legible and in simple language, which the subject may adopt or not, by a written or graphic answer or by click or tap.

   The only conduct of expressing the will in any of the forms regulated by this section does not eliminate or considers complied with the other requisites of consent referring to freedom, opportunity and information.

4. **Informed**: When the data subject is communicated clearly, expressly and undoubtedly, in a simple language, at least the following:

   a. The identity and domicile or address of the holder of the database or data controller which he may address to evoke the consent or exercise his rights.
   b. The purpose or purposes of the processing to which his data will be subject.
   c. The identity of those who are or may be his addressees, if applicable.
   d. The existence of databases in which they will be stored, when such is the case.
   e. The mandatory or optional character of his answers to the questionnaire offered to him, when applicable.
   f. The consequences of providing his personal data and his refusal to do so.
   g. If applicable, national and international transfer of data made.

Article 13.- Privacy policies.
The publication of privacy policies, as provided in the second paragraph of article 18 of the Law, must be understood as a form of complying with the duty of information, which does not exempt it from the requisite of obtaining the consent of the data subject.

Article 14.- Consent and sensitive data.
In the case of sensitive data, the consent must be granted in writing, by handwritten signature, digital signature or any other mechanism of authentication guaranteeing the unequivocal will of the subject.

Article 15.- Consent and burden of proof.
In order to demonstrate that the consent was obtained in the terms established in the Law and this regulation, the burden of proof will lie in all cases with the holder of the database or the data controller.

Article 16.- Denial, revocation and scope of consent.
The data subject may revoke his consent for the processing of his personal data at any time, without prior justification, and without attributing retroactive effects. For the revocation of consent, the same requisites observed in connection with its granting will be followed, but may be simpler, if so indicated in said opportunity.

The data subject may refuse or revoke his consent to the processing of his data for additional purposes to those that gave rise to the authorized processing, without affecting the relationship that leads to the consent granted or not revoked. In the event of revocation, it is the obligation of the data processor to adapt the new processing to the revocation and the processing that was about to be done, within the term resulting from his diligent action, which may not be longer than five (5) days.

If the revocation affects the entire data processing that was done, the holder or processor of the personal database, or if applicable, the data controller, will apply the rules for cancellation or elimination of personal data.

The holder of the database or the data controller must establish easily accessible and unconditional mechanisms, easy, quick and free of charge for the implementation of the revocation.

Chapter II

Limitations to consent

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

1. Electronic, optical or other technology communication means, provided that the place where the personal data are located is conceived to facilitate the information to the public and is open to general consultation.

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

3. Newspapers and magazines, regardless of the medium on which they are available and within the terms of their specific regulation.

4. Social communication media.

5. The lists of persons belonging to professional groups that contain only data concerning the name, title, profession, activity, academic degree, postal address, telephone number, fax number, email address and those establishing their belonging to the group.

   In the case of professional associations, it is possible to also indicate the following data of their members: membership number, data of incorporation and union situation concerning the practice of the profession.

6. Repertories of jurisprudence, duly anonymized.

7. The Public Registers administered by the National Superintendence of Public Registers – SUNARP, as well as any other register or database qualified as public according to the law.

8. Entities of the Public Administration, concerning the information that must be delivered pursuant to Law No. 27806, Law of Transparency and Access to Public Information.
   The provisions of the previous section do not mean that any personal data contained in information administered by the entities subject to the Law of Transparency and Access to Public Information is considered accessible public information. The evaluation of the access to personal data in possession of public administration entities will be done according to the circumstances of each concrete case.

The processing of data obtained from public access sources must respect the principles established in the Law and in this regulation.

Chapter III

Transfer of personal data

Article 18.- General provisions.
The transfer of data implies the communication of personal data in or out of the national territory done by a person other than the data subject, the processor of the database or the personal data controller.

Trans-border flow of personal data means the transfer of personal data outside the national territory.

The party to whom the personal data are transferred undertakes, by the mere fact of the transfer, to observe the provisions of the Law and this regulation.

Article 19.- Conditions for transfer.
Any transfer of personal data requires the consent of its subject, except for the exceptions provided in article 14 of the Law, and must be limited to the purpose that justifies it.

Article 20.- Proof of obligation with the obligations in matters of transfers.
In order to demonstrate that the transfer was made according to the provisions of the Law and this regulation, the burden of proof will lie in all cases with the issuer of the data.

Article 21.- Transfer within a sector or corporate group and code of conduct.
In the event of transfers of personal data within corporate groups, subsidiaries, affiliated or related companies under common control of the same group of the holder of the database or data controller, or the affiliates or companies related to a parent company or to any company of the same group of the holder of the database or data controller, the personal data processing will be guaranteed if there is a code of conduct that establishes the internal rules for the protection of personal data with the content provided in article 31 of the Law, and recorded according to articles 89 to 97 of this regulation.

Article 22.- Receiver of personal data.
The receiver of the personal data assumes the condition of holder of the database or data controller in the aspects referred to by the Law and this regulation, and must process the personal data complying with the provisions of the information given by the issuer prior to the consent obtained from the data subject.

Article 23.- Formalization of national transfers.
The transfer must be formalized by mechanisms that allow demonstrating that the holder of the database or the data controller communicated to the receiver responsible the conditions in which the data subject consented to their processing.

Article 24.- Trans-border flow of personal data.
Trans-border flows of personal data will be possible when the receiver or importer of the personal data assumes the same obligations of the holder of the database or the data controller who transferred the personal data as issuer or exporter.

Pursuant to article 15 of the Law, in addition to the events provided in the first and third paragraph of said rule, the provisions of the second paragraph thereof also do not apply in case of personal data arising from a scientific or professional relationship of the subject, and they are necessary for its development or performance.

Article 25.- Formalization of the trans-border data flow.
For the purposes of the previous article, the issuer or exporter must use contractual clauses or other legal instruments, establishing at least the same obligations as to those to which it is subject, as well as the conditions under which the subject consented to the processing of his personal data.

Article 26.- Participation of the General Department of Personal Data Protection in the trans-border flow of data.
The holders of the database or data controllers may request the opinion of the General Department of Personal Data Protection as to whether the trans-border flow of data they carry out or will carry out complies with the provisions of the Law and this regulation.

In any case, the trans-border flow of data will be communicated to the General Department of Personal Data Protection, including the information required for the transfer of data and registration of the database.

Chapter IV

Special personal data processing

Article 27.- Processing of personal data of minors.
For the processing of personal data of a minor, the consent of the holders of parental authority or guardians will be required, as the case may be.

Article 28.- Exceptional consent.
The personal data of children over fourteen years of age and less than eighteen years of age may be done with their consent, provided that the information supplied is expressed in a language that is understandable for them, except if the law requires the assistance of the holders of parental authority or guardianship to be granted.

In no case may the consent to process personal data of minors be granted in order to have them access activities or related to goods or services that are reserved for persons of legal age.

Article 29.- Prohibition of recompiling.
Under no circumstances is it possible to collect from a minor data that allow obtaining information on the other members of his family group, such as data concerning the professional activity of his parents, economic information, sociological data or any other, without the consent of the subjects of such data.

It is only possible to collect the identity and address data of the parents or guardians in order to obtain the consent referred to in article 27 of this regulation.

Article 30.- Support of protection.
It is the obligation of all holders of databases and especially of public entities to collaborate with the support of the knowledge of the right to the protection of the personal data of children and adolescents, as well as the need to process them with special responsibility and safety.

Article 31.- Data processing in the communications and telecommunications sector.
The operators of communications or telecommunications services have the responsibility of assuring the confidentiality, security, adequate use and integrity of the personal data obtained from their subscribers and users during commercial operations. In this sense, said personal data may not be processed for purposes other than those authorized by their subject, except in case of court order or express legal mandate.

Article 32.- Confidentiality and security.
The communications or telecommunications operators must assure the confidentiality, security and proper use of any personal datum obtained as a consequence of their activity and will adopt the technical, legal and organizational measures as established in the Law and this regulation, without prejudice to the measures established in the rules of the communications and telecommunications sector that are not opposed to the provisions of the Law and this regulation.

Article 33.- Processing of personal data in "cloud computing"
The processing of personal data by services, applications and infrastructure in the so-called cloud computing may be done by the data controller, provided they guarantee compliance with the provisions of the Law and this regulation.

The holder of the database or, if applicable, the data controller, may not execute the contract if the services for the processing of personal data in the computer cloud do not guarantee the due protection of such data. For the contracting for cloud computing service to be considered pursuant to the Law, it is necessary to comply with the provisions of articles 34 and 35 and this regulation.

Article 34.- Obligations of the provider of cloud computing.
In addition to the indications of article 23 of this regulation, the provider of cloud computing will comply at least with the following:

1. Report with transparency the subcontracting involving the information on which the service is rendered.

2. Refrain from including conditions in the performance of the service that authorize or permit it to assume ownership or property of the information concerned by the service.

3. Keep confidentiality concerning the personal data on which it renders the service.

Article 35.- Mechanisms for provision of cloud computing.
The provider of the service must have the following mechanisms:

1. Inform on changes in its privacy policies or in the conditions of the service rendered to the data controller in order to obtain the consent if it means increasing its processing powers.

2. Allow the data controller to limit the type of processing of personal data on which it renders the service.

3. Establish and maintain adequate safety measures for the protection of personal data on which it renders the service.

4. Guarantee the elimination of the personal data after the service rendered to the controller is completed and the latter was able to recover them.

5. Prevent access to personal data to parties that do not have access privileges, or if it is requested by the competent authority, report this fact to the controller.

Article 36.- Provision of services or processing by order.
For the purposes of the Law, the delivery of personal data by the holder of the database to the processor does not constitute a transfer of personal data.

The processor of the database is prohibited from transferring to third parties the personal transfer concerned by the performance of processing services, unless the holder of the database who ordered the processing authorized it, and the data subject has given his consent, in the event that such consent is required pursuant to the Law.

The term for the conservation of the data will be two (2) years from the end of the last task performed.

The provisions of this article will apply, as it corresponds, to the subcontracting of personal data processing services.

Article 37.- Processing by subcontracting.
Personal data processing may be done by a third party other than the data processor, through an agreement or contract between these two.

In this event, it will be required to have a prior authorization from the holder of the database or data controller. Said authorization will also be understood granted if it was provided in the legal instrument formalizing the relationship between the data controller and the data processor. The processing done by the subcontractor is done in the name and on behalf of the data controller, but the burden of proving the authorization lies with the data processor.

Article 38.- Responsibility of the third party subcontracted.
The natural or legal persons subcontracted assumes the same obligations established for the data processor under the Law, this regulation and other applicable provisions. However, he will assume the obligations of the holder of the database or data controller, when:

1. It intends or uses the personal data for a different purpose than that authorized by the holder of the database or data controller; or

2. It makes a transfer, violating the instructions of the holder of the database, even when it is for the conservation of the data.

Chapter V

Security measures

Article 39.- Security for the processing of digital information.
The computer systems that handle databases or imply the processing of personal data must include in their operation records that keep all types of interaction with logical data, so as to identify the users, changes, consultations, starting and closing hours of a session and other actions carried out. These records will admit only the access of competent, authorized and identified personnel.

Furthermore, it is necessary to establish security measures related to the authorized accesses to the data by procedures of identification and authentication that guarantee the confidentiality and integrity of the data.

Article 40.- Conservation, backup and recovery of personal data.
The environments in which the information is processed, stored or transmitted must be implemented, taking into account the controls, policies, standards and recommendations related to physical and environmental security established in Peruvian Technical Standards "NTP-ISO/IEC 17799: 2007 EDI. Technology of Information. Code of Good Practice for the management of the security of the information. 2nd Edition," as well as taking into account "NTP ISO/IEC 27001: 2008 EDI Technology of Information. Security Techniques. Systems of Management of Information Security. Requisites."

Furthermore, the holders of databases will implement the necessary mechanisms for correct application of the procedures for making backup copies and recovery of the data. These mechanisms must guarantee the reconstruction in the status they had at the time of the loss or destruction.

Article 41.- Logical or electronic transfer of personal data.
The withdrawal or transfer of information assets containing personal data from the processing or storage environments will be done only with the authorization of the holder of the database and using the transport means authorized by it.

Any information that contains personal data must be protected in its storage and electronic transport with current encrypting algorithms. Furthermore, the electronic components that allow the transfer of information must contain security procedures and standards that protect the equipment and the information.

Article 42.- Storage of non-automated documentation.
The cabinets, filing cabinets and other elements where non-automated documents with personal data are stored must be in areas where access is protected with access doors with opening systems with key or other equivalent provision. Said areas must remain closed when it is not necessary to access the documents included in the database.

If, due to the characteristics of the rooms, it is established that it is not possible to comply with the provisions of the previous paragraph, alternative measures will be adopted, according to the instructions of the General Department of Personal Data Protection.

Article 43.- Copy or reproduction.
The generation of copies or the reproduction of documents may be done only under the control of authorized personnel.

It is necessary to destroy the copies or reproductions discarded so as to avoid access to the information contained therein or its subsequent recovery.

Article 44.- Access to the documentation.
The access to the documentation will be limited exclusively to the authorized personnel.

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

The access of persons not included in the previous paragraph must be adequately recorded according to the security instructions issued by the General Department of Personal Data Protection.

Article 45.- Non-automated documentation transfer.
Whenever the documentation contained in a database is physically transferred, it is necessary to adopt measures intended to prevent the access or handling of the information transferred.

Article 46.- Provision of services without access to personal data.
The controller or the processor of the information or processing will adopt adequate measures to limit the access of the personnel to personal data, to the media containing them or to the resources of the information system, to do work that does not imply the processing of personal data.

In the case of foreign personnel, the service contract will contain expressly the prohibition of accessing personal data and the secrecy obligation concerning the data that the personnel may have become aware of in connection with the performance of the service.

TITLE IV

Rights of the personal data holder

Chapter I

General provisions

Article 47.- Personal character.
The rights of information, access, rectification, cancellation or suppression, opposition or objective processing of personal data may only be exercised by the data subject, without prejudice to the rules governing the representation.

Article 48.- Exercise of the rights of the data subject.
The exercise of one or several of the rights does not exclude the possibility of exercising one or several of the others, nor may it be understood as a prior requisite to exercise any of them.

Article 49.- Legitimacy to exercise the rights.
The exercise of the rights contained in this article is done:

1. By the data subject, proving his identity and presenting a copy of the National Identity Document or equivalent document.

The use of the digital signature according to current regulations replaces the presentation of the National Identity Document and its copy.

2. By legal representative accredited as such.

3. By representative, expressly authorized to exercise the right, attaching the copy of his National Identity Document or equivalent document, and the title proving the representation.
When the holder of the database is a public entity, the representation may be proven by any valid means under the law that leaves a reliable record, pursuant to article 115 of Law No. 27444, Law of General Administrative Procedure.

4. In the event that the procedure indicated in article 51 of this regulation is chosen, the accreditation of the identity of the subject will be subject to that provision.

Article 50.- Requisites of the request.
The exercise of the rights is done by request addressed to the holder of the database or data controller, containing:

1. Names and surnames of the subject of the right and accreditation thereof and, if applicable, of his representative, according to the previous article.

2. Concrete petition that gives right to the request.

3. Domicile or address that may be electronic, for the purposes of applicable notifications.

4. Date and signature of the applicant.

5. Documents supporting the petition, if applicable.

6. Payment of the consideration, in the case of public entities, provided that it is included in their procedures established prior to the enactment of this regulation.

Article 51.- Public services
When the holder of the database or data controller have a service of any nature for their public or for complaints related to the service rendered or products offered, it may also resolve the requests for the exercise of the rights included in this title through said services, provided that the terms are not longer than those established in this regulation.

In this case, the identity of the data subject is considered accredited by the means established by the holder of the database or data controller to identify him, provided that it is accredited according to the nature of the service or product offered.

Article 52.- Receipt and remediation of the petition.
It is necessary to receive all the requests presented, the holder of the database or data controller leaving record of their receipt. If the request does not comply with the requisites indicated in the previous article, the holder of the database or data controller will have five (5) days from the day following the receipt of the request, to make observations due to noncompliance, which may not be remedied ex officio, inviting the subject to remedy them within a maximum term of five (5) days.

Once the term indicated lapses without the remediation, the request will be deemed not submitted.

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

Article 53.- Facilities to exercise the right.
The holder of the database or data controller is obligated to establish a simple procedure for the exercise of the rights. Without prejudice to that indicated and regardless of the means or mechanism established by the Law and this regulation to exercise the rights of the data subject, the holder of the database or the data controller may offer mechanisms that facilitate the exercise of such rights for the benefit of the data subject.

For the purposes of the consideration payable by the data subject to exercise his rights before the public administration, the first paragraph of article 26 of the Law will apply.

The exercise of his rights by the data subject before the personal databases privately administered will be free of charge, except as established in the special rules on the matter. Under no circumstances will the exercise of these rights imply an additional income for the holder of the database or data controller with which these rights are exercised.

It will not be possible to establish as means to exercise the rights any that imply the collection of an additional rate from the applicant or any other means that imply an excessive cost.

Article 54.- Form of the answer.
The holder of the database or data controller must give an answer to the request in the form and term established in this regulation, regardless of whether or not the personal data of the subject appears in the personal databases administered by them.

The answer to the data subject must refer only to the data indicated specifically in the request and must be presented clearly, legibly, understandably and in an easy to access form.

Should it be necessary to use keys or codes, the corresponding meanings must be provided.

The holder of the database or data controller will be responsible for the proof of compliance with the duty of answer, keeping the means to do so. This will apply, in the pertinent aspects, to prove the performance of the aspects established in the second paragraph, article 20 of the Law.

Article 55.- Answer terms.

1. The maximum answer term of the holder of the database or data controller concerning the exercise of the information right will be eight (08) days from the day following the presentation of the corresponding request.

2. The maximum term for the answer of the holder of the database or data controller to the exercise of the right of access will be twenty (20) days from the day following the presentation of the request by the data controller.

   If the request is approved and the holder of the database or data controller does not enclose the information requested with its answer, the access will be effective within ten (10) days following said answer.

3. In the case of the exercise of the other rights, such as that for update, inclusion, rectification, suppression or opposition, the maximum term for the answer of the holder of the database or data controller will be ten (10) days from the day following the presentation of the corresponding request.

Article 56.- Request for additional information.
In the event that the information provided in the request is insufficient or erroneous, so as to not allow it to be used, the holder of the database may require, within seven (7) days after receiving the request, additional documentation from the data subject in order to respond.

Within the term of ten (10) days from the receipt of the request, from the day following that of its receipt, the data subject will accompany the additional documentation he deems appropriate to support his request. Otherwise, the request will be deemed not presented.

Article 57.- Expansion of the terms.
Except for the term established for exercising the information right, the terms corresponding to the answer or the provision of the other rights may be expanded once only, for the same term as a maximum, provided the circumstances justify it.

The justification of the expansion of the term must be communicated to the data subject within the term to be expanded.

Article 58.- Application of specific legislation.
When the provisions applicable to certain databases, according to the special legislation regulating them, establish a specific procedure for the exercise of the rights regulated by this title, they will apply if they offer the same or higher guarantees to the data subject and do not violate the provisions of the law and this regulation.

Article 59.- Partial or total refusal for the exercise of a right.
The total or partially negative answer from the holder of the database or data controller to the request for a right of the data subject must be duly justified and must indicate his right to appeal with the General Department of Personal Data Protection by complaint, pursuant to article 24 of the Law and this regulation.

Chapter II

Special provisions

Article 60.- Right to information.
The data subject has the right, by access, to be given all the information indicated in articles 18 of the Law and 12 of this regulation.

The answer will contain the aspects provided in the articles cited in the previous paragraph, except if the subject requested the information regarding only some of them.
For the answer to the exercise of the right to information, in the pertinent aspects, the provisions of articles 62 and 63 of this regulation will apply.

Article 61.- Right of access.
Without prejudice to the provisions of article 19 of the Law, the data subject has the right to obtain from the holder of the database or data controller the information concerning his personal data, as well as all the conditions and general provisions of their processing.

Article 62.- Means to comply with the right of access.
The information corresponding to the right of access, at the choice of the data subject, may be provided in writing, by electronic means, by telephone, image or other appropriate means for this purpose.

The data subject may choose through one or several of the following forms:

1. Visualization on site.

2. Writing, copy, photocopy or fax.

3. Electronic transmission of the answer, provided that the identity of the interested party is guaranteed, the same as the confidentiality, integrity and receipt of the information.

4. Any other form or means that are adequate to the configuration or material implementation of the database or the nature of the processing, established by the holder of the database or data controller.

Regardless of the form used, the access must be in clear, legible and intelligible format, without using keys or codes that require mechanical devices for proper understanding and, if applicable, accompanied by an explanation. Furthermore, the access must be in accessible language to the average knowledge of the population, of the terms used. Notwithstanding, in order to use the most ecological communication means available in each case, the data controller may agree with the subject on the use of reproduction means of the information other than those established in this regulation.

Article 63.- Content of the information
The information made available to the data subject in connection with the exercise of the access right must be ample and include the entire record corresponding to the data subject, even if the request will include only one aspect of such data. The report may not disclose data belonging to third parties, even if they are related to the interested party.

Article 64.- Update.
It is the right of the data subject, by rectification, to update the data that have been modified on the date of exercise of the right.

The request for updating must indicate to what data it refers, as well as the modification to be made in them, enclosing the documentation supporting the suitability of the update requested.

Article 65.- Rectification.
It is the right of the data subject to modify the data that are inexact, erroneous or false.

The request for rectification must indicate to what personal data it refers, as well as the correction that must be made in them, enclosing the documentation supporting the suitability of the rectification requested.

Article 66.- Inclusion
It is the right of the data subject, by rectification, to have his data incorporated into a database, as well as to have incorporated, when processing his personal data, the missing information that makes them incomplete, omitted or eliminated, due to its relevance for said processing.

The request for inclusion must indicate to what personal data it refers, as well as the incorporation to be made in them, enclosing the documentation supporting the suitability and interest for the inclusion.

Article 67.- Suppression or cancellation.
The data subject may request the suppression or cancellation of his personal data from a database when they stopped being necessary or pertinent for the purpose for which they were collected, when the term established for their processing has lapsed, when he has revoked his consent for processing and in the other cases where they are not processed, pursuant to the Law and this regulation.

The request for suppression or cancelation may refer to all personal data of the subject contained in a database or only in some part of them.
Within the content of article 20 of the Law and section 3) article 2 of this regulation, the request for suppression implies the stoppage of the personal data processing, based on blocking thereof and their subsequent elimination.

Article 68.- Communication of the suppression or cancellation.
The holder of the database or data controller must document to the data subject that it complied with the request and indicate the transfers of the data suppressed, identifying to whom they were transferred, as well as the communication of the corresponding suppression.

Article 69.- Inapplicability of the suppression or cancellation.
The suppression will not be applicable when the personal data must be kept for historic, statistical or scientific reasons, according to applicable legislation or, if applicable, in contractual relationships between the controller and the data subject justifying the processing thereof.

Article 70.- Protection in case of refusal of suppression or cancellation.
Whenever possible, depending on the nature of the reasons supporting the refusal provided in the previous paragraph, it is necessary to use means of disassociation or anonymization to continue processing.

Article 71. Opposition.
The data subject has the right not to have his personal data processed or to terminate processing when he did not give his consent for their collection because they were taken from a public access source.

Even if he gave consent, the data subject has the right to oppose the processing of his data if he proves the existence of founded and legitimate reasons related to a concrete personal situation that justifies the exercise of this right.

In the event that the opposition is found justified, the holder of the database has the right to oppose the processing of his data if he proves the existence of founded and legitimate reasons related to a concrete personal situation that justifies the exercise of this right.

In the event that the opposition is justified, the holder of the database or data controller must stop the processing that gave rise to the opposition.

Article 72.- Right to the objective processing of personal data.
To guarantee the exercise of the right to objective processing, pursuant to article 23 of the Law, in case of personal data as part of a decision-making process without the participation of the data subject, the holder of the database or data controller must report it as soon as possible, without prejudice to the provisions concerning the exercise of the other rights in the Law and this regulation.

Chapter III

Protection procedure

Article 73.- Direct protection procedure.
The exercise of the rights governed by the Law and this regulation starts with the request to be addressed directly by the data subject to the holder of the database or data controller, according to the characteristics governed in the previous articles of this Title.
The holder of the database or data controller must give the answer, within the terms provided in article 55 of this regulation, expressing the corresponding items to each of the aspects of the request.
If the term lapses without receiving the answer, the applicant may consider his request denied.

The denial or unsatisfactory answer gives the applicant the right to start the administrative proceeding with the General Department of Personal Data Protection, according to article 74 of this regulation.

Article 74.- Trilateral protection procedure.
The administrative procedure for the protection of the rights regulated by the Law and this regulation is subject to the provisions of articles 219 to 228 of Law No. 27444, Law of General Administrative Procedure, and will be resolved by resolution of the General Department of Personal Data Protection.

To start the administrative procedure referred to in this article, without prejudice to the general requisites provided in this regulation, the data subject must present with his request for protection:

1. The charge of the request previously sent to the holder of the database or data controller to obtain from him directly the protection of his rights.

2. The document containing the answer of the holder of the database or data controller, which in turn contains the denial of his request or the answer that he considers not satisfactory, if he received it.

   The maximum term in which it is necessary to resolve the request for protection of the rights will be thirty (30) days from the day following receiving the answer of the respondent or the expiration of the term to give it.

   The term may be expanded up to a maximum of thirty (30) additional days, given the complexity of the case.

   The order to carry out an inspection visit suspends the term provided for the resolution until the corresponding report is received.

Article 75.- Inspection visit
To better resolve, it is possible to order to the Department of Supervision and Control to make an inspection visit, which will be done according to articles 108 to 114 of this regulation, within five (5) days following the receipt of the order.

TITLE V

National Register of Personal Data Protection

Chapter I

General provisions

Article 76.- Registration.
The National Register of Personal Data Protection is the storage unit intended to contain mainly the information on databases publicly or privately owned, and its purpose is to give advertising to the registration of said bases, so that it would be possible to exercise the rights of access to the information, rectification, cancellation, opposition and others regulated by the Law and this regulation.

Article 77.- Acts and documents that may be recorded in the Register.
The following will be registered in the National Register of Personal Data Protection, pursuant to the Law and this Title:

1. Publicly administered databases, with the exceptions provided in the Law and this regulation.

2. Privately administered databases, with the exceptions provided in section 1) article 3 of the Law.

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

4. The sanctions, provisional or corrective measures imposed by the General Department of Personal Data Protection pursuant to the Law and this regulation.

5. The communications referring to the trans-border flow of personal data.

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

Article 78.- Obligation of registration.
The natural or legal persons of the private sector or public entities that create, modify or cancel databases are obligated to process the registration of these acts with the National Register of Personal Data Protection.

Chapter II

Registration procedure

Article 79.- Requisites.
The holders of databases must register them with the National Register of Personal Data Protection, providing the following information:

1. Name and location of the database, its purposes and uses provided.

2. Identification of the holder of the database and, if applicable, the identification of the data controller.

3. Types of data subject to processing in said bank.

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

5. Technical description of security measures.

6. Addressees of transfers of data.

Article 80.- Models or forms
The General Department of Personal Data Protection will publish by resolution the models or electronic forms of the request for creation, modification or cancellation of databases that allow their presentation through computer means or on paper, pursuant to the procedure established in this regulation.

The models or electronic forms may be obtained free of charge at the Institutional Portal.

Article 81.- Beginning.
The procedure will begin with the presentation to the Department of the National Register of Personal Data Protection, the request for creation, modification or cancellation of the database made by its holder or controller duly accredited.

In the case of request for registration, it must contain the requisites set forth in this regulation; if any of the requisites is missing, it will be required to remedy the omission as provided in the following article.

Furthermore, in case of request for modification or cancellation of a database, it is necessary to indicate the code of registration of the database with the National Register of Personal Data Protection.

The request must declare a domicile or address, for remittance of notifications concerning the respective procedure.

Article 82.- Remediation of defects and filing.
If the request presented does not meet the requisites of the regulation, the Department of the National Register of Personal Data Protection will ask the applicant to remedy the omission within the term of ten (10) days. Upon the lapse of the maximum term, if the interested party has not remedied the omission, the request will be filed off.

Article 83.- Registration resolution.
The Director of the Department of National Registration of Personal Data Protection will render the resolution ordering the registration of the database, provided it meets the requisites required by the Law and this regulation.

The resolution must contain:

1. The code assigned by the Register.

2. The identification of the database.

3. The description of the purpose and uses provided.

4. The identification of the holder of the database.

5. The category of the personal data contained.

6. The procedure to obtain them.

7. The processing system of the personal data and the indication of the security measures.

Furthermore, if applicable, it will include the identification of the data processor, the location of the database and the receivers of the personal data and of the trans-border flow.

After the registration of the database with the National Register of Data Protection, the decision will be communicated to the interested party.

The registration of a database in the National Register of Personal Data Protection does not exempt the subject from complying with the other obligations provided in the Law and this regulation.

Article 84. - Modification or cancellation of databases.
The registration of a database must be kept updated at all times. Any modification affecting the content of the registration must be previously communicated to the Department of the National Register of Personal Data Protection for registration.

When the holder of a database decides to cancel it, it must communicate this to the Department of the National Register of Personal Data Protection to cancel the registration. The applicant will specify the destination to be given to the data or the provisions for its destruction.

Article 85.- Duration of the procedure.
The maximum term to issue and communicate the resolution about the registration, modification or cancellation will be thirty (30) days.

If within said term no express resolution has been rendered and communicated, the database will be deemed registered, modified or cancelled for all purposes.

Article 86.- Inapplicability or denial of the registration.
The Director of the Department of the National Register of Personal Data Protection will render a resolution denying the registration when the request does not meet the requisites provided in the Law and this regulation or other provisions rendered by the General Department of Personal Data Protection, according to the legal powers granted to it.

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

Article 87.- Challenge.
The resolution denying the registration is subject to the motion for reconsideration and appeal, pursuant to the procedure indicated in Law No. 27444, Law of General Administrative Procedure.

Article 88.- The authorities.
The Department of the National Register of Personal Data Protection constitutes the first authority in order to file the administrative remedies against the denial of registration of a database. It will resolve the motion for reconsideration and will forward the appeals to the General Department of Personal Data Protection, which will resolve as last administrative authority the applicability or inapplicability of the registration.

Chapter III

Procedure for registration of code of conducts

Article 89.- Scope of application of code of conducts.

1. The code of conducts will be voluntary.

2. Industry code of conducts may refer to all or part of the processing carried out by the sector, being formulated by representative organizations.

3. The code of conducts promoted by a company or corporate group must refer to all processing done by them.

Article 90.- Content.

1. The code of conducts must be drafted in clear and accessible terms.

2. The code of conducts must be suitable to the provisions of the law and include as a minimum the following aspects:

    2.1. Clear and precise delimitation of their scope of application, the activities to which the code refers and the processing subject to it.

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

    2.3. Establishment of homogenous standards for compliance by those adhering to the code with the obligations established in the Law.

    2.4. Establishment of procedures facilitating the exercise by the appropriate parties of their rights of information, access, update, inclusion, rectification, suppression and opposition.

2.5. The determination of the national and international transfers of personal data which, if applicable, are provided with indication of the guarantees to be adopted.

2.6. The actions of support and spreading in matter of protection of data intended for the parties processing them, especially concerning their relationship with the parties affected.

2.7. The inspection mechanisms which guarantee compliance by the adhering parties of the provisions of the code of conduct.

3. In particular, the code must contain:

3.1. Clauses to obtain consent of the data subjects for the processing or transfer of their data.

3.2. Clauses to inform the data subjects about the processing when the data are not obtained from them.

3.3. Models for the exercise by the affected parties of their rights of information, access, updating, inclusion, rectification, suppression and opposition.

3.4. If applicable, models of clauses for compliance with the formal requisites to contract a data processor.

Article 91.- Beginning of the procedure.
The procedure for the registration with the National Register of Personal Data Protection of the code of conducts will always start at the request of the entity, body or association promoting the code of conduct.

The request, in addition to meeting the legally established requisites, will comply with the following additional requisites:

1. Accreditation of the representation of the person submitting the request.

2. Content of the agreement, convention or decision approving within the corresponding scope the content of the code of conduct presented.

3. If the code of conduct comes from an industry agreement or a company decision, the certification of the adoption of the decision and legitimacy of the entity adopting it will be attached, along with a copy of the bylaws of the association, industry organization or entity which approved the code.

4. In the case of code of conducts presented by industry associations or organizations, documentation concerning its representation in the sector will be attached.

5. In the case of code of conducts based on decisions of the company based on corporate decisions, the description of the processing to which they refer will be attached.

Article 92.- Remediation of defects.
After analyzing the substantive aspects of the code of conduct, if it is necessary to produce new documents or modify their content, the Department of National Registration of Personal Data Protection will ask the applicant to make the modifications needed within the term of ten (10) days.

Article 93.- Process.
After the term indicated in the previous article lapses, the Department of National Registration of Personal Data Protection will prepare a report on the characteristics of the draft code of conduct, which will be sent to the Department of Regulations and Legal Assistance to report within seven (07) days whether it complies with the requirements of the Law and this regulation.

Article 94.- Issue of the resolution.
After complying with the previous paragraphs, the Director of the Department of National Registration of Personal Data Protection will render the resolution ordering the registration of the code of conduct, provided it matches the requisites of the Law and this regulation.

Article 95.- Duration of the procedure.
The maximum term to render and communicate the resolution will be thirty (30) days from the date of presentation of the request to the Department of National Registration of Personal Data Protection. If, within said term, the resolution has not been rendered and communicated, the applicant may consider his request approved.

Article 96.- Inapplicability or denial of the registration.
The denial of the registration of the code of conduct will be resolved by resolution of the Director of the Department of the National Registration of Data Protection, when the request does not meet the requisites of the Law, this regulation and the provisions rendered by the General Department of Personal Data Protection in the framework of its legal and statutory competence.

The resolution denying the registration is subject to the motion for reconsideration and appeal, pursuant to the procedure indicated in articles 87 and 88 of this regulation.

Article 97.- Advertising
The National Register of Personal Data Protection will advertize the content of the codes of conduct using electronic or computer means.

TITLE VI

Violations and sanctions

Chapter I

Inspection Procedure

Article 98.- Object.
The inspection procedure will have the object of determining whether the circumstances justifying the beginning of the sanctioning procedure exist, with identification of the holder of the database or data controller and the alleged perpetration of acts contrary to the Law and this regulation.

Article 99.- Beginning of the inspection procedure.
The inspection procedure starts always ex officio as a consequence of:

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

2. By complaint of a public entity, natural or legal person.

In both cases, the Department of Supervision and Control will require the holder of the database, the processor or the person found responsible, information concerning personal data processing or the necessary documentation. In the event of inspection visits to the headquarters of public or private entities where the databases administered are found, the inspectors will have access to them.

Article 100.- Forwarding of the procedure.
If from the complaint presented it may be seen that it does not address the objectives of an inspection procedure but the protection of rights, the corresponding procedure will be forwarded.

Article 101.- Certification.
In the exercise of the inspection functions, the personnel of the Department of Supervision and Control of the General Department of Personal Data Protection will have the power of certification to establish the truthfulness of the facts in connection with the formalities of their position.

Article 102.- Requisites of the complaint.
The complaint must indicate the following:

1. Name of the complainant and domicile to receive notices.

2. List of the facts on which the complaint is based and the documents that support it.

3. Name and domicile of the respondent or, if applicable, data to locate him.

Article 103.- Form of the complaint.
The complaint may be presented on physical medium or according to the automated forms shown in the Institutional Portal of the Ministry of Justice and Human Rights.

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

Article 104.- Request for information.
When the complaint is formulated, the Department of Supervision and Control may request the documentation it deems appropriate from the complainant in order to carry out the procedure.

Article 105.- Development of inspection.
The inspection procedure will have a maximum duration of ninety (90) days; this term runs from the date the Department of Supervision and Control receives the complaint or starts ex oficio the procedure and with the report indicating an opinion on the existence of elements that sustain or not the alleged commission of violations provided in the Law.

The term established may be expanded once, up to a period of forty-five (45) days, by motivated decision, given the complexity of the matter inspected and with the knowledge of the General Director of Personal Data Protection.

Article 106.- Visits program.
The inspection may include various visits to obtain the necessary elements of conviction, which will be developed with a maximum term of ten (10) days between them. After the first visit, a program of visits will be communicated to the holder of the database or to the processor or the data controller, and if applicable to the complainant.

Article 107.- Identification of the inspecting personnel.
When the visit starts, the inspecting personnel must show valid credentials with photo, issued by the General Department of Personal Data Protection, accrediting them as such.

Article 108.- Inspection visits.
The personnel making inspection visits must have a written order with autograph signature of the executive, of which he will leave a copy, with charge to the person receiving the visit.

The order must specify the place or places where the public or private entity or the natural person inspected is located, or where the databases subject to inspection are located, the generic object of the visit, and the legal provisions on which it is based.

Article 109.- Inspection minutes.
Inspection visits require drawing up the corresponding minutes, in which note will be left of the actions carried out during the verification visits. Said minutes will be drawn up in the presence of two witnesses proposed by the person with whom the action took place. If he denied to offer them or the persons offered do not participate, the signature of the person with whom the action took place will be sufficient, or the proof of his refusal to sign, if applicable.

The minutes will be prepared in two copies, and will be signed by the inspecting personnel and those who participated in the action. The minutes may include the declaration that the participants deem appropriate for their right.

The inspected party will receive one of the originals of the inspection minutes, incorporating the other to the file.

Article 110.- Content of the inspection minutes
The inspection minutes will contain:

1. Name, denomination or corporate name of the party inspected.

2. Time, day, month and year when the inspection starts and ends.

3. The data that fully identifies the place where the inspection took place, such as street, avenue, passage, number, district, ZIP code, public or private entity located at the place where the inspection was conducted, as well as the telephone number or other form of communication available with the inspected party.

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

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

6. Name and domicile of the persons who participated as witnesses.

7. Data and details related to the action.

8. Declaration of the inspected party, if requested.

9. Name and signature of those who participated in the inspection, including those who carried it out. If the inspected party, his legal representative or the person who received the inspector refused to sign, it will not affect the validity of the minutes, the inspecting personnel having to enter the respective reason.

The signature of the inspected party will not imply his agreement with the content, but only his participation and its receipt.

Article 111.- Obstruction to the inspection.
If the inspected party directly refuses to collaborate or presents an obstructive conduct, delaying without justification his collaboration, asking unreasonable questions from the inspecting personnel, not complying with the indications of the inspectors or any other similar or equivalent conduct, note thereof will be entered in the minutes, with the specification of the obstructive act or acts and its systematic nature, if applicable.

Article 112.- Observations in the act of inspection or subsequently.
Without prejudice to the possibility of the inspectors to make observations in the inspection minutes and declare what they deem appropriate concerning the acts contained in the minutes, they may also do so in writing within the term of five (5) days following the date of the minutes.

Article 113.- Report.
The inspection procedure will be completed with the report issued by the Department of Supervision and Control, determining in it preliminarily the circumstances that justify the opening of the sanctioning procedure or their absence.

If applicable, the measures to be ordered from the alleged responsible party will be ordered by injunction. The investigation of the sanctioning procedure will be made according to the Law and this regulation.

The determination of the alleged responsibility for acts contrary to the Law and this regulation contained in the Report will be communicated to the inspected party and to the complainant, if applicable, within a term not exceeding five (5) days.

Article 114.- Inapplicability of challenging means.
The inspection report issued by the Department of Supervision and Control is not subject to filing any appeal, contradiction of its content and any form of defense concerning it will be enforced in the sanctioning procedure, if applicable.

Chapter II

Sanctioning procedure

Article 115.- Authority of the Sanctioning Procedure.
For the application of the rules on the sanctioning procedure established in the Law, the authorities are:

1. The Director of the Department of Sanctions is the authority that investigates and resolves, in first instance, the existence of violation and the imposition or non-imposition of sanctions and the accessory obligations tending to protect personal data. Furthermore, he is competent to conduct and develop the investigation phase, and is responsible to carry out the actions necessary to determine the circumstances of the commission, or not, of acts contrary to the provisions of the Law and this regulation.

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

Article 116.- Beginning of the sanctioning procedure.
The sanctioning procedure will always be carried out ex officio, following a report of the Department of Supervision and Control that may follow an ex parte complaint or the motivated decision of the General Director of Personal Data Protection.

Article 117.- Preliminary rejection
The Department of Sanctions may, by express motivated resolution, decide to file off the cases that do not justify the opening of a sanctioning procedure, in spite of the report of the Department of Supervision and Control. This decision may be appealed by the complainant.

Article 118.- Provisional and corrective measures.
After the beginning of the sanctioning procedure, the Department of Sanctions may order, by motivated act, the adoption of provisional measures to ensure the efficacy of the final resolution that may be rendered in the respective procedure, observing the applicable rules of Law No. 27444, Law of General Administrative Procedure.

Furthermore, without prejudice to the corresponding administrative sanction for a violation of the provisions of the Law and this regulation, corrective measures may be rendered, when possible, intended to eliminate, avoid or stop the effects of the violations.

Article 119.- Content of the resolution for the beginning of the sanctioning procedure.
The Department of Sanctions communicates the resolution of beginning of the sanctioning procedure, containing:

1. The identification of the authority issuing the notification.

2. The indication of the corresponding file and the mention of the inspection minutes, if applicable.

3. The identification of the public or private entity for which the procedure is opened.

4. The decision to open a sanctioning procedure.

5. The statement of background that motivates the beginning of the sanction procedure, including the declaration of the facts attributed to the citizen, and the qualification of the violations that such facts may constitute.

6. The sanction or sanctions that may be imposed, if applicable.

7. The term to present defenses and evidence.

Article 120.- Presentation of defenses and evidence.
The citizen has a maximum term of fifteen (15) days, calculated from the day following that corresponding to the notice, to present his defense, in which he may declare concretely concerning one of the facts blamed on him expressly, affirming them, denying them, indicating that he does not know about them because they are not his own or presenting how they occurred, as applicable. Furthermore, he may present arguments to deny the violation presumed and the corresponding evidence.

In the event that expert or witness evidence is offered, the facts they concern will be specified, indicating the names and domiciles of the expert or witnesses, presenting the respective questionnaire or interrogatory for their preparation. Without these requisites, such evidence will be deemed not offered.

Article 121.- Acts for the investigation of the facts.
After the term of fifteen (15) days for the presentation of the defense, with or without it, the Department of Sanctions will carry out, ex oficio, all actions necessary to examine the facts and may order an inspection visit to be carried out by the Department of Supervision and Control, if not done earlier, in order to collect the information necessary or relevant to determine, if applicable, the existence of violations likely to be punished.

Article 122.- Closing of the investigation and resolution.
Upon the completion of the investigation actions, within a term not exceeding fifty (50) days, the Department of Sanctions issues a resolution closing the investigation stage and resolving in first instance, within fifteen (15) days after the notice of closing of the investigation stage. The resolution will be communicated to all parties participating in the procedure.
In the event of justified cause, the Department of Sanctions may extend once, for an equal period, the term of fifty (50) days referred to in this article.

Article 123.- Challenge.
The resolution resolving the sanctioning procedure may be challenged by motion for reconsideration or appeal, within fifteen (15) days from the communication of the resolution to the citizen.

The motion for reconsideration will be supported by new evidence wand will be resolved by the Department of Sanctions within a term not exceeding thirty (30).
The appeal will be resolved by the General Director of Personal Data Protection, being addressed to the same authority that issued the challenged act. To forward the action, the appeal must be resolved within no more than thirty (30) days.

Chapter III

Sanctions

Article 124.- Determination of the administrative sanction of fine.
Fines are determined in Tax Value Units valid on the date of the violation, and, when such date cannot be established, that valid on the date the General Department of Personal Data Protection detected the violation.

Article 125.- Establishment of the amount of the administrative sanction of fine.
In order to establish the amount of the sanction to be imposed, it is necessary to observe the principle of reason of the sanctioning power recognized in section 3, article 230, Law No. 27444, Law of General Administrative Procedure, as well as the condition of recidivating party sanctioned, and the procedural conduct of the violator.

In the event that the violations continue, after being sanctioned, it is necessary to impose a higher sanction than that previously imposed pursuant to the terms established in section 7, article 230, Law No. 27444, Law of General Administrative Procedure.

Article 126.- Mitigating circumstances.
The collaboration with the actions of the authority and the spontaneous acknowledgement of the recognition of the violations accompanied by actions of amendment will be considered mitigating circumstances. In light of the opportunity for recognition and the formulas of amendment, the mitigation will also permit the motivated reduction of the sanction below the range provided in the Law.

Article 127.- Delay in the payment of the fines.
The citizen who does not timely pay the fines incurs in automatic default; consequently, the amount of the unpaid fines will produce late interest applied daily from the day following the maturity of the term for payment of the fine until the date of payment, inclusive, the amount of the unpaid fine being multiplied by the daily valid Late Interest Rate [Tasa de Interes Moratoria = TIM). The daily valid Late Interest Rate (TIM) results from dividing the current Late Interest Rate (TIM) by thirty (30).

Article 128.- Incentives for the payment of the sanction of fine.
It will be considered that the sanctioned party has paid the sanction of fine if, before the expiration of the term granted to pay the fine, he deposits in the bank account determined by the General Director of Personal Data Protection sixty percent (60%) of its amount. For said benefit to produce effects, the fact must be communicated to the General Department of Personal Data Protection, attaching the proof of the corresponding bank deposit. After said term, the payment will be admitted only in the entire amount of the fine imposed.

Article 129.- Execution of the sanction of fine.
The execution of the sanction of fine is governed by the applicable law referring to the procedure of coercive execution.

Article 130.- Register of sanctions, provisional and corrective measures.
The Department of National Register of Personal Data Protection will have in its charge the Register of Sanctioned parties for noncompliance with the Law and this regulation, the Register of Provisional Measures and the Register of Corrective Measures, which will be published in the Institutional Portal of the Ministry of Justice and Human Rights.

Article 131.- Application of coercive fines
In the event of noncompliance with accessory obligations to the sanction of fine imposed for violation of the Law and this regulation, the Department of Sanctions may impose coercive fines according to the following levels:

1. For noncompliance with accessory obligations to the sanction of fine imposed for light violations, the coercive fine will be from zero point two to two Tax Value Units (0.2 to 2 UIT).

2. For noncompliance with accessory obligations to the sanction of fine imposed for severe violations, the coercive fine will be from two to six Tax Value Units (2 to 6 UIT).

3. For noncompliance with accessory obligations to the sanction of fine imposed for very severe violations, the coercive fine will be from six to ten Tax Value Units (6 to 10 UIT).

TRANSITORY COMPLEMENTARY PROVISIONS

One.- Adaptation of databases.
Within the term of two (2) years from the enactment of this regulation, the existing databases must be adapted to the provisions of the Law and this regulation, without prejudice to the registration referred to in the Final Complementary Provision Five of Law No. 29733, Law of Personal Data Protection.

Two.- Sanctioning power.
The sanctioning power of the General Department of Personal Data Protection, in connection with databases existing on the date of enactment of this regulation, is suspended until the expiration of the adaptation term established in the Transitory Complementary Provision One.

Three.- Forms.
The General Department of Personal Data Protection will create the standard forms necessary for the procedures regulated in this regulation within a term not exceeding sixty (60) days from the enactment of this regulation.

843954-1