Preliminary Title

General provisions

Article 1.- Purpose and scope of application.

The purpose of this law is to regulate the manner and conditions in which the processing and protection of the personal data of natural persons is carried out, in accordance with Article 19 No. 4 of the Political Constitution.

Any processing of personal data carried out by a natural or legal person, including public bodies, must respect the rights and freedoms of individuals and shall be subject to the provisions of this law.

The data processing and protection regime established in this law shall not apply to the processing of data carried out in the exercise of the freedoms to express opinions and to inform regulated by the laws referred to in Article 19, No. 12, of the Political Constitution of the Republic. The media will be subject to the provisions of this law regarding the processing of data that they carry out for a purpose other than that of issuing opinions and informing.

Nor shall the rules of this law be applicable to the processing of data carried out by natural persons in relation to their personal activities.

Article 1 bis.- **Territorial scope of application.** The provisions of this law shall apply to the processing of personal data that is carried out under any of the following circumstances:

a) When the data controller or data processor is established or incorporated in the national territory.

b) When the data processor, regardless of its place of establishment or incorporation, carries out the processing of personal data on behalf of a data controller established or incorporated in the national territory.

c) When the data controller or data processor is not established in the national territory but its personal data processing operations are intended to offer goods or services to data subjects who are in Chile, regardless of whether they are required to make a payment, or to monitor the behavior of data subjects who are in the national territory, including their analysis, tracking, profiling, or prediction of behavior.

This law shall also apply to the processing of personal data carried out by a data controller who, although not being established in the national territory, is subject to national law by reason of a contract or international law.

Definitions

Article 2.-

For the purposes of this law, the following shall be understood:

a) Data storage: the conservation or custody of data in a registry or database.

b) Data blocking: the temporary suspension of any operation for the processing of the stored data.

c) Communication of personal data: disclosure by the data controller, in any way, of personal data to persons other than the data subject to whom the data concern, without assigning nor transferring them.

d) Expired data: data that has lost relevance by provision of the law, by the fulfillment of the condition or the expiration of the period indicated for its validity or, if there is no express rule, by the change of the facts or circumstances that it records.

e) Statistical data: data that, at its origin, or as a result of its processing, cannot be associated with an identified or identifiable data subject.

f) Personal data: any information linked to or referring to an identified or identifiable natural person. Any person whose identity can be determined, directly or indirectly, in particular by means of one or more identifiers, such as name, identity card number, analysis of elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person, shall be considered identifiable.

To determine whether a person is identifiable, all objective means and factors that could reasonably be used for such identification at the time of the treatment must be considered.

g) Sensitive personal data: Personal data that refer to the physical or moral characteristics of people or to facts or circumstances of their private life or intimacy, that reveal ethnic or racial origin, political, union or trade group affiliation, socioeconomic situation, ideological or philosophical convictions, religious beliefs, data relating to health, human biological profile, biometric data, and information relating to a natural person's sex life, sexual orientation and gender identity.

h) Suppression or cancellation of data: the destruction of data stored in registers or databases, whatever the procedure used for this purpose.

i) Sources of public access: all those databases or sets of personal data, whose access or consultation can be carried out lawfully by any person, such as the Official Gazette, the media or the public registries provided by law. The processing of personal data from publicly accessible sources shall be subject to the provisions of this law.

j) Public bodies: the authorities, State bodies and agencies described and regulated by the Political Constitution of the Republic, and those included in the second paragraph of Article 1 of Law No. 18,575, Constitutional Organization of the General Bases of the State Administration.

k) Anonymization: an irreversible procedure by virtue of which personal data cannot be linked or associated with a specific person, or allow their identification, because the link with the information that links, associates or identifies that person has been destroyed or eliminated. An anonymized piece of data is no longer personal data.

l) Pseudonymization: personal data processing that is carried out in such a way that it can no longer be attributed to a data subject without the use of additional information, provided that such additional information is contained separately and is subject to technical and organizational measures aimed at ensuring that the personal data are not attributed to an identified or identifiable natural person.

m) Personal database: an organized set of personal data, whatever the purpose, form or modality of their creation, storage, organization and access, which allows the data to be related to each other, as well as to carry out their processing.

n) Data controller or controller: any natural or legal person, public or private, who decides on the purposes and means of the processing of personal data, regardless of whether the data are processed directly by him or her or through a third party (data processor or processor).

ñ) Data subject or subject: natural person, identified or identifiable, to whom the personal data concern or refer.

o) Data processing: any operation or set of operations or technical procedures, whether automated or not, that allow in any way to collect, process, store, communicate, transmit or use personal data or sets of personal data.

p) Consent: any expression of free, specific, unequivocal and informed will, granted through a declaration or a clear affirmative action, by which the data subject, their legal representative or agent, as appropriate, authorizes the processing of personal data concerning him/her.

q) Right to access: the right of the data subject to request and obtain from the data controller, confirmation as to whether his/her personal data is being processed by such data controller, access to them, where appropriate, and to the information provided for in this law.

r) Right to rectification: the right of the data subject to request and obtain from the data controller, to modify or complete his/her personal data, when they are being processed by him/her, and are inaccurate, outdated or incomplete.

s) Right to suppression: the right of the data subject to request and obtain from the data controller that he or she suppress or delete his or her personal data, in accordance with the grounds provided for by the law.

t) Right to objection: the right of the data subject to request and obtain from the data controller, that a specific data processing is not carried out, in accordance with the grounds provided for under the law.

u) Right to portability of personal data: the right of the data subject to request and obtain from the data controller a copy of his/her personal data in a structured, generic and commonly used electronic format, which allows it to be operated by different systems, and to be able to communicate or transfer them to another data controller.

The data subject shall have the right to have his/her personal data transmitted directly from controller to controller when it is technically feasible.

v) Transfer of personal data: transfer of personal data by the data controller to another data controller.

w) Profiling: any form of automated processing of personal data that consists of using such data to evaluate, analyze or predict aspects relating to the professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of a natural person.

x) Third-party agent or data processor: the natural or legal person who processes personal data, on behalf of the data controller.

y) Agency: the Personal Data Protection Agency.

z) National Register of Sanctions and Compliance: this is a national public register administered by the Agency that records the certified prevention models; the data controllers who have adopted them, and the penalties that have been imposed on the data controllers who have broken the law.

Article 3.- Principles.

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

a) Lawfulness and faithfulness principles. Personal data may only be processed lawfully and fairly.

The controller must be able to prove the lawfulness of the processing of personal data that it carries out.

b) Purpose principle. Personal data must be collected for specific, explicit and lawful purposes. The processing of personal data must be limited to the fulfilment of these purposes.

In application of this principle, personal data may not be processed for purposes other than those reported at the time of collection, unless the processing is for purposes compatible with those originally authorized; that there is a contractual or pre-contractual relationship between the data subject and the data controller that justifies the processing of the data for a different purpose, provided that it is framed within the purposes of the contract or is consistent with the negotiations or negotiations prior to the execution of the contract; the data subject grants again his or her consent and when it is provided by the law.

c) Proportionality principle. The personal data processed must be limited to those necessary, appropriate and relevant in relation to the processing's purposes.

Personal data may be kept only for the time necessary to comply with the processing's purposes, after which they must be deleted or anonymized, without prejudice to the exceptions established by law. A longer period of time requires legal authorization or consent from the data subject.

d) Quality principle. Personal data must be accurate, complete, current and relevant in relation to its origin and the purposes of the processing.

e) Responsibility principle. Those who process personal data shall be legally responsible for compliance with the principles contained in this article, and for the obligations and duties in accordance with the law.

f) Security principle. In the processing of personal data, the controller must ensure adequate standards of security, protecting them against unauthorized or unlawful processing, and against their loss, leakage, accidental damage or destruction. The security measures must be appropriate and in accordance with the processing to be carried out and with the nature of the data.

g) Transparency and information principle. The data controller must provide the data subject with all the information necessary for the exercise of the rights established by this law, including the policies and practices on the processing of personal data, which must also be permanently accessible and available to any interested party in a precise, clear, unequivocal and free manner. The controller must adopt the appropriate and timely measures to facilitate the data subject's access to all the information indicated in this law, as well as any other communication relating to the processing carried out.

h) Confidentiality principle. The data controller and those who have access to personal data must maintain secrecy or confidentiality about them. The controller shall establish appropriate controls and measures to preserve secrecy or confidentiality. This duty subsists even after the relationship with the data subject has ended.

Title I Of the rights of the data subject of personal data

Article 4.- Rights of the data subject.

Any person acting on their own behalf or through their legal representative or agent, as appropriate, has the right of access, rectification, suppression, objection, portability and blocking of their personal data, in accordance with this law.

Such rights are personal, non-transferable and inalienable and cannot be limited by any act or agreement.

In the event of the death of the data subject, the rights recognized by this law may be exercised by his or her heirs. However, the heirs may not access the deceased's data, or request its rectification or suppression, when the deceased person has expressly prohibited it or is established by law.

Article 5.- Right to access.

The data subject has the right to request and obtain from the data controller, confirmation as to whether the personal data concerning him or her is being processed by the controller, and if so, to access such data and the following information:

a) The data processed and their origin.

b) The purpose or purposes of the processing.

c) The categories, classes or types of recipients, or the identity of each recipient, if requested by the data subject, to whom the data have been, or it is planned to be, communicated or transferred.

d) The period of time for which the data will be processed.

e) The legitimate interests of the controller, where the processing is based on the provisions of Article 13 d);

f) Significant information on the logic applied if the controller carries out data processing in accordance with article 8 bis.

The controller will always be compelled to provide information and access to the requested data except when a law expressly provides otherwise.

Article 6.- Right to rectification.

The data subject has the right to request and obtain from the data controller, the rectification of the personal data that concern him or her and that are being processed by him/her, when they are inaccurate, outdated or incomplete.

The rectified data must be communicated to the persons, entities or bodies to which the controller has communicated or transferred the aforementioned data, except in cases where such communication is impossible or requires a disproportionate effort.

Once the rectification has been made, the data cannot be processed again without rectification.

Article 7.- Right to suppression. The data subject has the right to request and obtain from the data controller the elimination of his/her personal data in the following cases:

a) When the data are not necessary in relation to the purposes of the processing for which they were collected.

b) When the data subject has revoked their consent for the processing, and this has no other legal basis.

c) When the data has been obtained or processed unlawfully by the data controller.

d) When it is expired data.

e) When the data must be deleted in order to comply with a court ruling, a decision of the data protection authority or a legal obligation; and

f) When the data subject has exercised his right of objection in accordance with the following article and there is no other legal basis for its processing.

Suppression is not applicable when the treatment is necessary:

i. To exercise the right to freedom to express opinions and to inform.

ii. For the fulfillment of a legal obligation or the execution of a contract signed between the data subject and the data controller.

iii. For the performance of a public function or for the exercise of an activity of public interest.

iv. For reasons of public interest in the area of public health, in accordance with the conditions and guarantees established by law.

v. For processing for historical, statistical or scientific purposes and for studies or research that serve purposes of public interest, and

vi. For the formulation, exercise or defense of an administrative or judicial claim.

Article 8.- Right to Object.

The data subject has the right to object to the data controller to the specific or particular processing of personal data concerning him/her, in the following cases:

a) When the legal basis for the processing is the satisfaction of the legitimate interests of the controller. In this case, the data subject may exercise its right to object at any time. The Data Controller must stop processing the personal data, unless it can demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims.

b) If the processing is carried out exclusively for marketing purposes or direct marketing of goods, products or services, including profiling, in accordance with Article 8 bis.

c) If the processing is carried out with respect to data obtained from a publicly accessible source and there is no other legal basis for its processing.

Objection to processing shall not be admissible when it is carried out for scientific or historical research purposes or statistical purposes, and provided that they are necessary for the performance of a public function or for the exercise of an activity of public interest.

Article 8 bis.- Automated individual decisions, including profiling. The data subject has the right to object to and not be subject to decisions based on the automated processing of his or her personal data, including profiling, whenever such processing renders legal effects on him/her or gravely affects him/her.

The preceding paragraph shall not apply in the following cases:

a) When the decision is necessary for the conclusion or execution of a contract between the data subject and the data controller.

b) When there is prior and express consent of the data subject in the manner prescribed in Article 12.

c) When indicated by law, to the extent that it provides for the use of safeguards to the rights and freedoms of the data subject.

In all cases of decisions based on the automated processing of personal data, including those indicated in letters a), b) and c) above, the controller must adopt the necessary measures to ensure the rights and freedoms of the data subject, his/her right to information and transparency, the right to obtain an explanation, human intervention, and to express his/her point of view and to request a review of the decision.

Article 8 ter.- Right to block the processing.

The data subject has the right to request the temporary suspension of any processing operation of his/her personal data when he/she makes a request for rectification, suppression or objection in accordance with Article 11 of this Law, until such request is resolved. Likewise, the data subject may exercise the right as an alternative to the suppression in the cases of Article 7.

The exercise of this right shall not affect the storage of the data by the controller.

Article 9.- Right to portability of personal data.

The data subject has the right to request and receive a copy of the personal data concerning him/her, which he/she has provided to the controller, in an electronic, structured, generic and

commonly used format, which allows it to be operated by different systems and to communicate or transfer them to another data controller, when the following circumstances occur:

a) The processing is carried out in an automated manner, and

b) The processing is based on the consent of the data subject.

The data controller must use the most expeditious, least onerous means and without placing obstacles or obstacles to the exercise of this right.

The controller must also communicate to the data subject in a clear and precise manner the measures necessary to obtain their personal data and specify the technical characteristics to carry out these operations.

The data subject shall have the right to have his/her personal data transmitted directly from controller to controller where technically feasible.

However, the exercise of the right of portability will not imply the suppression of the data before the assigning controller, unless the data subject jointly requests it in the petition.

Article 10.- Form and means of exercising the rights of the data subject.

The rights recognized in this law are exercised by the data subject before the data controller. If the data subject's personal data is processed by several controllers, the data subject may exercise his or her rights before any of them.

In the case of legal entities not incorporated in Chile, the data controller must indicate in writing, before the Agency, an e-mail address or an equivalent valid and operative electronic mean of communication of a natural or legal person capable of acting on its behalf, so that the data subject may exercise its rights and communicate with the data controller, and where the communications and administrative notification provided by law may be validly made. The data controller must keep this information updated.

Data controllers must implement mechanisms and technological tools that allow the data subject to exercise their rights expeditiously, agilely, and effectively. The means provided by the data controller must be simple in their operation.

The exercise of the rights of rectification, suppression and objection will always be free of charge for the data subject. The right of access shall also be exercised free of charge, at least quarterly.

The data controller may only demand payment of the direct costs incurred when the data subject exercises his right of access and right to portability more than once in the quarter. The data controller may not demand this payment in the cases referred to in article 27 f) of this law.

The parameters and mechanisms for determining the costs derived from the exercise of the rights indicated in the previous paragraph shall be determined by the Agency, through a general instruction that shall consider, among other antecedents, the volume of data to be provided, the legal nature and the size of the entity or company that has the status of data controller.

The Agency will ensure the effective exercise and compliance with the rights that this law recognizes to the data subject, in accordance with the provisions of this law.

Article 11.- Procedure before the data controller.

To exercise the rights recognized by this law, the data subject must submit a written request or requirement to the data controller, addressed to the email address established for this purpose, a contact form or an equivalent electronic means. The application must contain, at least, the following mentions:

a) Identification of the data subject and his or her legal representative or agent, as appropriate, and authentication of their identity in accordance with the procedures, forms and modalities established by the Agency.

b) Indication of an address or an e-mail address or other equivalent means of communicating the response.

c) Identification of the personal data or the specific processing, in respect of which the corresponding right is exercised.

d) In the requests for rectification, the data subject must indicate the necessary modifications or updates to be made and provide, where appropriate, the background information that supports them. In the case of requests for suppression, the data subject must indicate the cause invoked and attach the background information that supports it, if applicable. For objection requests, the data subject must indicate the cause invoked and in the case of letter a) of Article 8, he/she must briefly substantiate his request and may also attach the background information he/she deems appropriate. In the case of the right of access, the individualization of the data subject will suffice.

Once the request has been received, the data controller must acknowledge receipt of it and make a decision no later than thirty calendar days, following the date of receipt of the application. This period may be extended, only once, for up to thirty calendar days.

The controller must respond in writing to the data subject at his/her address or the email address set by him/her. The data controller must store the backups that allow him/her to demonstrate the sending of the response to the corresponding physical or electronic address, its date and the full content of it.

In the event of total or partial denial of the request, the data controller must justify his/her decision by indicating the cause invoked and the background that justifies it. On the same occasion, the data controller must indicate to the data subject that he or she has a period of thirty working days to file a claim with the Agency, in accordance with the procedure established in Article 41.

After the period referred to in the second paragraph above, without a response from the data controller, the data subject may directly file a complaint with the Agency, under the same terms as the previous paragraph.

When a request for rectification, suppression or objection is made, the data subject will have the right to request and obtain from the controller the temporary blocking of their data or the processing they carry out, as appropriate. The request for temporary blocking must be

substantiated and the data controller must respond to the request within two working days of its receipt. As long as this request is not resolved, the data controller may not process the data of the data subject that is part of the requirement. The temporary blocking of the data will not affect its storage by the data controller. In the event of rejection, the data controller must justify his response and communicate his/her decision electronically to the Agency. The data subject may lodge a complaint against this decision with the Agency, applying the provisions of Article 41(a).

The rectification, suppression or objection to the processing of the data will apply only with respect to the data controllers to whom the request has been made. However, when the controller has communicated such data to other persons, they must notify them of the changes made by virtue of the rectification, suppression or objection.

The data subject may provide any other background information that facilitates the location of the personal data.

Title II

Processing of personal data and special categories of data

First Paragraph

The consent of the data subject, the obligations and duties of the controller and the processing of data in general

Article 12.- General rule of data processing.

The processing of personal data concerning the data subject is lawful when he or she gives his or her consent to do so.

The consent of the data subject must be free, informed and specific in terms of its purpose or purposes. Consent must also be expressed in advance and unequivocally, by means of a verbal, written or expressed declaration through an equivalent electronic means, or by means of an affirmative act that clearly reflects the will of the data subject.

When consent is granted by an agent, the latter must be expressly authorized to do so.

The data subject may revoke the consent granted at any time and with no cause, using means similar or equivalent to those used to grant it. The revocation of consent will not have retroactive effects.

The means used for the granting or revocation of consent must be expeditious, reliable, free of charge and permanently available to the data subject.

It is presumed that consent to process data has not been freely granted when the controller collects it in the context of the performance of a contract or the provision of a service in which it is not necessary to carry out such collection.

However, the provisions of the previous paragraph shall not apply when the person offering goods, services or benefits requires consent to process data as the only consideration.

It is up to the data controller to prove that it had the consent of the data subject, and that the data processing was carried out in a lawful, fair and transparent manner.

Article 13.- Other sources of lawfulness of data processing.

The processing of personal data is lawful with no consent of the data subject, in the following cases:

a) When the processing refers to data relating to obligations of an economic, financial, banking or commercial nature and is carried out in accordance with the rules of Title III of this law, including data referring to the socio-economic situation of the data subject.

b) When the processing is necessary for the execution or compliance with a legal obligation or is provided for by law.

c) When the data processing is necessary for the conclusion or execution of a contract between the data subject and the controller, or for the execution of pre-contractual measures adopted at the request of the data subject.

d) When the processing is necessary for the satisfaction of the legitimate interests of the controller or a third party, provided that this does not affect the rights and freedoms of the data subject. In any case, the data subject may always demand to be informed about the processing that affects him or her and what is the legitimate interest on the basis of which such processing is carried out.

e) When the processing of data is necessary for the formulation, exercise or defense of a right before the courts of justice or public bodies.

The controller must prove the lawfulness of the data processing.

Article 14.- Obligations of the data controller.

The data controller, without prejudice to the other provisions provided for in this law, has the following obligations:

a) To inform and make available to the data subject the background information that proves the lawfulness of the data processing carried out. Likewise, it must expeditiously deliver said information when required;

b) To ensure that personal data are collected from lawful sources of access for specific, explicit and lawful purposes, and that their processing is limited to the fulfilment of these purposes;

c) To communicate or transfer, in accordance with the provisions of this law, accurate, complete and current information;

d) Delete or anonymize the data subject's personal data when they were obtained for the execution of pre-contractual measures, and

e) Comply with the other duties, principles and obligations governing the processing of personal data provided for in this law.

The data controller who is not domiciled in Chile and who processes the data of persons residing in the national territory, must indicate and keep updated and operative, an email

address or other suitable means of contact to receive communications from the data subjects and the Agency.

Article 14 bis.- Duty of secrecy or confidentiality.

The data controller is obliged to maintain secrecy or confidentiality regarding personal data concerning a data subject, except when the data subject has made them manifestly public. This duty subsists even after the relationship with the data subject has ended. In the event that the data controller has carried out any action on personal data obtained from publicly accessible sources, such as organizing or classifying them under some criteria, or combining or complementing them with other data, the personal data resulting from such action will be protected under this duty of secrecy or confidentiality.

The duty of secrecy or confidentiality does not prevent the communications or transfers of data that must be made by the controller in accordance with the law, and compliance with the obligation to give access to the data subject and inform the origin of the data, when this information is required by the data subject or by a public body within the scope of its legal powers.

The data controller must adopt the necessary measures in order to ensure that its dependents or the natural or legal persons who carry out data processing operations under its responsibility, comply with the duty of secrecy or confidentiality established in this article.

The persons and institutions and their dependents referred to in Article 24 are subject to the obligation of confidentiality, as regards the request and the fact of having submitted such information.

Article 14 ter. Duty of information and transparency.

The data controller must provide and keep permanently available to the public, on its website or in any other equivalent means of information, at least the following information:

a) The personal data processing policy you have adopted, the date and version of the same;

b) The identification of the data controller and its legal representative and the identification of the prevention officer, if any;

c) The postal address, e-mail address, contact form or identification of the equivalent technological means of common use and easy access through which the requests made by the data subjects are notified;

d) The categories, classes or types of data that is processes; the generic description of the universe of people who comprise its databases; the recipients to whom the data are intended to be communicated or transferred; the purposes of the processing carried out; the legal basis of the processing; and in the case of processing being based on the satisfaction of legitimate interests, what these would be;

e) The policy and security measures adopted to protect the personal databases it administers;

f) The right of the data subject to request from the data controller access, rectification, suppression, objection and portability of their personal data, in accordance with the law.

g) The right of the data subject to appeal to the Agency, in the event that the controller rejects or does not respond in a timely manner to the requests made to him/her.

h) Where applicable, the transfer of personal data to a third country or international organization and whether or not these offer an adequate level of protection. In the event that they do not have an adequate level of protection, information should be provided on the existence of guarantees supporting said transfer.

i) The period for which the personal data will be retained.

j) The source from which the personal data come and, where appropriate, whether they come from publicly accessible sources.

k) When the processing is based on the consent of the data controller, the existence of the right to withdraw it at any time, without this affecting the lawfulness of the processing based on consent prior to its withdrawal.

l) The existence of automated decisions, including profiling. In such cases, significant information about the logic applied, as well as the expected consequences of such processing for the data subject.

Article 14 quarter.- Duty of protection from design and by default.

In order to comply with the principles and rights of the data subjects established in this law, the controller must apply appropriate technical and organizational measures from the design before and during the processing of personal data.

The measures to be applied must consider the state of the art; implementation costs; the nature, scope, context and purposes of the data processing; and the risks associated with such activity.

Likewise, the data controller must apply technical and organizational measures to ensure that, by default, only specific and strictly necessary personal data are processed for such activity. To this end, the number of data collected, the extent of the processing, the storage period and its accessibility will be considered.

Article 14 quinquies.- Duty to adopt security measures.

The data controller must adopt the necessary measures to safeguard compliance with the security principle established in this law, considering the current state of the art and the costs of application, together with the nature, scope, context and purposes of the processing, as well as the probability of the risks and the severity of their effects in relation to the type of data processed. The measures applied by the controller must ensure the confidentiality, integrity, availability and resilience of the data processing systems. They must also prevent alteration, destruction, loss, treatment or unauthorized access.

Considering the state of the art, cost of implementation, and the nature, scope, context and purposes of processing, as well as the risks of variable likelihood and severity to the rights and freedoms of data subjects, the data controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, but not limited to:

a) The pseudonymization and encryption of personal data.

b) The ability to guarantee permanent confidentiality, integrity, availability and resilience of treatment systems and services.

c) The ability to restore availability and access to personal data quickly in the event of a physical or technical incident.

d) A process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the processing.

In the event of a security incident, and in the event of a judicial or administrative dispute, it will be the responsibility of the data controller to prove the existence and operation of the security measures adopted based on the levels of risk and the available technology.

Article 14 sexies.- Duty to report violations of security measures.

The data controller must report to the Agency, by the most expeditious means possible and without undue delay, any breaches of security measures that result in the accidental or unlawful destruction, leakage, loss or alteration of the personal data processed or the unauthorized communication or access to such data, when there is a reasonable risk to the rights and freedoms of the data subjects.

The controller must record these communications, describing the nature of the breaches suffered, their effects, the categories of data and the approximate number of data subjects affected, and the measures taken to manage them and prevent future incidents.

When such breaches refer to sensitive personal data, data relating to children under fourteen years of age or data relating to economic, financial, banking or commercial obligations, the controller must also make this communication to the data subjects of these data, through their representatives where appropriate. This communication must be made in clear and simple language, singling out the data affected, the possible consequences of the security breaches and the solution or safeguarding measures adopted. The notification must be made to each affected data subject and if this is not possible, it will be made through the dissemination or publication of a notice in mass social communication media of national scope.

The information duties indicated in this article do not preclude the other information duties established by other laws.

Article 14 septies.- Differentiation of compliance standards.

The minimum standards or conditions imposed on the data controller for compliance with the information and security duties established in Articles 14 ter and 14 quinquies, respectively, shall be determined considering the type of data in question, whether the data controller is a natural or legal person, the size of the entity or company in accordance with the categories established in Article 2 of Law No. 20,416, which establishes special rules for smaller companies, the activity they carry out and the volume, nature and purposes of the personal data they process.

The minimum standards or conditions of compliance and the differentiated measures referred to in the previous paragraph shall be determined by the Agency by means of a general instruction.

Article 15.- Transfer of personal data.

Personal data may be transferred with the consent of the data subject and for the fulfillment of the purposes of the processing. Personal data may also be transferred when the transfer is necessary for the performance and execution of a contract to which the data subject is a party; when there is a legitimate interest of the assignor or the assignee, in the terms provided for in letter d) of Article 13, and when provided for by law.

In the event that the consent granted by the data subject at the time of collecting the personal data has not considered the transfer thereof, such consent shall be obtained before the transfer takes place, being considered for all legal purposes as a new processing operation.

The transfer of data shall be in writing or by any suitable electronic means. This document shall contain identification of parties, data to be transferred, intended purposes of the processing and any other background information or stipulations agreed upon by the by the assignor and the assignee.

The personal data transferred must be processed by the assignee in accordance with the assignment contract's purposes.

Once the assignment has been completed, the assignee acquires the status of data controller for all legal purposes. The assignor, for its part, also maintains the status of data controller, with respect to the processing operations that it continues to carry out.

If a transfer of data is verified without the consent of the data subject, which is necessary, the transfer will be null and void, and the assignee must delete all the data received, without prejudice to the corresponding legal responsibilities.

Article 15 bis.- Processing of data through a third-party data processor or agent.

The data controller may carry out the data processing directly or through a third-party data processor or agent. In the latter case, the third party data processor or agent carries out the processing of personal data in accordance with the assignment and instructions given by the data controller, being prohibited its processing for a purpose other than that agreed with the data controller, as well as its transfer or delivery in cases where the data controller has not given its express and specific authorization to comply with the purpose of the assignment.

If the third-party data processor or agent processes the data for a purpose other than the assignment agreed upon or transfers or delivers data with no authorization under the terms set forth in the preceding paragraph, such third-party shall be considered the data controller for all legal purposes, and shall be personally liable for any infringements incurred, and jointly with the data controller for any damages caused, notwithstanding the contractual liabilities that may correspond to it vis-à-vis the data processor or the data controller.

The processing of data through a third-party data processor or agent will be governed by the contract entered between the controller and the processor, in accordance with the legislation in force. The contract must establish the subject matter of the assignment, the duration of

the assignment, the purpose of the processing, the type of personal data processed, the categories of data subjects to whom the data concern, and the rights and obligations of the parties. The data controller may not delegate part or all of the assignment, unless there is a specific written authorization from the data controller. The processor who delegates part or all of the assignment to another processor will continue to be jointly liable for said assignment and may not be exempted from liability by arguing that he/she has delegated the processing. The Agency will make standard contract models available to the public on its website.

The third-party data processor or data controller must comply with the provisions of Articles 14 bis and 14 quinquies. The differentiation of standards established in the first paragraph of Article 14 septies shall also be applicable to the third-party data processor or data controller. In the case of a violation of security measures, the third party or data processor must report this fact to the data controller.

Once the processing service has been provided by the third-party data processor or agent, the data in its possession must be deleted or returned to the data controller, as appropriate.

Article 15 ter.- Impact assessment on the protection of personal data.

Where a type of processing, by its nature, scope, context, technology used or purposes, is likely to result in a high risk to the rights of data subjects, the data controller of data shall, prior to the start of processing operations, carry out an impact assessment on the protection of personal data.

The impact assessment will always be required in cases of:

a) Systematic and exhaustive evaluation of personal aspects of data subjects, based on automated processing or decisions, such as profiling, and which produce significant legal effects on them.

b) Massive data processing or large scale.

c) Treatment that involves systematic observation or monitoring of an area of public access.

D) Processing sensitive and specially protected data, in case of an exception to consent.

The Data Protection Agency shall establish and publish an indicative list of the types of processing operations that do or do not require a personal data protection impact assessment. The Agency shall also establish the minimum guidelines for carrying out this assessment, taking into account at least in those criteria, the description of the processing operations, their purpose, the assessment of necessity and proportionality with respect to their purpose, the assessment of risks and mitigation measures.

Data controllers may consult the Data Protection Agency when, by virtue of the outcome of the assessment, the processing proves to be high risk for obtaining recommendations from said entity.

Second Paragraph

Processing of sensitive personal data

Article 16.- General rule for the processing of sensitive personal data.

The processing of sensitive personal data may only be carried out when the data subject expressly gives his or her consent by means of a written or verbal statement or by an equivalent technological means.

Notwithstanding the foregoing, the processing of sensitive personal data, without the consent of the data subject, is lawful in the following cases:

a) When the processing refers to sensitive personal data that the data subject has made manifestly public and their processing is related to the purposes for which they were published.

b) When the processing is based on a legitimate interest carried out by a legal person under public or private law that does not pursue profit purposes, and the following conditions are met:

i.- Its purpose is political, philosophical, religious, cultural, trade union or trade association;

ii.- The processing carried out refers exclusively to its members or affiliates;

iii.- The purpose of data processing is aimed at fulfilling the specific objectives of the institution;

iv.- The legal entity provides the necessary guarantees to prevent leaks, thefts or unauthorized use or treatment of the data; and

v.- Personal data are not communicated or transferred to third parties.

If these conditions are met, the legal entity will not require the consent of the data subject to process their data, including sensitive personal data. In the event of administrative or judicial doubt or controversy, the data controller must prove its concurrence.

When a member of the legal entity ceases to belong to it, his or her data must be anonymized or deleted.

c) When the processing of the data subject's personal data is essential to safeguard the life, health or physical or mental integrity of the data subject or another person, or when the data subject is physically or legally prevented from granting his or her consent. Once the impediment ceases, the controller must inform the data subject in detail of the data that was processed and the specific processing operations that were carried out.

d) When the processing of the data is necessary for the formulation, exercise or defense of a right before the courts of justice or an administrative body.

e) When the data processing is necessary for the exercise of rights and compliance with the data controller or data subject's obligations, in the field of employment or social security, and is done within the law's framework.

f) When the processing of sensitive personal data is authorized or expressly mandated by law.

Exemptions for processing data without consent, as referred to in this article, are deemed applicable to the processing of data not considered as to be sensitive data.

Article 16 bis.- Sensitive personal data relating to health and the human biological profile.

If the provisions of the first paragraph of Article 16 are met, personal data relating to the data subject's health, as well as those relating to the biological profile of the data subject, such as genetic, proteomic or metabolic data, may only be processed for the purposes provided for by special laws on health matters.

Sensitive personal data relating to the health of the data subject and his or her biological profile may only be processed without his or her consent, in compliance with the principles and rules established in this law, in the following cases:

a) When this is essential to safeguard the life or physical or mental integrity of the data subject or of another person or, when the data subject is physically or legally prevented from granting his consent. Once the impediment ceases, the controller must inform the data subject in detail of the data that was processed and the specific processing operations that were carried out.

b) In cases of legally decreed health alert.

c) When they are used for historical, statistical or scientific purposes, for studies or research that serve purposes of public interest or benefit human health, or for the development of medical products or supplies that could not be developed in any other way. The results of scientific studies and research using personal data relating to health or biological profile may be freely published or disseminated. To this end the data that is published must be previously anonymized.

d) When the processing of the data is necessary for the formulation, exercise or defence of a right before the courts of justice or before an administrative body.

e) When the processing is necessary for the purposes of preventive or occupational medicine, evaluation of the worker's work capacity, medical diagnosis, provision of health or social assistance or treatment, or management of health and social care systems and services.

f) When the law so permits and expressly indicates the purpose that such processing must have.

It is prohibited to process and transfer data relating to the health and biological profile of a data subject and biological samples associated with an identified or identifiable person, including the storage of biological material, in cases where the data or samples have been collected for work, education, sports, social, insurance, security or identification purposes, save where the law expressly authorizes their processing in qualified cases and which refer to any of the cases mentioned in this article.

Exemptions for processing data without consent, as referred to in this article, are deemed applicable to the processing of data outside the special nature referred to in this provision.

Article 16 ter.- Biometric personal data

Biometric personal data are those obtained from specific technical processing, relating to the physical, physiological or behavioral characteristics of a person that allow or confirm the unique identification of that person, such as fingerprint, iris, hand or facial features and voice.

These data may only be processed when the provisions of the first paragraph of Article 16 are complied with and provided that the data controller provides the data subject with the following specific information:

(a) The identification of the biometric system used;

b) The specific purpose for which the data collected by the biometric system will be used;

c) The period during which the biometric data will be used; and

d) The way in which the data subject can exercise his rights.

Biometric personal data may be processed without consent only as provided for in the second paragraph of article 16 bis.

Third Paragraph

Processing of special categories of personal data

Article 16 quarter.- Personal data relating to children and adolescents.

The processing of personal data concerning children and adolescents may only be carried out in accordance with their best interests and respect for their progressive autonomy.

In compliance with the requirement established in the previous paragraph, in order to process the personal data of children, the consent granted by their parents or legal representatives or by the person in charge of the personal care of the child is required, unless expressly authorized or mandated by law.

The personal data of adolescents may be processed in accordance with the authorization rules provided for in this law for adults, except as provided in the following paragraph.

The sensitive personal data of adolescents under 16 years of age may only be processed with the consent granted by their parents or legal representatives or whoever is in charge of the personal care of the minor, unless expressly authorized or mandated by law.

For the purposes of this law, children are considered to be those under fourteen years of age, and adolescents are considered to be those over fourteen and under eighteen years of age.

It is a special obligation of educational institutions and of all individuals or public or private entities that process or manage personal data of children and adolescents, including those who exercise their personal care, to ensure the lawful use and protection of personal information concerning children and adolescents.

Article 16 quinquies.- Personal data for historical, statistical, scientific and study or research purposes.

Personal data processing by natural persons or corporate bodies, public or private, including government agencies, is deemed to have a legitimate interest when such processing is carried out for historical, statistical or scientific purposes only, and for studies or research, all of which must serve purposes in the public interest.

Data controllers shall adopt and prove that they have complied with all the quality and security measures necessary to safeguard that the data are used for such purposes only. For sensitive

personal data, the data controller shall identify potential risks and implement measures to reduce or mitigate them. Upon fulfilment of these conditions, the data controller may store and use the data for an undetermined period of time.

The data controller who has processed personal data exclusively for these purposes may publish the results and analyses thus obtained, if they have previously taken the necessary measures to anonymize the data to be published.

Article 16 sexies.- Geolocation data.

The processing of the personal geolocation data of the data subject may be carried out under the same legal basis established in articles 12 and 13.

The data subject must be informed in a clear, sufficient and timely manner, of the type of geolocation data that will be processed, of the purpose and duration of the processing and whether the data will be communicated or transferred to a third party for the provision of a value-added service.

Title III

The use of personal data relating to economic, financial, banking or commercial obligations

Article 17.- General rule for the processing of data relating to financial, banking or commercial obligations.

Data controller of registries or personal databases may only communicate information concerning obligations of an economic, financial, banking or commercial nature, when they are contained in protested bills of exchange and promissory notes; checks protested for lack of funds, checks drawn on a closed current account or for any other reason; as well as compliance or non-compliance with obligations derived from mortgage loans and loans or credits from banks, financial companies, mortgage loan administrators, savings and credit cooperatives, public agencies and State companies subject to common legislation, and companies administrating credits granted for purchases in retail stores. Information related to credits granted by the National Agency for Agricultural Development [INDAP, from the Spanish *Instituto Nacional de Desarrollo Agropecuario*] to its users, and information related to economic, financial, banking or commercial obligations insofar as they have been rescheduled, renegotiated or novated, or these are in any pending modality, are excepted.

Other monetary obligations determined by the President of the Republic by means of a supreme decree may also be communicated, which shall be supported by validly issued payment or credit instruments, stating the express consent of the debtor or obligor to payment and their maturity date. Information related to debts contracted with public or private companies that provide electricity, water, telephone and gas services may not be disclosed, nor debts contracted with higher education institutions pursuant to Laws Nos. 18,591 and 19,287, nor those acquired with banks or financial institutions pursuant to Law No. 20,027, or within the framework of lines of financing to students for higher education studies, administered by the Corporation for Production Development [CORFO, from the Spanish *Corporación de Fomento de la Producción*], nor any debt contracted for the purpose of receiving for itself or for third parties a formal educational service at any level; nor debts contracted with public or private health care providers and related companies, whether

financial institutions, commercial houses or other similar ones, in the framework of an ambulatory, hospital or emergency health care or action, whether these are consultations, procedures, examinations, programs, surgeries or operations; nor debts contracted with highway concessionaires for the use of their infrastructure may be reported.

Entities responsible for the administration of personal databases may not publish or communicate the information referred to in this article, especially the protests and delinquencies contained therein, when they originated during the period of unemployment affecting the debtor.

For these purposes, the Severance Funds Administrator [AFC, from the Spanish *Administradora de Fondos de Cesantía*] will communicate the data of its beneficiaries to the Bulletin of Commercial Information [*Boletín de Informaciones Comerciales*] only as long as their benefits continue to exist in order for the latter to block the information concerning such persons.

Nevertheless, individuals not covered by unemployment insurance shall prove this condition before the Bulletin of Commercial Information, accompanying the legally severance payment issued or, in case of dispute, the certificate of appearance before the Office of Labour Inspection, for the purpose of claiming this right for three months, renewable up to once. In order for such renewal to be effective, an affidavit from the debtor stating that he/she is still unemployed must be attached.

The blocking of data will be free of charge for the debtor.

Blocking of data shall not apply with regard to whomever records annotations in the commercial information system during the year prior to the date of termination of his/her labour relation.

The data controllers shall delete from their records or databases each and every personal information regarding the prescribed obligations, without there being need for a request, court order, or instruction from the data protection authorities.

The entities in charge of administrating the personal databases may not, under any circumstance, signal, or characterisation, state that the individual is somehow benefitted by this law.

Article 18. Limitation of data processing for financial, banking or commercial obligations.

In no case may the data referred to in the preceding article, which relate to an identified or identifiable person, be communicated after five years have elapsed since the respective obligation became due.

Nor may data relating to such obligation continue to be communicated after it has been paid or otherwise legally extinguished.

However, the information required by the courts in connection with pending lawsuits shall be communicated to the courts of justice.

Article 19.- Effects of the extinction of the economic, banking or commercial obligation.

The payment or extinction of these obligations, on whatever the account, does not result in the expiry or loss of legal grounds of the relevant data for the purposes of article 4, for as long as the time spans set forth in the preceding article have not yet elapsed.

In the payment being made, or the obligation being otherwise extinguished by direct intervention of creditor, the latter shall inform this fact, by no later than the seventh business day that follows, to the party in charge of the registry or database accessible to the public who had in due time informed about the protest notice or delinquency, so that the relevant new data may be recorded, after paying the applicable fee, to be borne by debtor. Debtor may choose to directly request the modification of the database and to free creditor from compliance with the obligation of presenting it with sufficient proof of payment; decisions all that shall be stated in writing.

Those carrying out the processing of personal data stemming or collected from the foregoing source accessible to the public shall modify the data in that same sense as soon as the latter informs it about the payment or extinction of the obligation, or within the following three (3) days. Were it impossible for them to do so, they shall block the data of the relevant subject up until the information is updated.

The breach of any of these obligations shall be heard and penalised pursuant to Title VII hereof.

Title IV

Processing of personal data by public bodies

Article 20.- General rule of data processing by public bodies.

The processing of personal data by public bodies is lawful when it is carried out for the fulfillment of their legal functions, within the scope of their competencies, in accordance with the rules established by law, and the provisions set forth in this Title. Under these conditions, public bodies act as data controllers and do not require the consent of the data subject to process his or her personal data.

Article 21.- Principles and rules applicable to the processing of data by public bodies.

The processing of personal data by public bodies is governed by the principles set forth in Article 3 of this law and the general principles governing the State Administration, especially the principles of coordination, probity and efficiency.

Under the principle of coordination, public agencies must achieve high interoperability and consistency to avoid contradictions in the information stored and repetition of information or document requirements to data subjects. In accordance with the principle of efficiency, duplication of procedures and formalities among public agencies and between them and the data subjects must be avoided.

Without prejudice to the other rules set forth in this Title, the provisions set forth in Articles 2°, 14, 14 bis, 14 ter, 14 quater, 14 quinquies, 14 sexies and 15 bis, the articles of the Second and Third Paragraphs of Title II, the articles of Title V and the articles of Title VII of this law are applicable to the processing of data carried out by public bodies. Likewise, Articles 4°, 5°, 6°, 7° and 8° are applicable to it, in accordance with the provisions of Article 23.

Article 22.- Communication or transfer of data by a public body.

Public bodies are entitled to communicate or transfer specific personal data, or all or part of their databases or data sets, to other public bodies, provided that the communication or transfer of the data is necessary for the performance of their statutory functions and both bodies act within the scope of their competences. The communication or transfer of the data must be made for a specific processing and the receiving public body may not use the data for other purposes.

Likewise, personal data or databases may be communicated or transferred between public bodies, exclusively when they are required for a treatment whose purpose is to grant benefits to the data subject, avoid duplication of procedures for citizens or repetition of information or document requirements for the same data subjects.

The public body receiving the data may only keep them for the time necessary to carry out the specific processing for which they were required, after which they must be deleted or anonymized. This data may be stored for a longer period of time when the public body needs to attend to claims or challenges, carry out control or follow-up activities, or serve to guarantee the decisions adopted.

For the purposes of communicating or transferring personal data to private persons or entities, public agencies must have the consent of the data subject, unless the communication or transfer of data is necessary to fulfill the functions of the public agency in terms of control or inspection.

In the case of communication or transfer of personal data pursuant to a request for access to information made in accordance with the provisions of Article 10 of Law No. 20,285, public agencies must have the consent of the data subject obtained in the opportunity provided for in Article 20 of said law.

Regarding the communication of data relating to criminal, civil, administrative and disciplinary offenses, Article 25 provisions shall apply.

Public bodies shall report monthly through their institutional website the agreements entered into with other public bodies and private entities regarding the assignment or transfer of personal data. This obligation shall be supervised by the Agency.

Article 23.- Exercise of the rights of the data subject, administrative procedure for protection and claim of illegality.

The data subject may exercise before the public body the rights of access, rectification and opposition recognized by this law. The data subject may also object to a specific processing when it is contrary to the provisions of this title. The data subject may exercise the right of suppression in the cases provided for in the third paragraph of the preceding article.

Public bodies shall not grant requests for access, rectification, objection, suppression or temporary blocking of personal data in the following cases:

a) When this impedes or hinders the fulfillment of the supervisory, investigative, victim and witness protection or sanctioning functions of the public agency, and

b) When this would affect the secrecy of the information, as established by law.

The exercise of the data subject's rights shall be carried out in accordance with the procedure established in article 11 of this law, addressing the superior head of the service.

The data subject may complain to the Agency when the public body has denied, expressly or tacitly, a request in which he exercises any of the rights recognized by this law. The complaint shall be subject to the rules provided for in the administrative procedure for the protection of rights established in article 41.

Article 24.- Special regimes.

The processing, communication or transfer of personal data, carried out by competent public bodies in the matters indicated below, will be subject exclusively to the special regulation regime established in this article:

a) Those that are carried out for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions, including activities of protection and prevention against threats and risks against public security, and the protection of victims and witnesses, criminal analysis and reportability of criminal information. With respect to data collected for this purpose, the provisions of Article 25 shall not apply.

b) Those in matters directly related to the security of the Nation, national defense and the foreign policy of the country.

c) Those carried out for the exclusive purpose of dealing with an emergency or catastrophe situation, declared in accordance with the law and only while this declaration remains in force.

d) Those that are protected by rules of secrecy, reserve or confidentiality, established in their respective laws. This exception also includes data that, in compliance with a legal obligation, public bodies must transfer to another public body or to third parties, in which case the recipient must process them maintaining the same obligation of secrecy, reserve or confidentiality.

The corresponding public bodies may process, transfer and communicate personal data in a lawful manner, as long as it is done for the fulfillment of their legal functions, within the scope of their competences and respecting the fundamental guarantees established in Article 19, No. 4, of the Political Constitution of the Republic and the principles established in Article 3.

In order to carry out the processing, transfer and communication of data for the purpose set out in letters a), b) and c) above, public bodies and their authorities shall be obliged to exchange information and provide the personal data required of them for these purposes, provided that they refer to processing that is carried out for a specific purpose authorized by law or, when this is not possible, the requirement is a necessary and proportional measure.

The Agency may, after hearing the competent bodies, issue instructions to specify the way to apply the aforementioned guarantees and principles to the aforementioned cases, in order to ensure their safeguarding and allow the due fulfillment of the legal functions of the corresponding bodies.

Article 25.- Data relating to criminal, civil, administrative and disciplinary offences.

Personal data relating to the commission and punishment of criminal, civil, administrative and disciplinary offences may only be processed by public bodies for the fulfilment of their legal functions, within the scope of their competences and in the cases expressly provided for by law.

Communications by State bodies due to the processing of these personal data shall always ensure that the information conveyed or disclosed be accurate, sufficient, current, and complete.

Personal data relating to the commission and conviction of criminal, civil, administrative or disciplinary offences may not be communicated or made public, once the respective criminal, civil, administrative or disciplinary action has expired, or once the penalty or sanction imposed has been served or prescribed, which must be declared or verified by the competent public authority. The foregoing is without prejudice to the incorporation, maintenance and consultation of this information in the records kept by public bodies by express provision of the law, in the manner and for the time provided for in the law that establishes the corresponding specific obligation. Persons who work in public bodies are obliged to maintain secrecy with respect to this information, which must be kept confidential.

When the law provides that information relating to the commission and punishment of criminal, civil, administrative and disciplinary offenses must be made public through its incorporation in a registry of sanctions, or its publication on the website of a public body or in any other means of communication or dissemination, without setting a period of time during which this information must remain available, the following rules shall be followed:

a) With respect to criminal offences, the periods for publicity shall be governed by the specific rules governing this type of offence.

b) With respect to civil, administrative and disciplinary offences, they shall remain accessible to the public for a period of five years.

The massive processing of personal data contained in the electronic records of criminal, civil, administrative and disciplinary offenses kept by public agencies is prohibited. Failure to comply with this prohibition constitutes a very serious offense under this law.

Cases in which the information is requested by the courts of justice or other public bodies for the fulfillment of their legal functions and within the scope of their competence, who shall maintain due confidentiality, shall be exempted from the prohibition of communication.

Notwithstanding the provisions of the third paragraph of this article, personal data relating to the commission and punishment of criminal offenses are of a reserved nature and, except for the legal provisions authorizing their processing, may not be communicated or transferred to third parties by the public agencies that possess them.

Article 26.- Regulations.

The conditions, modalities and instruments for the communication or transfer of personal data between public bodies and with private persons or bodies shall be regulated by a regulation issued by the Ministry of the General Secretariat of the Presidency and signed by the Minister of Finance and the Minister of Economy, Development and Tourism, following a report from

the Agency. This same regulation will regulate the procedures for anonymizing personal data, especially sensitive personal data.

However, these regulations will not be applicable to those transfers in which any of the bodies referred to in Title VIII of this law have participation.

Title V

International transfer of personal data

Article 27.- General rule of authorization.

If the requirements that, in accordance with this law, authorize the processing of data are met, international data transfer operations are lawful in any of the following cases:

a) When the transfer is made to a person, entity or public or private organization, subject to the legal system of a country that provides adequate levels of protection of personal data, in accordance with the provisions of Article 28.

b) When the transfer of data is covered by contractual, binding corporate rules, or other legal instruments signed between the data controller making the transfer and the data controller or third-party data processor receiving it, and they establish adequate guarantees, in accordance with the provisions of Article 28.

c) When the data controller carrying out the transfer and the data controller or third-party data processor receiving it, adopt a compliance model or certification mechanism and establish adequate guarantees, in accordance with Article 28.

In the absence of an adequacy decision or adequate guarantees, a specific and unusual transfer may be made if any of the following are met:

a) When there is express consent from the data subject to carry out a specific and specific international data transfer.

b) When it refers to a specific bank, financial or stock market transfers and that are carried out in accordance with the laws that regulate these transfers.

c) When data must be transferred to comply with obligations acquired in international treaties or conventions that have been ratified by the Chilean State and are in force.

d) When the transfer is necessary by application of cooperation, information exchange or supervision agreements that have been signed by public bodies for the performance of their functions and in the exercise of their powers.

e) When the transfer of data carried out by a natural or legal person, public or private, has been expressly authorized by law and for a specific purpose.

f) When the transfer is made for the purpose of providing or requesting international judicial cooperation.

g) When the transfer is necessary for the conclusion or execution of a contract between the data subject and the controller, or for the execution of pre-contractual measures adopted at the request of the controller.

h) When it is necessary to adopt urgent measures in medical or health matters, for the prevention or diagnosis of diseases, for medical treatment or for the management of health or health services.

Article 28.- Rule for the determination of suitable countries and other rules applicable to the international transfer of data.

It is understood that the legal system of a country has adequate levels of data protection when it complies with similar or higher standards than those set forth in this law. The Agency shall determine the countries that have adequate levels of data protection considering, at least, the following:

a) The establishment of principles that govern the processing of personal data.

b) The existence of rules that recognize and guarantee the rights of data subjects and the existence of a jurisdictional or administrative public authority for control or protection.

c) The imposition of information and security obligations on data controllers and third-party data processors.

d) The determination of responsibilities in the event of infringements.

Will be considered as adequate guarantees those instruments, mechanisms, clauses that contain similar or greater principles, rights and guarantees to those offered by this law, and in particular, that grant enforceable rights and effective legal actions to the data subjects of the data. The Agency may approve model clauses and other legal instruments only if they contain such safeguards for the transborder flow of data, which shall be available to data controllers. Model clauses and other legal instruments providing for adequate safeguards approved by the Agency shall not require any additional safeguards or authorization.

The Agency will make available on its website a list of suitable countries and model contractual clauses and other legal instruments for the international transfer of data.

When the transfer is made between companies or entities that belong to the same business group, related companies or subject to the same controller under the terms provided for in the Securities Market Law, provided that all of them operate under the same standards and policies regarding the processing of personal data, the transfers may be covered by binding corporate rules previously approved by the Agency. The data transferee will be liable for any breach of binding corporate standards and policies by some members of the corporate group. The data controller may only be exonerated from this liability when he proves that the infringement was not attributable to the member of the corresponding business group.

When none of the circumstances indicated in the previous article are verified, the Agency may authorize, by means of a reasoned decision, the international transfer of data for a particular case, provided that the transmitter and receiver of the data provide the appropriate guarantees in relation to the protection of the rights of the persons who are the data subjects of these data and the security of the information transferred, in accordance with this law.

It will be the responsibility of the data controller who carried out the international transfer of data to prove to the Agency that it was carried out in accordance with the rules established in this law.

Article 29.- Inspection.

The Agency will supervise international data transfer operations, being able to make recommendations, adopt conservative measures and, in qualified cases, temporarily suspend the sending of data.

Title VI

Supervisory Authority for the Protection of Personal Data

Article 30.- Personal Data Protection Agency.

It is hereby created the Personal Data Protection Agency, an autonomous corporation under public law, of a technical, decentralized nature, with legal personality and its own assets, which shall be related to the President of the Republic through the Ministry of Economy, Development and Tourism.

The purpose of the Agency shall be to ensure the effective protection of the rights that guarantee the private life of individuals and their personal data, in accordance with the provisions of this law, and to monitor compliance with its provisions.

The address of the Agency shall be fixed in the regulations, without prejudice to the addresses it may establish in other parts of the country.

Article 30 bis.- Functions and powers of the Agency.

The Agency shall have the following functions and powers:

a) To issue general and mandatory instructions and rules in order to regulate personal data processing operations in accordance with the principles established in this law. The instructions and general rules issued by the Agency shall be issued after public consultation through the institutional web page and shall be strictly related to the regulation of the processing of personal data and which is necessary for the faithful compliance with this law, providing the necessary mechanisms so that the interested parties can make observations on it.

b) To administratively apply and interpret the legal and regulatory provisions on the protection of personal data and the instructions and general rules issued by the Agency.

c) To supervise compliance with the provisions of this law, its regulations and the instructions and general rules issued with respect to the processing of personal data. For this purpose, it may require those who process personal data to deliver any document, book or record and all the information that may be necessary for the fulfillment of its auditing function.

d) To determine the infractions and non-compliances incurred by those who process personal data, in their data processing operations, with respect to the principles and obligations established in this law, its regulations and the instructions and general rules issued by the Agency. For such purposes, and in a well-founded manner, it may summon to testify, among others, the data subject, the legal representatives, administrators, advisors and dependents of the person who processes personal data, as well as any person who has had participation or knowledge regarding any fact that is relevant to resolve a sanctioning procedure. Likewise, it may take the respective statements by other means that ensure their fidelity.

e) To exercise the sanctioning power over natural or legal persons who process personal data in breach of this law, its regulations and general instructions and rules issued by the Agency, applying the sanctions established in this law.

f) To resolve requests and claims made by data subjects against those who process personal data in breach of this law, its regulations or the instructions and general rules issued by the Agency.

g) To develop programs, projects and actions for dissemination, promotion and information to the citizens in relation to respect for the protection of their personal data.

h) To propose to the President of the Republic and the National Congress, where appropriate, the legal and regulatory rules to ensure individuals the due protection of their personal data and to perfect the regulation on the processing and use of this information.

i) To provide technical assistance, when required, to the National Congress, the Judiciary, the Comptroller General of the Republic, the Criminal Prosecutor's Office, the Constitutional Court, the Central Bank, the Electoral Service, the Electoral Justice and other special courts created by law, in the issuance and implementation of the internal policies and rules of these bodies; in order for its operations and personal data processing activities are carried out in accordance with the principles and obligations established in this law.

j) To interact and collaborate with public bodies in the design and implementation of policies and actions aimed at ensuring the protection of personal data and their correct processing.

k) To enter into cooperation and collaboration agreements with public or private, national, foreign or international entities, with competence or related to the field of personal data. In the case of signing agreements with international public entities, prior consultation with the Ministry of Foreign Affairs will be required, in accordance with the provisions of Article 35 of Law No. 21,080.

l) To participate, receive cooperation and collaborate with international organizations in matters of personal data protection.

m) To certify, register and supervise infringement prevention models and compliance programs and to manage the National Registry of Sanctions and Compliance.

n) To exercise the other functions and powers entrusted to it by law.

If an agency of the Administration is required to exercise the functions or powers granted to the Agency, it shall comply with the provisions of the second paragraph of Article 14 of Law No. 19,880.

Article 30 ter.- Management of the Agency.

The superior management of the Agency shall correspond to the Board of Directors of the Agency, which shall have the following functions and attributions:

a) To exercise the attributions and fulfil the functions entrusted to the Agency.

b) To establish internal regulations for the operation of the Agency for the fulfillment of the functions entrusted by law.

c) To establish policies for the planning, organization, direction, supervision, coordination and control of the Agency's operation, as well as those for the administration, acquisition and disposal of assets.

d) To issue general rules, newsletters, circular letters and other resolutions that are required.

e) To formulate to the President of the Republic or to the National Congress the proposals for the reform of legal and regulatory rules.

f) To prepare, within the first four months period of each year, an annual public account detailing the work carried out by the Agency in the immediately preceding year.

Article 30 quarter.- Members of the Directive Council of the Agency.

The Board of Directors of the Agency shall be composed of three counselors, appointed by the President of the Republic, with the agreement of the Senate, adopted by two-thirds of its members in office.

For the purposes of their appointment, the President of the Republic shall propose the corresponding list, and the Senate shall decide on the proposal.

The candidates for director must be people of recognized professional or academic prestige in matters of personal data protection.

The Agency's Board of Directors shall appoint its President and Vice-President from among its members, in accordance with the provisions of the Agency's statutes. The offices of president and vice-president shall last for three years or the time remaining as councilors in each case.

The directors shall hold office for a term of six years, may not be appointed for a new term and shall be renewed individually, every two years.

The position of director of the Agency's Board of Directors requires exclusive dedication.

The Agency's Board of Directors shall adopt its decisions by a majority of its members and, in the event of a tie, its chairman, or its vice-chairman in the event of the latter's absence. The minimum quorum for a session will be two directors. The regulations shall establish the other rules necessary for their operation.

The Board of Directors of the Agency shall hold ordinary sessions at least once a week, and extraordinary sessions when specially convened by its chairman himself or at the written request of two directors, in the manner and under the conditions determined by its internal operating regulations. The president may not refuse to issue the indicated summons, and the respective session must take place within two working days following the indicated request.

Article 30 quinquies.- Disqualifications and incompatibilities.

The position of director is incompatible with the performance of any position or service, whether remunerated or not, rendered in the private sector. Likewise, it is incompatible with the status of member of the management bodies of political parties, officials of the State Administration, and of any employment or service remunerated with fiscal or municipal funds, and with the functions, remunerated or not, of director, director or worker of institutions, national or foreign autonomous organizations, State companies and, in general, of any public

service created by law, as well as of companies, corporations or public or private entities in which the State, its companies, corporations or centralized or decentralized institutions, have contributions of majority capital or in equal proportion or, under the same conditions, representation or participation. Likewise, it is incompatible with any other paid or free service or employment in any branch of the State.

The position of director is compatible with the performance of teaching positions in public or private institutions recognized by the State, up to a maximum of twelve hours per week.

The spouse or civil partner of any of the directors and their relatives up to and including the second degree of consanguinity, may not be a director or have a share in the data subject ship of a company whose purpose or business line is related to the collection, processing or communication of personal data.

Additionally, they may not be appointed as a director:

a) An individual who has been convicted of a crime punishable by imprisonment or perpetual disqualification from holding public office or positions, for crimes of legal prevarication, bribery and those committed in the exercise of public office, tax crimes and crimes against public faith.

b) An individual who is dependent on illegal narcotic or psychotropic substances or drugs, save when justifying their use by medical treatment.

c) An individual who has been sanctioned, within the last five years, for serious or very serious infringement of the rules governing the processing of personal data and its protection.

d) Those who, within the last year, have been managers, data delegates, directors or have had a stake in the data subjectship of a company whose purpose or business line is related to the processing of personal data.

In all matters not expressly regulated in this article, the rules of Paragraph 2 of Title III of Decree with the force of law No. 1-19,653, of 2000, of the Ministry of the General Secretariat of the Presidency, which establishes the consolidated, coordinated and systematized text of Law No. 18,575, Constitutional Organization of General Bases of the State Administration, shall apply.

Article 30 sexies.- Removal of directors and grounds for dismissal.

The councilors shall be removed by the Supreme Court, at the request of the President of the Republic or of the Chamber of Deputies by resolution adopted by a simple majority, or at the request of fifteen deputies, for incapacity, misbehavior or manifest negligence in the exercise of their functions. The Supreme Court shall hear the matter in a plenary session specially convened for this purpose and in order to agree on the removal it shall gather the concurring vote of the majority of its members in office.

In addition to removal, the following shall be grounds for dismissal from the office of director:

a) Expiration of the term for which he/she was appointed.

b) Resignation before the President of the Republic.

c) Nomination for a popularly elected office.

d) Supervening inability or incompatibility, which circumstance shall be qualified by the majority of the directors to the exclusion of the affected person.

In the event that one or more directors cease for any reason, a new director shall be appointed, by means of a proposal by the President of the Republic, subject to the same procedure provided for in Article 30 quarter, for the remainder of the term.

If the director who leaves office by virtue of this Article is the President or Vice-President of the Board of Directors of the Agency, his replacement shall be appointed in the manner provided for in Article 30 quarter, for the time remaining from the time that the vacancy occurred.

Article 30 septies.- Remuneration.

The Chairman of the Board of Directors of the Agency shall receive a gross monthly remuneration equivalent to that of an Undersecretary of State and shall be responsible for exercising the functions indicated in Article 30h and in the other pertinent legal provisions.

The other directors will receive a remuneration equivalent to 85% of the remuneration corresponding to the Chairman of the Board of Directors of the Agency.

Article 30 octies.- Agency Statutes.

The statutes of the Agency shall establish its rules of operation. The statutes and their modifications shall be proposed by the Agency to the President of the Republic and their approval shall be provided by means of a supreme decree issued through the Ministry of Economy, Development and Tourism.

Article 30 nonies.- Functions and powers of the Chairman of the Board of Directors of the Agency.

The Chairman of the Agency's Board of Directors shall be the Agency's head of service and shall have the judicial and extrajudicial representation of the Agency. It will be responsible for the organization and administration of the Agency and shall be responsible for exercising hierarchical supervision and control of the actions of the Agency's staff.

The Chairman of the Agency's Board of Directors shall be responsible for the following functions and attributions:

a) To exercise the role of head of service.

b) To execute and comply with the rules and agreements adopted by the Agency's Board of Directors.

c) To convene and preside over the meetings of the Agency's Board of Directors, as well as to establish the table of matters to be dealt with at each meeting.

d) To represent the Agency legally, judicially and extrajudicially.

e) To issue the internal regulations necessary for the proper functioning of the Agency's Board of Directors, with the prior agreement of the Agency's Board of Directors, ensuring compliance with the rules applicable to the Agency.

f) To hire the Agency's staff and terminate their services, in accordance with the law.

g) To execute the acts and enter into the agreements necessary for the fulfilment of the purposes of the Agency's Board of Directors.

h) To delegate specific attributions or faculties to officials of the Agency.

i) To conduct the Agency's relations with public bodies and other State bodies and with the persons or entities subject to its supervision, as well as with the international regulatory entities of personal data.

j) To exercise the other functions delegated to it by the Agency's Board of Directors.

The Vice-President of the Agency's Management Board shall assume the functions and powers of the Chairperson of the Agency's Management Board in the event of the latter's absence.

Article 31.- Regulatory coordination with the Transparency Council.

When the Agency must issue an instruction or rule of a general and mandatory nature that may have effects in the areas of competence of the Transparency Council [CPLT, from Spanish *Consejo para la Transparencia*], in accordance with the functions and powers indicated in Law No. 20,285, it shall send it all the background information and shall request a report from the latter in order to avoid or prevent potential conflicts of rules and ensure coordination, cooperation and collaboration between both bodies.

The Transparency Council shall issue the requested report within thirty calendar days from the date of receipt of the request referred to in the preceding paragraph.

The Agency shall consider the content of the opinion of the Transparency Council by expressing it in the reasons for the instruction or rule it issues. Once the term has elapsed without the report having been received, it shall be in accordance with the second paragraph of Article 38 of Law No. 19,880.

In turn, when the Transparency Council must issue a general instruction that has clear effects in the areas of competence of the Agency, in accordance with the functions and powers indicated in this law, the Transparency Council shall send the background information and request a report from the Agency, which shall issue it within thirty calendar days counted from the date on which the request was received. The Transparency Council shall consider the content of the Agency's opinion, expressing it in the reasons for the general instruction issued for this purpose. Once the term has elapsed without the report having been received, it shall proceed in accordance with the second paragraph of Article 38 of Law No. 19,880.

Article 32.- Agency staff and supervision.

Individuals rendering services to the Agency shall be governed by the Chilean Labour Code.

Notwithstanding the foregoing, the standards of probity established in Law No. 20,880 on probity in the public service and prevention of conflicts of interest and in Title III of Decree

No. 1-19,653 of 2000 of the Ministry of the General Secretariat of the Presidency, which establishes the consolidated text, shall be applicable to these personnel, coordinated and systematized of Law No. 18,575, Constitutional Organic Law of General Bases of the State Administration, and a clause must be recorded in the respective contracts that so provides.

The persons who perform managerial functions in the Agency shall be selected through a public competition carried out by the National Civil Service Office, on the basis of a shortlist formed by the Senior Public Management Council for each case, in accordance with the rules that regulate the selection processes of the Senior Public Management according to Law No. 19,882.

In the event that third parties exercise, against the Agency's directors or staff for formal acts or for actions or omissions occurring in the exercise of their duties, the Agency shall provide them with legal defense. This defense shall be extended to all those actions that are initiated against him/her even after he has ceased to hold office.

The defense referred to in the preceding paragraph shall not be applicable in those cases in which the formal acts, actions, or omissions in question have constituted a cause for termination attributable to the conduct of the respective official.

The Agency shall comply with the rules established in Decree Law No. 1,263 of 1975 on State Financial Administration.

Likewise, the Agency shall be subject to the control of the Office of the Comptroller General of the Republic, as regards its personnel and the examination and judgment of its accounts.

The resolutions of the Agency shall be exempt from the process of acknowledgment by the Office of the Comptroller General of the Republic.

Article 32 bis. Assets.

The Agency's assets shall be formed by:

a) Contribution that is contemplated annually in the Public Sector Budget Law.

b) Movable and immovable property that may be transferred to it or that it acquires under any title and for the fruits received from it.

c) Donations accepted by the Agency. Donations shall not require the judicial insinuation procedure referred to in Article 1401 of the Civil Code.

d) The inheritances and legacies that the Agency accepts, which must always be done with the benefit of inventory. Such allowances shall be exempt from all kinds of taxes and from any levy or payment affecting them.

e) The contributions of international cooperation.

Title VII

Infringements and their penalties, procedures and responsibilities

Article 33.- General liability regime.

The data controller, whether a natural or legal person, under public or private law, who in its personal data processing operations infringes the principles indicated in Article 3, and the rights and obligations established in this law, shall be sanctioned in accordance with the rules of this Title.

First Paragraph

Liability, infringements and penalties applicable to natural or legal persons under private law

Article 34.- Minor, serious and very serious infractions.

The infractions committed by data controllers to the principles established in Article 3, rights and obligations established in this law are classified, considering their seriousness, as minor, serious and very serious.

The responsibilities incurred by a natural or legal person for the infractions established in this law are without prejudice to the other legal, civil or criminal responsibilities that may correspond to them.

Article 34 bis.- Minor infractions.

The following are considered minor infractions:

a) Total or partial breach of the duty of information and transparency, established in Article 14 ter.

b) Lack of an updated and operative postal address, e-mail or equivalent electronic means of communication with the data controller or its legal representative, through which data subjects may address their communications or exercise their rights

c) Failure to respond, incomplete or untimely response to requests made by the data subject pursuant to this law.

d) Failure to send to the Agency any communication mandatory under this law or its regulations.

e) Failure to comply with the general instructions issued by the Agency when they are not penalized as a major or very major infringement.

f) Commit any other infringement against the rights and obligations established in this law, not classified as a major or very major infringement.

Article 34 ter.- Serious infractions.

The following are considered serious infringements:

a) Process personal data in the absence of the consent of the data subject or without a background or legal basis that makes the processing lawful, or to process them for a purpose other than that of their collection.

b) Communicate or transfer personal data, in the absence of the consent of the data subject, in cases where such consent is necessary, or communicate or transfer the data for a purpose other than the authorized.

c) Process unnecessary personal data in relation to the purposes of the processing in violation of the provisions of paragraph c) of article 3°.

d) Process inaccurate, incomplete or outdated personal data in relation to the purposes of the processing, save that the updating of this data is incumbent upon the data subject by virtue of the law or contract.

e) Prevent or hinder the legitimate exercise of rights of access, rectification, deletion, opposition or portability of data subjects.

f) Omitting to respond, responding late or denying the request without just cause, in cases of well-founded requests for temporary blocking of the processing of personal data of a data subject.

g) Process personal data of children and adolescents in violation of the rules set forth in this law.

h) Process personal data in breach of the requirements established for non-profit legal entities under private law and whose purpose is political, philosophical, religious, cultural, union or association, with respect to the data of its associates.

i) Infringe the duty of secrecy or confidentiality established in article 14 bis.

j) Infringe or breach the security obligations in the processing of personal data set forth in Article 14 quinquies.

k) Omit communications or records in cases of breach of the security measures set forth in Article 14 quinquies.

l) Adopt insufficient or unsuitable quality and security measures for the processing of personal data for historical, statistical or scientific purposes and for studies or research in the public interest.

m) Carry out international data transfer operations in contravention of the rules set forth in this law.

n) Failure to comply with a resolution or a specific and direct requirement issued by the Agency.

Article 34 quarter.- Very serious infringements.

The following are considered to be very serious infringements:

a) Process personal data in a fraudulent manner.

b) Maliciously use of personal data for a purpose other than the purpose consented to by the data subject or provided for in the law authorizing its processing.

c) Knowingly communicate or transfer untrue, incomplete, inaccurate or outdated information regarding the data subject.

d) Violate the duty of secrecy or confidentiality regarding sensitive personal data and personal data related to the commission and punishment of criminal, civil, administrative and disciplinary offenses.

e) To knowingly treat, communicate or transfer sensitive personal data or personal data of children and adolescents, in contravention of the provisions of this law.

f) Deliberately omitting to report breaches of security measures that may affect the confidentiality, availability or integrity of personal data.

g) Carrying out massive processing of personal data contained in electronic records of criminal, civil, administrative and disciplinary offenses kept by public agencies, without having legal authorization to do so.

h) Knowingly carrying out international data transfer operations in contravention of the provisions of this law.

i) Failure to comply with a resolution of the Agency that resolves the claim of a data subject on the exercise of his rights of access, rectification, suppression, opposition, portability or temporary blocking of his data

j) To knowingly deliver false, incomplete or manifestly erroneous information in the process of registration or certification of the infringement prevention model.

k) Failure to comply with the obligation established in Article 15 ter, in the appropriate cases.

Article 35.- Sanctions.

The penalties for infringements incurred by data controllers will be as follows:

a) Minor infractions will be punished with a written warning or a fine of up to 5,000 monthly tax units per month (UTM).

b) Serious infractions will be punished with a fine of up to 10,000 monthly tax units (UTM).

c) Very serious infractions shall be punishable by a fine of up to 20,000 tax units per month (UTM).

In each case, the Agency will indicate the measures aimed at correcting the causes that gave rise to the sanction, which must be adopted within a period of no more than sixty (60) days, otherwise a surcharge of 50% will be imposed on the fine issued, without prejudice to the provisions of Article 49. In the event of a repeat offense, in accordance with paragraph a) of the second paragraph of Article 36, the Agency may apply a fine of up to three times the amount assigned to the infraction committed.

If the offender corresponds to a company other than those defined as smaller companies in the second article of Law No. 20,416, which reoffends in an infraction of a serious or very serious nature in the terms of letter a) of the second paragraph of article 36, the fine may reach the most onerous among those indicated in the previous paragraph or up to the amount corresponding to 2% or 4% of the annual income from sales and services and other activities of the line of business in the last calendar year, depending on whether they are serious or very serious infractions, respectively.

Article 36.- Mitigating and aggravating circumstances of responsibility.

The following will be considered mitigating circumstances:

1) The unilateral actions of reparation carried out by the data controller and the reparation agreements agreed with the data subjects who were affected.

2) The cooperation that the offender provides in the administrative investigation carried out by the Agency.

3) The absence of prior sanctions from the data controller.

4) Self-reporting to the Agency. Along with the self-report, the offender must communicate the measures adopted to cease the events that gave rise to the infraction, or the mitigation measures implemented, as appropriate.

5) To have diligently fulfilled their duties of management and supervision for the protection of the personal data subject to processing, which will be verified with the certificate issued in accordance with the provisions of Article 51.

The following will be considered aggravating circumstances:

a) Recidivism. Recidivism occurs when the data controller has been sanctioned on two or more occasions, in the last thirty months, for infringement of this law. The resolutions applying the respective sanctions must be final or enforceable.

b) The continuous nature of the infringement.

c) Having jeopardized the security of the rights and freedoms of the data subjects in relation to their personal data.

Article 37.- Determination of the amount of fines.

In order to determine the amount of the fines indicated in this law, the Agency shall prudently apply the following criteria:

1. The seriousness of the conduct.

2. If the conduct was carried out with a lack of diligence or care in those cases where these elements are not considered in the configuration of the infraction.

3. The damage caused by the infringement, especially the number of data subjects that were affected.

4. The economic benefit obtained as a result of the infringement, if any.

5. If the processing carried out includes sensitive personal data or personal data of children and adolescents.

6. The economic capacity of the offender.

7. Sanctions previously applied by the Agency in the same circumstances.

8. The mitigating and aggravating circumstances that concur.

In the event that a conduct gives rise to two or more infringements, or when one infringement is a means to commit another, a single fine will be imposed, always considering the sanction

of the most serious infringement. In the event of two or more infringing conducts, independent of each other, the penalties corresponding to each of them shall be accumulated.

The fines must be paid to the General Treasury of the Republic [TGR, from the Spanish *Tesorería General de la Republica]*, through the face-to-face or digital means that it disposes, within a period of ten working days from the date the Agency's resolution is final. The corresponding proof of payment must be submitted to the Agency within ten working days from the date of payment.

When for the same facts and legal grounds, the offender could be sanctioned under this law and under one or more other laws of the possible sanctions, the most serious shall be imposed.

Article 38.- Accessory sanctions.

In the event that fines are imposed for repeated very serious infringements, within a period of twenty-four months, the Agency may order the suspension of the data processing operations and activities carried out by the data controller, for a period of up to thirty days. This suspension will not affect the storage of data by the controller.

The suspension ordered by the Agency as an accessory sanction may be partial or total and may not be decreed when it affects the rights of the data subjects.

During this period the data controller must adopt the necessary measures in order to adapt its operations and activities to the requirements set forth in the resolution that ordered the suspension.

If the data controller does not comply with the provisions of the temporary suspension resolution, this measure may be extended indefinitely, for successive periods of a maximum of thirty days, until the data controller complies with the order.

When the suspension affects an entity subject to supervision by a public supervisory body, the Agency must inform the corresponding regulatory authority to protect the rights of the users of such entity.

Article 39.- National Registry of Sanctions and Compliance.

The National Registry of Sanctions and Compliance, administered by the Agency, is hereby created. The register will be public, and access will be free. It will be consulted and kept in electronic form.

In this registry, data controllers who have been sanctioned for infringing the rights and obligations established in this law must be recorded. A distinction should be made according to the seriousness of the infringement. In addition, the infringed conduct, the mitigating and aggravating circumstances of responsibility and the sanction imposed must be recorded. Those responsible for adopting certified models for the prevention of infringements, with a current character, must also be listed.

The entries in the register will be publicly accessible for five years, starting from the date the entry was made.

Article 40.- Statute of limitations.

Actions to pursue liability for the infractions provided for in this law are time-barred within four years from the event that gave rise to the infraction.

In the event of continuous infringements, the limitation period for the aforementioned actions will be counted from the day on which the infringement has ceased.

The statute of limitations is interrupted with the notification of the initiation of the corresponding administrative procedure.

The penalties imposed for an infringement of this law are time-barred within three years from the date on which the resolution imposing the sanction becomes enforceable.

Second Paragraph

Administrative procedures

Article 41.- Administrative procedure for the protection of rights.

The data subject may complain to the Agency when the data controller has denied a request made in accordance with article 11 of the present law or has not responded to such request within the legal term established in that article.

The claim submitted shall be processed in accordance with the following rules:

a) It must be filed in writing, in physical or electronic format within fifteen working days from the receipt of the negative response from the data controller or the expiration of the term available to the data controller to respond to the request made by the data subject. The complaint must state the decision challenged in the case of rejection or failure to respond and include all the background information on which it is based and indicate a postal address or an e-mail address or other equivalent electronic means where notifications will be made.

b) Together with the filing of the claim, at the data subject's justified request and only in justified cases, the Agency may suspend the processing of the personal data concerning the data subject and which are the object of the claim, having previously heard the data controller.

c) Once the claim has been received, the Agency, within the following ten working days, shall determine whether it complies with the requirements set forth in letter a) in order to be accepted for processing. In the event that the claim is not accepted for processing, the Agency's decision must be reasoned and shall be notified to the data subject. In any case, it shall be understood that the claim has been accepted for processing if the Agency does not make a decision within the term indicated above.

d) Once the claim has been accepted for processing, the Agency shall notify the data controller, who shall have a term of thirty calendar days, extendable up to the same term, to respond to the claim, attaching all the background information it deems pertinent. The notifications to be made to the data controller shall be sent to its postal address, e-mail address or other equivalent electronic means referred to in letter c) of article 14 ter.

e) Once this term has expired, whether or not the data controller has replied, and only if there are substantial, pertinent and controversial facts, the Agency may open an evidentiary term of ten working days in which the parties may present all the means of proof they deem convenient.

f) In its response, the data controller may accept the claim, in which case it must include the background information or testimonies that prove this circumstance. Once the above is verified, the data subject will be notified and will have ten days to assert his rights. Once the term has expired, the Agency shall proceed to file the records, prior application of the sanction or instruction to the data controller, when applicable.

g) The Agency shall have broad powers to request background information or reports that may contribute to its resolution. It may summon the parties to a hearing and urge them to reach an agreement. The opinions expressed by the Agency's officials at this hearing shall not disqualify them from continuing to hear the matter if an agreement is not reached. Once an agreement has been reached, the records shall be filed.

h) The resolution of the claim must be issued by the Agency and must be reasoned. The administrative procedure for the protection of rights may not exceed six months.

i) The resolution of the Agency that does not accept a claim for processing and the resolution that resolves the claim may be judicially challenged within a term of fifteen working days from its notification, through the procedure established in article 43.

Complaints and requests for suspension of processing made in the event of refusal of a request for temporary blocking must be resolved by the Agency within a maximum of three working days, without the need to hear the parties beforehand.

Article 42.- Administrative procedure for violation of law.

The determination of the infractions committed by data controllers for non-compliance or violation of the principles set forth in article 3°, rights and obligations established in this law and the application of the corresponding sanctions, shall be subject to the following special rules:

a) The sanctioning procedure shall be instructed by the Agency.

b) The Agency may initiate a sanctioning procedure, ex officio or at the request of a party, as a result of an inspection process or as a consequence of a claim filed by a data subject, by virtue of the procedure established in articles 23 and 41 of this law. In the latter case, the receipt of the complaint must be certified. Together with the opening of the file, the Agency shall designate an official responsible for the investigation of the procedure.

c) The Agency shall file a formulation of charges against the data controller describing the facts constituting the infringement, the principles and obligations breached or violated by the data controller, the legal norms infringed and any other background that may serve to support the formulation.

d) The data controller must be notified of the filing of the charges to its postal address, e-mail address or other equivalent electronic means indicated in letter c) of article 14 ter.

e) The data controller shall have a period of fifteen working days to present his or her defense. In that opportunity, the data controller may attach all the background information it deems pertinent to discredit the alleged facts. Together with the disclaimers, the data controller shall establish an e-mail address through which all other communications and notifications shall be made.

f) Upon receipt of the releases or once the term granted for such purpose has elapsed, the Agency may open a ten-day evidentiary term in the event that there are substantial, pertinent and controversial facts.

g) The Agency shall give place to the measures or evidentiary diligences requested by the data controller in its discharges, provided that they are pertinent and necessary. In the event of rejection, the Agency shall justify its decision.

h) The facts investigated, and the responsibilities of the alleged infringers may be accredited by any means of evidence admissible in law, which shall be assessed according to the rules of sound criticism.

i) The Agency shall have broad powers to request background information or reports that contribute to its resolution.

j) The resolution that puts an end to the sanctioning procedure must be reasoned and resolve all the issues raised in the file, ruling on each of the allegations and defenses made by the data controller and will contain the declaration of having configured the breach or violation of the principles, rights and obligations established in the law by the data controller or his acquittal, as the case may be. In the event that the Agency considers that the infringement has been verified, in the same resolution it shall weigh the circumstances that aggravate or attenuate the responsibility of the infringer and shall impose the sanction, according to the seriousness of the infringement committed.

k) The resolution that establishes the non-compliance or violation of the principles, rights and obligations of this law and applies the corresponding sanction must be reasoned. This resolution must indicate the administrative and judicial remedies that may proceed against it in accordance with this law, the bodies before which they must be presented and the time limits for their interposition. The resolution of the Agency that resolves the procedure for infringement of the law shall be subject to judicial appeal in accordance with the following article.

l) The administrative procedure for infringement of the law may not exceed six months. When more than six months have elapsed from the date of the certification indicated in letter b) of this article without the Agency having resolved the claim, the interested party may file a claim of illegality under the terms provided for in the following article.

Third Paragraph

Judicial complaint procedure

Article 43.- Judicial claim procedure.

The interested natural or juridical persons who consider that an administrative act that paralyzes the procedure, or a final or terminating resolution emanating from the Agency, is illegal, may file a claim of illegality before the Court of Appeals of Santiago or that of the place where the claimant is domiciled, at the choice of the latter. The claim must be filed within fifteen working days following the notification of the challenged resolution, according to the following rules:

a) The claimant shall state in its brief, with precision, the resolution that is the object of the claim, the legal norm or norms that are supposed to have been infringed, the manner in which the infringement has occurred, and when applicable, the reasons why the act causes him grievance.

b) The Court may declare the claim inadmissible if the written statement does not comply with the conditions set forth in letter a) above. Likewise, it may decree an order not to innovate when the execution of the challenged act would cause irreparable damage to the appellant.

c) Once the claim has been received, the Court shall request a report from the Agency, granting it a term of ten days for such a purpose.

d) Once the report has been served or if it is deemed to have been served in absentia, the Court may open a period of evidence, if it deems it necessary, which shall be governed by the rules of the incidents contemplated in the Code of Civil Procedure.

e) Once the term of proof has expired, the case shall be ordered to be brought in relation. The hearing of this case shall be given preference for inclusion in the table.

f) If the Court upholds the claim, in its judgment it shall decide whether there was a grievance and shall order, as appropriate, the rectification of the challenged act and the issuance of the respective resolution, as the case may be.

g) In the case of claims against a resolution that resolves a sanctioning procedure, the Court may confirm or revoke the challenged resolution, establish or dismiss the commission of the infraction, as the case may be, and maintain, leave without effect or modify the sanction imposed on the responsible party or his acquittal, as the case may be.

h) In all matters not regulated by this Article, the rules set forth in the Organic Code of Courts and the Code of Civil Procedure, as applicable, shall apply.

Fourth Paragraph

Responsibility of public bodies, of the authority or superior head of the body and of its officials

Article 44.- Administrative responsibility of the superior head of the public body.

The superior head of a public body shall ensure that the respective body carries out its personal data processing operations and activities in accordance with the principles, rights and obligations set forth in Title IV of this law.

Likewise, public bodies shall submit to the measures tending to remedy or prevent breaches indicated by the Agency or to the compliance or breach prevention programs of Article 49.

Violations of the principles set forth in article 3°, rights and obligations that may be incurred by public bodies are typified in articles 34 bis, 34 ter and 34 quater and shall be punishable by a fine of twenty percent to fifty percent of the monthly remuneration of the superior head of the offending public body. The amount of the fine will be determined considering the seriousness of the infringement, the nature of the data processed, and the number of data

subjects affected. In determining the penalty, consideration shall also be given to the circumstances that mitigate the offender's liability.

If the public body persists in the infringement, the superior head of the public body shall be subject to double the original sanction imposed and suspension from office for a period of five days.

In the case of sensitive personal data, the fine shall be 50% of the monthly remuneration of the senior manager of the public body and the suspension from office for up to thirty days.

The infringements incurred by a public body in the processing of personal data shall be determined by the Agency in accordance with the procedure established in article 42.

Once the infringement has been established, the administrative sanctions set forth in this article shall be applied by the Agency. However, the Office of the Comptroller General of the Republic (CGR, from Spanish *Contraloría General de la República*), at the request of the Agency, may, in accordance with the provisions of its organic law, initiate administrative proceedings and propose the corresponding sanctions.

The claim of illegality established in article 43 may be filed against the resolutions of the Agency.

The sanctions provided for in this article shall be published on the website of the Agency and of the respective body or service within five working days from the date on which the respective resolution becomes final.

Article 45.- Liability of the offending official.

Without prejudice to the provisions of the preceding article, if in the corresponding administrative procedure it is determined that there are individual responsibilities of one or more officials of the public body, the Office of the Comptroller General of the Republic, at the request of the Agency, shall initiate a summary investigation to determine the responsibilities of such officials or shall do so in the administrative procedure already initiated, as the case may be. Penalties to the offending officials shall be determined in accordance with the provisions of the Administrative Statute.

In the event that the corresponding administrative procedure determines that any of the officials involved is responsible for any of the very serious infractions indicated in article 34 quater of this law, this conduct shall be considered a serious contravention of administrative probity.

Article 46.- Duty of officials to reserve and confidentiality.

Officials of public bodies that process personal data and especially when it refers to sensitive personal data or data relating to the commission and punishment of criminal, civil, administrative and disciplinary offenses, must keep secret or confidential the information they become aware of in the exercise of their duties and refrain from using such information for a purpose other than that which corresponds to the legal functions of the respective public body or use it for their own benefit or for the benefit of third parties. For the purposes of the provisions of the second paragraph of article 125 of the Administrative Statute, it shall be deemed that the facts that constitute violations of this provision seriously violate the principle

of administrative probity, without prejudice to the other sanctions and responsibilities that may apply.

When, in compliance with a legal obligation, a public body communicates or transfers to another public body data protected by secrecy or confidentiality rules, the receiving public body and its officials shall treat them with the same obligation of secrecy or confidentiality.

Fifth Paragraph

Civil liability.

Article 47.- General rule.

The data controller must compensate the material and non-material damage caused to the data subject(s), in case, within its data processing operations, it violates the principles established in Article 3, rights and obligations provided for in this law and cause them any harm. The foregoing does not prevent the exercise of the other rights granted by this law to the data subject(s).

The compensatory action referred to in the preceding paragraph may be filed upon enforcement of the decision that favorably resolved the claim filed before the Agency, or, a final and enforceable judicial decision has been reached, in the event of a filed complaint on illegality, and shall be processed in accordance with the rules of summary procedure established in Articles 680 et seq. of the Code of Civil Procedure.

Civil actions arising from an infringement of this law shall be subject to the statute of limitations of five years as from the date on which the administrative decision or court sentence, as the case may be, imposing the respective fine has been executed.

Article 48.- Prevention of infractions.

Data controllers, whether natural or corporate entities, either governmental or private, shall adopt actions aimed to preventing the commission of the infringements established in Articles 34 bis, 34 ter and 34 quarter.

Article 49.- Infringement prevention model.

Data controllers may voluntarily adopt an infringement prevention model consisting of a compliance program.

The compliance program must contain, the following elements:

a) Appointment of a personal data protection officer.

b) Establishment of the means and powers of the data protection officer.

c) The identification of the type of information that the entity processes, the territorial scope in which it operates, the category, class or types of data or databases that it manages, and the characterization of the data subjects.

d) The identification of the activities or processes of the entity, whether habitual or sporadic, which in the context of their execution, trigger or increase h the risk of committing the infringements indicated in Articles 34 bis, 34 ter and 34 quarter is generated or increased.

e) The establishment of protocols, rules and specific procedures that allow the individuals involved in the activities or processes referred in the previous paragraph to organize and execute their tasks or duties in a manner that prevents the commission of the aforementioned infractions.

f) Internal reporting mechanisms on compliance with the provisions of this law, and reporting mechanisms to the Data Protection Authority in the case of article 14 sexies.

g) The existence of internal administrative sanctions, as well as procedures for reporting or punishing persons who fail to comply with the infringement prevention system.

The internal regulationresulting from the implementation of the program , where appropriate, must be expressly included as an obligation in the employment or service contracts of all workers, employees and service providers of the entities acting as data controllers or the third parties that carry out the processing, including their top executives , or as an obligation of the internal regulations referred to in articles 153 et seq. of the [Chilean] Labor Code. For the latter case, the publicity measures established in Article 156 of the same Code must be carried out.

Article 50.- Powers of the Officer.

The data controller may appoint a personal data protection officer.

The data protection officer must be appointed by the highest directive or administrative authority of the data controller. The board of directors, a managing partner or the highest authority of the company or service, as applicable, shall be considered as the highest managerial or administrative authority.

The data protection officer must have autonomy from the administration in matters related to this law. In micro, small and medium-sized enterprises, the owner or its highest authorities may personally assume the tasks of data protection officer.

The data protection officer may perform other functions and tasks, seeking to maintain independence in their function. The data controller shall ensure that such functions and tasks do not give rise to a conflict of interest.

Companies or legal entities that belong to a same corporate group, affiliates, or companies subject to a same controller, according to the terms provided in the Securities Market Law, may appoint a sole data protection officer; provided all said companies operate under the same standards and policies in terms of personal data processing, and the officer is accessible to all entities and establishments.

The appointment of the data protection officer shall fall on a person who meets the requirements of suitability, capacity and specific knowledge for the exercise of their duties.

Data subjects may contact the Data Protection Officer regarding all matters relating to the processing of their personal data and the exercise of their rights under this law.

The data protection officer shall be obliged to maintain strict secrecy or confidentiality of the personal data that they become aware of in the exercise of their duties. Public officials who perform these functions and violate this duty of secrecy or confidentiality shall be punished

in accordance with the provisions of articles 246 to 247 bis of the [Chilean] Penal Code. The data controller will be liable for any breaches of the duty of secrecy or confidentiality its prevention officer or protection officer was required to comply with, notwithstanding any recourse actions that may be brought against him or her.

The data controller shall ensure that the officer has sufficient means and authority to perform his or her duties and shall provide him/her with the material resources necessary to properly perform his/her tasks, taking into consideration the size and economic capacity of the entity.

Notwithstanding any other duties that may be assigned to him/her, the data protection officer shall have the following duties:

a) To inform and advise the data controller, the third-party agent or data processors and the dependents of the controller, with respect to the legal and regulatory provisions relating to the right to the protection of personal data and the regulation of their processing.

b) To promote and participate in the policy issued by the data controller regarding the protection and processing of personal data.

c) To supervise compliance with this law and the policy dictated by the data controller, within the scope of its competence.

d) To ensure permanent training of the people involved in data processing operations.

e) To assist the members of the organization in identifying the risks associated with the processing activity and the measures to be adopted to safeguard the rights of the data subjects of personal data.

f) To develop an annual work plan and report on its outcomes.

g) To respond to the queries and requests of the data subjects.

h) To cooperate and act as the Agency's point of contact.

Article 51.- Certification, registration, supervision of the infringement prevention model and regulations.

The Agency shall be the entity in charge of certifying that the infringement prevention model meets the requirements and elements set forth in the law and its regulations as well as to supervise them.

The Agency will register in the National Registry of Penalties and Compliance those entities with a valid certification.

A regulation issued by the Ministry of Finance and subscribed by the Minister Secretary General of the Presidency and by the Minister of Economy, Development and Tourism shall set forth the requirements, modalities and procedures for the implementation, certification, registration and supervision of the Infringement Prevention Model.

Article 52.- Validity of certificates.

Certificates issued by the Agency will be valid for three years. Notwithstanding the foregoing, they shall be null and void in the following cases:

a) By revocation made by the Agency.

b) Due to the death of the data controller in the case of natural persons.

c) By dissolution of the body corporate.

d) By enforceable judicial decision.

e) By voluntary cessation of the activity of the data controller.

The term of validity of a certificate for any of the reasons indicated above shall be unenforceable against third parties, until it is removed from the registry.

Article 53.- Revoking the certification.

The Agency may revoke the certification referred to in the preceding articles, provided that the data controller does not comply with the provisions of this Paragraph. For this purpose, the Agency may request all the information necessary for the exercise of its duties.

Data controllers may be exempt from providing the requested information when it is covered by an obligation of secrecy or confidentiality and must prove this circumstance.

Failure to deliver the required information, as well as the delivery of false, incomplete or manifestly erroneous information, will be sanctioned in accordance with this law.

To re-apply for a certificate that has been revoked by the Agency, the data controller for data must provide reliable evidence that the reason for its revocation has been remedied

Title VIII

On personal data processing by National Congress, the Judiciary, and State instrumentalities that have autonomy pursuant to the Constitution

Article 54.- General rule for the processing of personal data.

The processing of personal data carried out by the National Congress, the Judiciary, the Office of the Comptroller General of the Republic, the Criminal Prosecutor's Office, the Constitutional Court, the Central Bank, the Electoral Service and the Electoral Justice, and the other special courts created by law, is lawful when carried out for the fulfillment of their legal functions. within the scope of their competences and, in accordance with the special rules established in their respective organic laws and the provisions of Title IV of this Law applicable to public bodies, with the exception of the provisions of Article 14 quinquies and Articles 44 to 46, with referring to the intervention of the Office of the Comptroller General of the Republic in the assessment of administrative liability and the application of Law No. 18,834. Officials of these bodies must observe the utmost secrecy with respect to such data. Under said conditions, these instrumentalities and bodies hold the status of data controller for data and do not require the consent of data subjects to process their personal data. Superior authorities of internal bodies of these instrumentalities shall dictate the policies, rules and instructions necessary to comply with the principles and obligations set forth in the present law, especially those that allow the exercise of the rights granted to data subjects and those that set the minimum standards or conditions of control, security and safeguard that must be observed in the processing of personal data, and may require the technical assistance of the Agency for

such purpose. Likewise, the heads of these bodies shall exercise disciplinary authority over their officials in relation to any infringements that may occur in the processing of personal data, particularly the infringements referred to in articles 34 bis, 34 *ter* and 34 quater.

The higher authorities of the internal bodies of these institutions must issue the policies, rules and instructions necessary to comply with the principles and obligations established in this law, especially those that allow the exercise of the rights recognized to data subjects and those that set the minimum standards or conditions of control. security and safeguarding that must be observed in the processing of personal data and may require the technical assistance of the Agency for this purpose. Likewise, the authorities of these bodies will exercise disciplinary power with respect to their officials, in relation to the infractions that occur in the processing of personal data, particularly the infractions indicated in articles 34 bis, 34 ter and 34 quarter.

Article 55.- Exercise of rights and claims. Data subjects shall exercise their rights under this law before the National Congress, the Judiciary, the Office of the Comptroller General of the Republic, the Public Prosecutor's Office, the Constitutional Court, the Central Bank, the Electoral Service and the Electoral Courts, and other special courts created by law, pursuant to rational and fair procedures, and before the bodies that these instrumentalities stipulate, as provided for in the preceding article.

In the event that the Office of the Comptroller General of the Republic, the Public Prosecutor's Office, the Central Bank or the Electoral Service deny the exercise of a right granted by this law to a data subject without justification or in an arbitrary manner, or violate any principle established in article 3°, duty or obligation established therein, thereby causing damage, the data subject who is aggrieved or affected by the decision of the instrumentality, may file a claim before the Court of Appeals, pursuant to the procedure set forth in article 43 of this law.

The superior authorities of the National Congress, the Judiciary, the Constitutional Court, the Electoral Courts and other special courts created by law, shall ensure that the principles set forth in article 3° and duties are strictly complied with in the processing of personal data by these institutions and that the rights of subjects set forth in the present law are observed, by adopting the necessary and appropriate internal control and oversight measures to this end.

INTERIM ARTICLES

Article One.-

The amendments to Laws No. 19,628, on the protection of personal data, No. 20,285, on access to public information, and executive law decree No.3, of the Ministry of Economy, Development and Tourism, of 2019, which establishes the consolidated, coordinated and systematized text of Law No.19,496, which provides rules on the protection of consumers' rights, contained in the first, second and third articles of this law, respectively, shall enter into force on the first day of the twenty-fourth month following the publication of the present law in the Official Gazette.

Article Two.-

The regulations referred to in this law shall be issued within six months following the publication of this law in the Official Gazette.

Article Three.-

Within sixty days prior to the entry into force of the amendments to Law No. 19,628, contained in the first article of this law, the Civil Registry and Identification Service shall eliminate the register of personal databases contemplated in the current article 22 of Law No. 19,628.

Article Four.-

The first appointment of the directors of the Board of Directors of the Personal Data Protection Agency and of the president and vice-president of the Board of Directors of the Agency shall be made within sixty days prior to the entry into force of this law.

The nomination to be made to the Senate for the first appointment will identify one board member who will serve a two-year term, one board member who will serve a four-year term, and one board member who will serve a six-year term. The aforementioned nomination shall be made in a single act and the Senate shall reach a decision on the nomination as a unit.

However, board members shall only assume their positions once this law enters into force, pursuant to the provisions of the first transitory article.

The statutes of the Agency shall be proposed to the President of the Republic, in accordance with Article 30 octies of this Law, within ninety days following the entry into force of this Law.

Article Five.-

Public entity who decides to appoint a prevention officer or personal data protection officer shall designate for this purpose an official from the current staff of the respective body.

Article Six.-

During the first 12 months after the entry into force of this law, in cases in which a sanction is applicable for companies classified as smaller, according to the categories established in the second article of Law No. 20,416, which establishes special rules for them, the Agency may apply a written warning as a sanction, indicating to data controllers the seriousness of the infraction, the infringing conduct, and the mitigating and aggravating circumstances of responsibility, if applicable. The duty of registration shall be applicable to this reprimand as provided for in Article 39 of this Law.

Article Seven.-

The institutions and agencies indicated in Article 54 shall issue the policies, regulations, and instructions referred to in its third paragraph, within eighteen months following the publication of this Law in the Official Gazette.

Article Eight.-

The greater fiscal expenditure arising from the implementation of this law, during its first budgetary year of effectiveness, shall be financed with the resources provided for in the budget of the Ministry of Economy, Development and Tourism and, whatever is lacking,

charged to the Budgetary Item of the Public Treasury of the corresponding budgetary year. The following years will be included in the Public Sector Budget Law.

Amendments to other legal rules and regulations

ARTICLE TWO.-

Article 33, letter m) of the first article of Law No. 20.285, on access to public information, is hereby deleted.

ARTICLE THREE.-

Article 15 bis of Law No. 19,496, which establishes Norms on the Protection of Consumers' Rights, is hereby deleted.