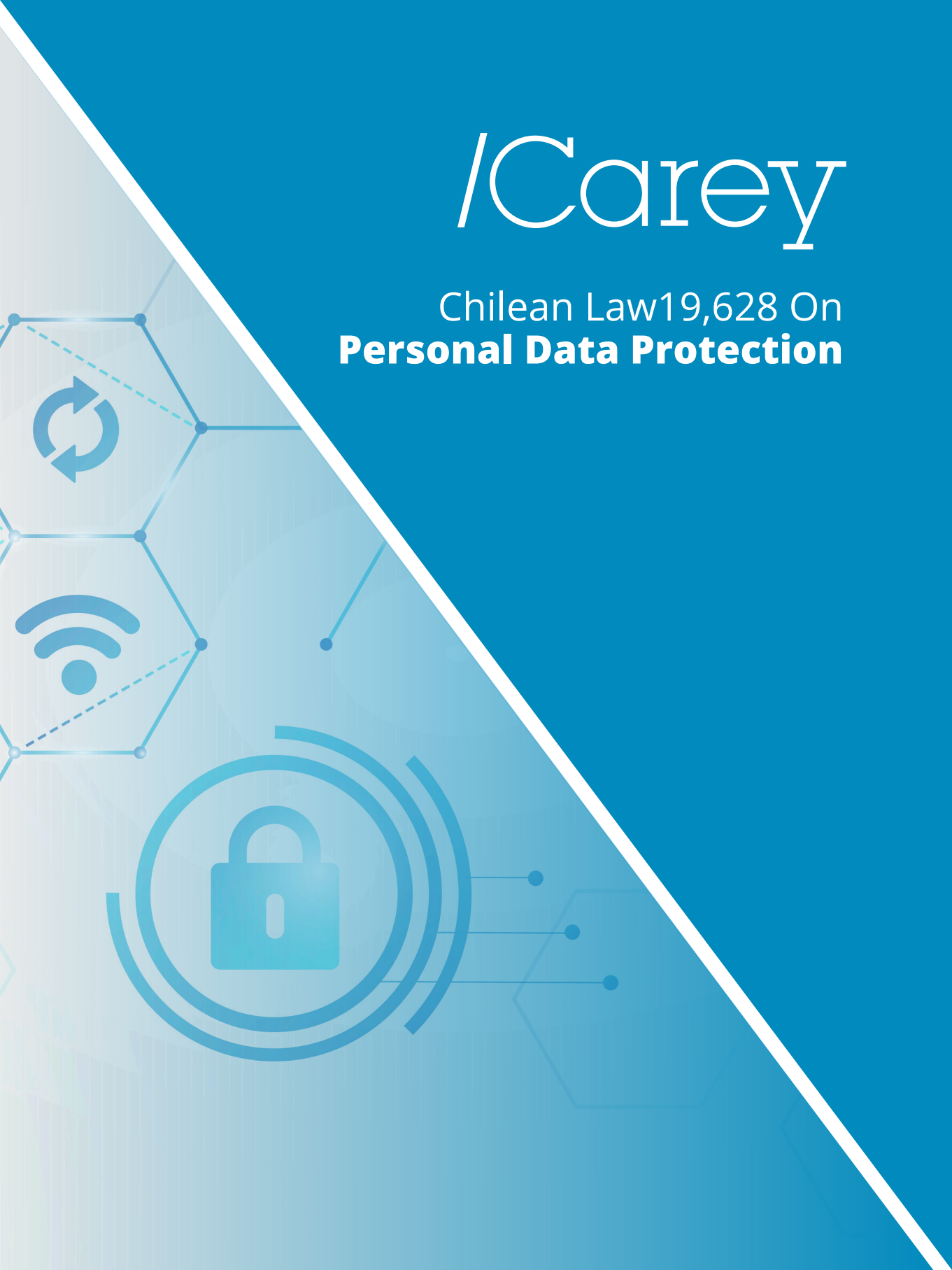
/Carey

Chilean Law19,628 On **Personal Data Protection**



Bill of law under discussion:

Preliminary Title

General provisions

Article 1.- Purpose and scope of application. This law is aimed at regulating the manner and conditions in which the processing and protection of individuals' personal data is to be performed, pursuant to article 19 No. 4 of the Political Constitution of the Republic of Chile.

All processing of personal data by an individual or body corporate, including State instrumentalities, ought to observe the rights and freedoms of individuals, and shall remain subject to the provisions herein.

The system for the processing and protection of data set forth herein shall not apply to the processing of data carried out in exercising the freedoms of speech and of information governed by the laws cited in article 19 No. 12 of the Political Constitution of the Republic. The media shall continue to be subjected to the provisions herein for everything associated to the processing of data carried out with a purpose other than that of issuing an opinion or informing.

The provisions herein shall not be applicable, either, to the processing of data carried out by individuals as regards their personal activities.

Article 1 bis.- Scope of territorial application. The provisions herein shall be applied to the processing of personal data performed under any of the following circumstances:

a) Whenever the party responsible, or the agent, is established or incorporated in the national territory.

b) Whenever the agent, regardless of the location of its establishment or incorporation, performs operations of personal data processing on behalf of a party responsible established or incorporated in the national territory.

c) Whenever the party responsible or the agent have not been established in the national territory, but its personal data processing operations are aimed at offering goods or services to data subjects located in Chile -regardless of whether they are requested a payment-, or at monitoring the behaviour of data subjects within the national territory, including their analysis, tracking, profiling, or forecast of behaviour.

This law shall also apply to personal data processing carried out by a party responsible that, albeit not being established within the national territory, can be applied Chilean legislation due to an agreement or pursuant to international law.

Definitions

Article 2.- For the purposes hereof, the following terms shall be understood as:

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

b) Blocking of data: the temporary suspension of any processing operation of the data stored.

c) Communication of personal data: to howsoever disclose, by action of the party responsible of the data, personal data to persons other than the data subject to whom the data concern, without actually transferring them.

d) Expired data: the one that has lost current validity on account of a law, the compliance of a given requisite, or the expiry of the term stated for its good standing or, were there no stated rule, due to a change in the events or circumstances it records.

e) Statistical data: datum that, in its origin, or as a consequence of its processing, cannot be associated to an identified or identifiable subject.

f) Personal data: any information linked or referring to an identified or identifiable individual. A person shall be identifiable if his/her/their identity can be directly or indirectly determined, particularly through one or more identifiers, such as the name, personal ID document number, and the analysis of elements typical of physical, physiological, genetic, mental, economic, cultural, or social identity of said person.

g) Sensitive personal data: personal data that refers to the physical or moral characteristics of individuals, or to events or circumstances of their private life or privacy, such as those that reveal an ethnic or racial origin, a political, union, or trade group affiliation, socioeconomic status, ideology or philosophical beliefs, religious beliefs, the human biological profile, biometric data, and the information regarding the sexual life, sexual orientation, and gender identity of an individual.

h) Data deletion or cancellation: the destruction of the data stored in records or databases, howsoever done.

i) Public access sources: all those databases, or sets of personal data, which access or query may be lawfully done by anybody, such as the Official Gazette, the media, or public records provided by law. The processing of personal data stemming from public access sources shall be subjected to the provisions herein.

j) State instrumentalities: the authorities, State agencies, and institutions described and regulated by the Political Constitution of the Republic, and those covered in the first paragraph of law No. 18,575, Organic Constitutional Law for the General Terms of the State Administration.

k) Anonymization: irreversible procedure through which a personal data cannot afterwards be linked or associated to a given individual, and neither enable identifying the latter, because the connection with the information that links to, associates with, or identifies, said individual has been destroyed or deleted. An anonymised data stops being a personal data.

l) Pseudonymization: personal data processing carried out in such a way as to afterwards no longer being attributable to a data subject without turning to additional information, provided that additional information is kept apart and is subject to technical and organizational measures aimed at ensuring the personal data are not attributed to an identified or identifiable individual.

m) Personal database: the organised set of personal data, whatsoever its purpose, manner, or modality of creation, storage, organization, and access, which enables associating data and processing it.

n) Party responsible for data or party responsible: any individual or body corporate from the public or private sector, which decides the purposes of, and means for, the processing of personal data, regardless of whether the data are processed by such person or through a third party agent or processor.

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

o) Data processing: any operation or set of operations or technical procedures, whether or not of an automated nature, that howsoever enable the collection, processing, storage, communication, transfer, or usage of personal data or sets of personal data.

p) Consent: Any and all statement of free, specific, unequivocal, and informed willingness, granted via a statement or clear affirmative action, through which data subjects, their legal representatives or agents, as applicable, authorise the processing of the personal data concerning them.

q) Right to access: the right of a data subject to request and obtain, from the party responsible, a confirmation on whether his/her/their personal data are being processed by it, access them if so, and access, too, the information consecrated herein.

r) Right to rectify: the right of a data subject to request and obtain from the party responsible, that his/her/their personal data be amended or completed, whenever they are being processed by that party responsible and they are inaccurate, dated, or incomplete.

s) Right to delete: the right of a data subject to request and obtain from the party responsible, the deletion or elimination of his/her/their personal data, pursuant to the causes set forth by law to such ends.

t) Right to oppose: the right of a data subject to request and obtain from the party responsible, that his/her/their data not be subjected to a specific processing, pursuant to the causes set forth by law to such ends.

u) Right to portability of personal data: the right of a data subject to request and obtain from the party responsible, a copy of his/her/their personal data in a structured, generic, and commonly used electronic format operational in various systems, and which allows for their communication or transfer to another party responsible for data.

The data subject shall be entitled to have his/her/their personal data directly transferred from one party responsible to another whenever the foregoing is technically feasible.

v) Transfer of personal data: the conveyance of personal data by one party responsible to another party responsible for data.

w) Profiling: any and all forms of automated processing of personal data that consists in using those data to assess, analyse, or forecast aspects in connection with professional performance, financial status, health state, personal preferences, interests, trustworthiness, behaviour, location, or movements of an individual.

x) Third party agent or processor: the individual or body corporate that processes personal data on behalf of the party responsible for data.

y) Agency: the Personal Data Protection Agency.

z) National Registry of Penalties and Compliance: a national public registry managed by the Agency, which records the certified prevention models; parties responsible for that data that adopt them, and the penalties applied to any parties responsible for data that have breached the law.

Article 3.- Principles. Processing of personal data is governed by the following principles:

a) Lawfulness and faithfulness principles. Personal data may only be processed in a lawful and faithful manner.

The party responsible shall be capable of certifying the lawfulness of the personal data processing it carries out.

b) Purpose principle. Personal data shall be collected for specific, explicit, and lawful purposes. Processing of personal data shall be limited to meeting said purposes.

In accordance with this principle, personal data cannot be processed for purposes other than those informed at the time of collection, except if said processing has purposes compatible with those originally authorised; there is a contractual or pre-contractual relationship between the data subject and the party responsible which justifies the processing of the data with another purpose, provided they fall within the contractual purposes or are coherent with the discussions or negotiations prior to the agreement being entered; the data subject again grants his/her/their consent, and whenever the law so instructs it.

c) Proportionality principle. Personal data processed shall be strictly limited to those necessary, suitable, and relevant as regards the processing purposes.

Personal data may be kept solely for the time span required to meet achieve the processing purposes, after which they shall be deleted or anonymized, notwithstanding the exceptions set forth by law. A lengthier time span requires legal authorization or data subject consent.

d) Quality principle. Personal data shall be accurate, complete, current, and relevant as regards their origin and processing purposes.

e) Liability principle. Those carrying out the processing of personal data shall be legally liable for the compliance with the principles provided in this article, and for the obligations and duties set forth by law.

f) Security principle. In processing of personal data, the party responsible shall guarantee suitable security standards, protecting them from unauthorised or unlawful processing, and from their loss, leakage, accidental damage, or destruction. Security measures applicable shall be suitable and fitting to the processing to be carried out, and with the nature of the data.

g) Transparency and information principle. The party responsible shall present the data subject with all the information necessary for the exercise of the rights set forth herein, including the policies and practices on processing

of personal data, all of which shall, as well, be always accessible and available to any interested party in an accurate, clear, unequivocal, and free-of-charge manner.

The party responsible shall adopt the suitable and timely measures to facilitate to the data subject the access to all the information stated herein, as well as any other communication in connection with the processing it carries out.

h) Confidentiality principle. The party responsible for personal data, and those who have access to them, shall keep the secrecy or confidentiality of said data. The party responsible shall set up the controls and suitable measures to preserve said secrecy or confidentiality. This duty survives the end of the relationship with the data subject.

Title I

On the rights of the personal data subject

Article 4.- Data subject rights Everyone, whether acting for itself or through a legal representative or agent, as applicable, is entitled to the access, rectification, deletion, opposition, portability, and blocking of his/her/their personal data, pursuant to law.

The foregoing rights are personal, non-transferable, and unwaiverable, and may not be limited by any sort of act or convention.

In the event of death of a data subject, the rights acknowledged herein may be exercised by the heirs.

Withal, heirs may not access the data of the originator, nor request their rectification or deletion, whenever the deceased had expressly forbidden it, or the law so provides.

Article 5.- Right to access. The data subject is entitled to request and obtain, from the party responsible, a confirmation on whether the personal data concerning him/her are being processed by it and, if so, to access said data and to the following information:

a) Data processed and their origin.

b) The purpose or purposes of the processing.

c) The categories, classes, or types of recipients or, alternatively, the identity of each recipient, if the data subject so requests it, to whom the data have been, or shall be, communicated or transferred.

d) The time span during which the data shall be processed.

e) The lawful interests of the party responsible, whenever the processing is based on that set forth in article 13, letter d).

f) Significant information on the rationale applied in the event the party responsible carries out Data processing pursuant to article 8 bis herein.

The party responsible shall always be compelled to surrender information and give access to the data requested, except whenever the law expressly provides otherwise.

Article 6.- Right to rectify. The data subject is entitled to request and obtain, from the party responsible, the rectification of the personal data concerning him/her being processed by that party responsible, whenever they are inaccurate, dated, or incomplete.

Rectified data shall be communicated to the individuals, entities, or bodies to which the party responsible had previously communicated or transferred the foregoing data.

Once rectification is achieved, the data not rectified may not be processed.

Article 7.- Right to deletion. Data subject is entitled to request and obtain, from the party responsible, the deletion of the personal data concerning him/her, especially in the following cases:

a) Whenever the data are necessary in respect of the purposes of the processing for which they were collected.

b) Whenever data subject had revoked his/her consent to the processing and the latter has no legal grounds.

c) Whenever the data had been unlawfully obtained or processed by the party responsible.

d) Whenever the data are outdated.

e) Whenever the data must be deleted in compliance with a court sentence, a resolution from the data protection agency, or a legal obligation, and

f) Whenever data subject had exercised his/her/their right to opposition pursuant to the article below and there are no other legal grounds for their processing.

Deletion does not apply whenever processing is necessary:

i. To exercise the right to freedoms of speech and of information.

ii. To comply with a legal obligation or the performance of a contract executed between data subject and the party responsible.

iii. To comply with a public duty or for the exercise of an activity of public interest.

iv. On reasons of public interest in the area of public health, in accordance with the conditions and guarantees set forth herein.

v. For processing of personal data for historical, statistical, or scientific purposes, and for studies or research in the public interest, and

vi. For the filing, exercise, or defence of an administrative or judicial claim.

Article 8.- Right to opposition. Data subject is entitled to oppose, before the party responsible, to the specific or given processing of the personal data concerning him/her, in the following cases:

a) Whenever the lawfulness basis for the processing is catering to lawful interests of the party responsible. In such a case, data subject may, at any given time, exercise his/her right to oppose, the party responsible having to stop the processing of the personal data, unless it may certify imperative lawful reasons for the processing that prevail over the interests, rights, and freedoms of data subject, or for the filing and exercise or, or defence against the claims.

b) If processing is carried out exclusively for marketing purposes, or direct marketing of goods, products, or services, including profiling, pursuant to article 8 bis herein.

c) If processing is carried out regarding data obtained from a public access source and there are no other legal grounds for their processing.

Opposition to processing shall not apply whenever such processing is done for purposes of scientific or historical research, or for statistical purposes, provided they were necessary for public duties, or for the exercise of an activity of public interest.

Article 8 bis.- Automated individual decisions, including profiling.

Data subject is entitled to oppose to, and to not be the object of, decisions based on automated processing of his/her personal data, including profiling, whenever such processing renders legal effects on him/her or gravely affects him/her.

The above paragraph shall not apply in the following cases:

a) Whenever the decision is necessary for the execution or performance of an agreement between data subject and the party responsible;

b) Whenever there is prior and stated consent from data subject in the form set forth in article 12 herein, and

c) Whenever the law so states it, inasmuch as the latter sets forth the use of safeguards for data subjects rights and freedoms.

In all cases of decisions based on the automated processing of personal data, even those set forth in letters a), b), and c) above, the party responsible shall adopt the necessary measures to safeguard the rights and freedoms of data subject, his/her right to information and transparency, the right to obtain an explanation, human intervention, to state an opinion, and to request a revision of the decision.

Article 8 ter.- Right to blocking. Data subject is entitled to request a temporary suspension of any personal data processing operation whenever the accuracy cannot be established, or the validity of which is questionable, and with regard to which deletion does not apply.

Article 9.- Right to personal data portability. Data subject is entitled to request and receive a copy of the personal data concerning him/her, that he/she had submitted to the party responsible, in an electronic, structured, generic, and commonly used format that is operational with different systems, and to communicate or transfer them to another party responsible for data, whenever the following circumstances coincide:

a) Processing is automated, and

b) Processing is based on data subject's consent.

The party responsible shall use the swiftest, least strenuous means, without hindering in any way the exercise of this right.

The party responsible shall also inform data subject, clearly and accurately, the measures necessary to obtain his/her personal data, and specify the technical characteristics to do so.

Data subject shall be entitled to have his/her/their personal data directly transferred from one party responsible to another whenever the foregoing is technically feasible.

Withal, exercising the right to portability shall not entail the deletion of the data before the transferor, unless the subject of said data so petitions it also

in the request.

Article 10.- Manner and means for data subject to exercise rights. The rights acknowledge herein are exercised by data subject before the party responsible for said data. If the personal data of data subject are processed by various parties responsible, data subject may exercise his/her rights before any of them.

In the case of bodies corporate that were not established in Chile, the parties responsible shall appoint, in writing, before the Agency, a representative domiciled in the country for the purposes of data subject being able to exercise the rights consecrated herein, and have the applicable judicial or administrative communications or notices be served.

The parties responsible for data shall implement mechanisms and technological tools that enable the exercise by data subject of his/her rights in a swift, agile, and effective manner. The means made available by the party responsible shall be simple in terms of their operation.

Exercising the rights to rectification, deletion, and opposition, shall always be free-of-charge for data subject. Right to access shall also be freely exercised, at least quarterly.

The party responsible for the data may only demand payment of direct costs incurred whenever data subject exercises more than once in a quarter his/her right to access and right to portability. The party responsible may not demand this payment in the cases listed in article 27 f) herein.

The parameters and mechanisms to determine the costs resulting from the exercise of the rights above cited shall be defined by the Agency, through a general instruction that will consider, among others, the volume of the data submitted, the legal nature, and size of the entity or company that boasts the capacity as responsible party.

The Agency shall ensure effective exercise and compliance with the rights that this law acknowledges to data subject, pursuant to this law.

Article 11.- Procedure before the party responsible for data. To exercise the rights granted by this law, the subject shall submit a written request or requirement to the party responsible, addressed to the e-mail address provided for this purpose, a contact form or an equivalent electronic means. The request shall include at least the following information:

a) Individualization of the subject and his/her legal representative or agent, if applicable, and authentication of his/her identity pursuant to the procedures, forms and modalities to be established by the Agency.

b) Provision of an address or e-mail address or other equivalent means to notify the response.

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

d) For rectification requests, the subject shall indicate the specific modifications or updates to be made and provide, if applicable, the background information supporting such modifications or updates. For deletion requests, the subject shall indicate the reason invoked and provide the background information supporting the request, if applicable. For opposition requests, the holder shall indicate the reason invoked and, in the case of letter a) of article 8°, shall briefly substantiate his/her request, and may additionally provide the background information he/she deems appropriate. With regard to the right of access, the individualization of subject will suffice.

Upon receipt of the request, the party responsible shall acknowledge receipt thereof and shall issue a decision no later than 15 business days following the date of receipt.

The party responsible shall respond in writing to the subject at the address or e-mail address provided by the latter. The party responsible must keep the backups to prove the forwarding of the response to the corresponding physical or electronic address, as well as its date and the full content of the response.

Should the request be denied in whole or in part, the party responsible shall justify its decision by stating the reason invoked and the background information that supports it. On the same occasion, the party responsible must inform the subject that he/she may file a claim with the Agency within 15 business days, pursuant to the procedure set forth in Article 41.

Upon expiration of the period of 15 business days referred to in the second paragraph above, failing a response from the party responsible, the subject may file a claim directly with the Agency, under the same terms as in the preceding paragraph.

In the event of a request for rectification, deletion or opposition, the subject shall be entitled to request and obtain from the party responsible the temporary blocking of his/her data or of the processing carried out, as applicable. The request for temporary blocking shall be substantiated and the party responsible shall respond to the request within 2 business days following its receipt. As long as this request is not resolved, the party responsible will not be able to process the data of the subject that are part of the request. This temporary blocking shall not affect the data storage by the party responsible. Should the request

be denied the party responsible shall justify its decision and communicate electronically its decision to the Agency. The subject may challenge this decision before the Agency, and the provisions of Article 41(a) shall apply.

Rectification, deletion or opposition to the processing of data shall apply solely with respect to the parties responsible to whom the request has been made. Withal, if the party responsible has communicated such data to other parties, he/she must inform the latter of the modifications made as a result of the rectification, deletion or opposition.

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

Title II

On the processing of personal data and special categories of data

First Paragraph

On the consent of the subject, the obligations and duties of the party responsible and data processing in general.

Article 12.- General rule for the processing of data. The processing of personal data related to the subject is lawful when he/she gives his/her consent thereto.

The consent of the subject ought to be free, informed and specific as to its purpose or purposes. Consent must also be expressed, in advance and unequivocally, by means of a verbal, written statement or expressed through an equivalent electronic means, or by means of an affirmative act that clearly shows the subject's will.

Where the consent is given by an agent, the latter must be expressly empowered with this power.

The subject may revoke the consent granted at any time and with no cause, using similar or equivalent means to those used for its granting. Revocation of consent shall not have retroactive effect.

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

It is deemed that the consent to process data has not been granted voluntarily when the party responsible collects it within the framework of the performance of a contract or the provision of a service in which it is not necessary to carry out such collection.

Withal, the provisions of the preceding paragraph shall not apply in cases where the person offering goods, services or benefits requires as sole consideration the consent to process data.

It is upon the party responsible to prove that it obtained 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) Processing is related to data on economic, financial, banking or commercial obligations and is carried out pursuant to the provisions of Title III of this law.

b) Processing is necessary for the performance or fulfilment of a legal obligation or as required by law.

c) Processing is necessary to enter into, or perform, an agreement between the data subject and the party responsible, or to execute any pre-contractual measures upon the request from the data subject.

d) Processing is necessary for the satisfaction of legitimate interests of the party responsible or of a third party, provided that this does not affect the rights and freedoms of the subject. In any case, the subject may always demand to be informed on the processing that affects him/her and the legitimate interest on which such processing is based.

d) Data processing is necessary for the formulation, exercise or defence of a right before the courts of law or a State instrumentality.

The party responsible must prove the lawfulness of the data processing.

Article 14.- Obligations of the party responsible for data. The party responsible for data, notwithstanding the other provisions set forth in this law, has the following obligations:

a) To inform and make available to the subject the background information that proves the lawfulness of the data processing it carries out. Likewise, it shall promptly deliver such information upon request;

b) To ensure that personal data are collected from lawfully accessible sources

for specified, explicit and lawful purposes, and that their processing is limited to the fulfilment of these purposes;

c) To communicate or transfer, in conformity with the provisions of this law, accurate, complete and up-to-date information;

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

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

The party responsible for data not domiciled in Chile processing data of persons residing in the national territory, shall indicate and keep updated and operative an e-mail address or other suitable means of contact to receive communications from data subjects and from the Agency.

Article 14 bis.- Duty of secret or confidentiality. The party responsible for data is obliged to maintain the secrecy or confidentiality of personal data concerning a data subject, except when the data subject has made such data manifestly public. This duty remains in force even after the relationship with the subject is terminated. In the event the party responsible has taken any action on personal data obtained from publicly available sources, such as organizing or classifying them under any criteria, or combining or supplementing them with other data, the personal data resulting from such action shall be protected under the present duty of secret or confidentiality.

The duty of secret or confidentiality does not prevent the communication or transfer of data that the party responsible must make pursuant to the law, and compliance with the obligation to provide access to the subject and inform the origin of the subject, whenever this information is required by the subject or by state instrumentalities within the scope of its legal competencies.

The party responsible must take the necessary measures to ensure that its employees or the natural individuals or corporate entities carrying out data processing operations under its responsibility comply with the duty of secret or confidentiality set forth in this article.

Individuals and institutions and their dependents referred to in Article 24 are subject to the obligation of confidentiality, as to the request and the fact of having provided said information.

Article 14 ter. Duty of information and transparency. The party responsible of data shall provide and keep permanent and publicly available on its website or any other equivalent means of information, at least the following information:

a) Policy adopted for the processing of personal data, along with its date and version;

b) Identification of the party responsible of data and its legal representative as well as the identification of the prevention officer, if any;

c) Postal address, e-mail address, contact form or other equivalent technological means of common use and easy access whereby it is notified of any requests made by data subjects;

d) Categories, classes or types of data being processed; a generic description of the universe of individuals comprising its databases; recipients to whom it intends to communicate or transfer the data, purposes of the processing carried out; lawful basis of the processing; and in the case of processing based on the satisfaction of legitimate interests, what such interests would be;

e) Policy and security measures adopted to protect personal databases it administers;

f) The right of the data subject to request before the party responsible, access, rectification, elimination, opposition and portability of his/her personal data, pursuant to law;

g) The right of data subject to appeal before the Agency, in the case the party responsible rejects or does not respond in a timely manner to the requests made by the data subject;

h) Transfer of personal data to a third country or international organization where appropriate, and whether or not they afford a sufficient level of protection. Should they not have a sufficient level of protection, information should be provided on the existence of guarantees supporting said transfer;

i) Period of time for the storage of personal data;

j) Source of personal data and, if applicable, whether it comes from a publicly available sources;

(k) Where processing is based on the consent of the data subject, the existence of the right to withdraw said consent at any time, without affecting the lawfulness of the processing based on the consent prior to its withdrawal, and

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

Article 14 quater. - Duty of protection by design and by default.

In order to comply with the principles and rights of data subjects set forth in this law, the party responsible must implement appropriate technical and organizational measures by design prior to and during the processing of personal data.

Measures to be applied shall take into consideration the state of the art; costs of implementation; nature, scope, context and purposes of the data processing; as well as the risks associated with such activity.

Likewise, the party responsible of data shall implement technical and organizational measures to ensure that, only personal data specific to and strictly necessary for such activity are processed by default. To this end, the number of data collected, the scope of processing, the storage period and their accessibility shall be taken into consideration.

Article 14 quinquies. - Duty to adopt security measures. The party responsible of data must adopt the necessary measures to safeguard compliance with the security principle set forth in this law, bearing in mind the current state of the art and the costs of implementation, along with the nature, scope, context and purposes of the processing, as well as the likelihood of risks and the magnitude of their effects in relation to the type of data processed. Measures implemented by the party responsible must ensure confidentiality, integrity, availability and resilience of data processing systems. Likewise, they shall avoid alteration, destruction, loss, unauthorized processing or access.

Taking into account the state of the art, cost of implementation, and the nature, scope, context and purposes of processing, as well as risks of variable likelihood and severity to the rights and freedoms of data subjects, the party responsible 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) Pseudonymization and encryption of personal data;

b) Ability to ensure permanent confidentiality, integrity, availability and resilience of processing systems and services;

c) Ability to restore availability and access to personal data on a rapid basis in the event of a physical or technical incident;

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

Upon the occurrence of a security incident, and in the event of a judicial or

administrative dispute, it shall be up to the party responsible to prove the existence and operation of the security measures adopted on the basis of the risk levels and the available technology.

Article 14 sexies. - Duty to report breaches of security measures. The party responsible shall report to the Agency, by the most expeditious means possible and without undue delay, any breaches of security measures that may result in the accidental or unlawful destruction, leakage, loss or alteration of personal data processed or unauthorized communication or access to such data, whenever there is a reasonable risk to the rights and freedoms of data subjects.

The party responsible shall record these communications, describing the nature of the breaches occurred, their effects, categories of data and the approximate number of data subjects affected, as well as the measures taken to manage them and prevent future incidents.

Whenever such breaches concern sensitive personal data, data relating to children under fourteen years of age or data relating to economic, financial, banking or commercial obligations, the party responsible shall also notify the subjects of such data, through their representatives, where appropriate. This communication shall be made in clear and simple language, identifying the data affected, potential consequences of security breaches and the remedial or protective measures taken. The notification shall be made to each subject affected and should this not be possible, it shall be made through the dissemination or publication of a notice in a mass social communication media of national scope.

Duties to inform set forth by this article do not preclude the other duties of information established by other laws.

Article 14 septies. - Differentiation of compliance standards. The minimum standards or conditions imposed on the party responsible of data for the compliance with the duties of information and security provided for in Articles 14 ter and 14 quinquies, respectively, shall be established by considering the type of data involved, on whether the party responsible is a natural or corporate body, the size of the entity or company pursuant to the categories established in the second article of Law No. 20,416, which sets special rules for smaller companies, the activity it performs and the volume, nature and purposes of the personal data processed.

The minimum standards or conditions of compliance and the differentiated measures referred to in the preceding 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 fulfilment of the purposes of the processing. Personal data may also be transferred when necessary for the fulfilment and performance of a contract to which the data subject is a party; in case of legitimate interest of the transferor or the transferee, under the terms provided for in Article 13(d), and when provided by law.

In the event that the consent granted by the data subject at the time of collection of 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 transferor and the transferee.

The processing of the personal data transferred shall be carried out by the transferee pursuant to the purposes set forth in the transfer contract.

Upon completion of the transfer, the transferee acquires the status of party responsible of data for all legal purposes. The transferor, for its part, also retains the status of party responsible of data, in respect of the processing operations it continues to carry out.

Should a transfer of data take place without consent of the data subject, such consent being necessary, said transfer shall be null and void and the transferee shall be obliged to eliminate all data received, notwithstanding the legal responsibilities that may apply.

Article 15 bis. - Data processing through a third party agent or processor. The data controller may carry out the data processing directly or through a third party agent or processor. In the latter case, the third party agent or processor 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 agent or data processor 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 party responsible of data for all legal purposes, and shall be personally liable for any infringements incurred and jointly and

severally with the data controller for any damages caused, notwithstanding the contractual liabilities that may correspond to it vis-à-vis the agent or the data controller.

The data processing through a third party agent or processor shall be governed by the contract entered into between the data controller and the processor, pursuant to the legislation in force. The contract shall set forth the purpose of the assignment, its duration, purpose of the processing, type of personal data processed, categories of data subjects to whom the data pertain, and rights and obligations of the parties. The processor may not delegate a portion or the entirety of the assignment, save with the specific written authorization of the data controller. The processor who delegates some or all of the assignment to another processor shall remain jointly and severally liable for the assignment and may not exempt itself from liability by arguing that it has delegated the processing. The Agency will make model contracts publicly available on its website.

The third party agent or processor shall comply with the provisions of articles 14 bis, 14 quater and 14 quinquies. The differentiation of security standards set forth in the first paragraph of Article 14 septies shall also be applicable to the third party agent or processor. Any breach of security measures shall be reported by the third party or agent to the controller.

Upon completion of the provision of the processing service by the agent or processor third party, data in its possession must be eliminated 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 party responsible 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 assessments on personal aspects of data subjects, based on automated processing or decisions, such as profiling, and which produce significant legal effects on them.

b) Massive or large scale data processing.

c) Processing involving systematic observation or monitoring of an area of public access.

d) Processing of sensitive and specially protected data, in the cases of

exceptions to consent.

Data Protection Agency shall establish and publish an indicative list of the types of processing operations that may or may not require an impact assessment on the protection of personal data. The Agency shall also establish the minimum guidelines to carry out this assessment, addressing among these criteria at least 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.

The party responsible may consult the Data Protection Agency, when by virtue of the outcome of the assessment, the processing proves to be of high risk in order to obtain recommendations from that body.

Second Paragraph

On the 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 is lawful, in the following cases, with no consent of the data subject:

a) Processing refers to sensitive personal data that the data subject has manifestly made public and its processing is related to the purposes for which it was published.

b) Processing is based on a legitimate interest carried out by a body corporate under either public law or private law that does not pursue a profit-making purpose 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 body corporate provides the necessary guarantees to prevent leakage, theft or unauthorized use or processing of data, and

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

Provided these conditions are met, the body corporate shall not require the consent of the data subject to process his or her data, including sensitive personal data. In case of questions or administrative or judicial dispute, the party responsible of data shall demonstrate its concurrence.

As soon as a member of the body corporate ceases to belong to it, his or her data shall be anonymized or eliminated.

c) Processing of the personal data of Data Subject is indispensable to safeguard life, health or physical or psychological integrity of the Data Subject or of another person, or when the Data Subject is physically or legally unable to give his/her consent. Upon termination of the impediment, the party responsible shall inform the data subject in detail of the data processed and the specific processing operations carried out.

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

e) Data processing is necessary for the exercise of rights and the fulfilment of obligations of the party responsible or the data subject, in the labour or social security field, and is carried out pursuant to the law.

f) The processing of sensitive personal data is expressly authorized or 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 related to health and human biological profile. Personal data relating to health of the data subject, 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 particular laws on health matters, in compliance with the provisions of the first paragraph of article 16.

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

c) Indispensable to safeguard life, health or physical or psychological integrity of the Data Subject or of another person, or when the Data Subject is physically or legally unable to give his/her consent. Upon termination of the impediment, the party responsible shall inform the data subject in detail

of the data processed and the specific processing operations carried out.

b) Sanitary alert legally decreed.

c) Used for historical, statistical or scientific purposes, for studies or research in the public interest or for the benefit of human health, or for the development of medical products or supplies that cannot be otherwise developed. Findings of scientific studies and research using personal data relating to health or biological profile may be freely published or disseminated, with prior anonymization of the data to be published.

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

e) Processing is necessary for the purposes of preventive or occupational medicine, evaluation of an employee's ability to work, medical diagnosis, provision of health or social care or treatment, or management of health and social care systems and services.

f) Legally permitted and expressly indicating the purpose for which such processing shall be carried out.

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.- Sensitive biometric personal data. Sensitive personal data of a biometric nature are those obtained from a specific technical processing, related to the physical, physiological or behavioural characteristics of a person that allow or confirm the unique identification of the person, such as fingerprint, iris, hand or facial features and voice.

Such data may only be processed when the provisions of the first paragraph of article 16 are complied with and provided that the party responsible provides the data subject with the following specific information:

a) Identification of the biometric system used;

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

c) Time period the biometric data will be used, and

d) The manner in which the data subject may exercise his or her rights.

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

Third Paragraph

On the processing of special categories of personal data

Article 16 quater. - Personal data relating to children and adolescents. The processing of personal data related to children and adolescents shall only be carried out in their best interest and with respect for their progressive autonomy.

In compliance with the requirement set forth in the preceding paragraph, the processing of personal data of children requires the consent given by their parents or legal representatives or by the person in charge of the personal care of the child, save when expressly authorized or mandated by law.

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

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

For the effects of this law, minors under fourteen years of age are considered children, while adolescents are 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 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.

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

The party responsible who have processed personal data exclusively for these purposes may publish the results and analyses thus obtained, provided that 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 sources of lawfulness established in articles 12 and 13.

The data subject shall be informed in a clear, sufficient and timely manner, of the type of geolocation data that will be processed, 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

On the use of personal data related to economic, financial, banking or commercial obligations

Article 17. - Party responsible 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 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 parties responsible 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.- Once 5 years have elapsed from the relevant obligation being enforceable, the data core to the prior article may not, under any circumstance, be informed, whenever they refer to an identified, or identifiable, individual.

It may not, either, continue to inform the data pertaining said obligation after the latter has been paid or legally extinguished.

Withal, the courts of Law shall be presented with the information they may require on account of pending proceedings.

Article 19.- 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

Of the processing of personal data by State instrumentalities

Article 20.- General application rule for data processing by State instrumentalities. The processing of personal data by State instrumentalities is lawful whenever carried out to meet its legal duties, within the scope of their competencies, pursuant to that set forth by law and by the provisions herein. In such a case, State instrumentalities act as party responsible for data, and do not require consent from the subjects in order to process their personal data.

Article 21.- Principles and rules applicable to data processing by State instrumentalities. Personal data processing by State instrumentalities is governed by the principles consecrated in article third herein, and the general principles that govern the State Administration, especially the principles of coordination, integrity, and efficiency.

By virtue of the principle of coordination, State instrumentalities must achieve a high level of interoperability and coherence, so as to avoid contradictions in the information stored and iteration in the requests to data subjects for information or documents. In accordance with to the principle of efficiency, the aim is to avoid duplication of procedures and processing among State instrumentalities, and between the latter and the subjects of the information.

Notwithstanding the remaining provisions herein, the provisions set forth in articles 2, 14, 14 bis, 14 ter, 14 quater, 14 quinquies, 14 sexies, and 15 bis, the articles in Paragraph Second, and Third of Title II, the articles in Title V, and the articles in Title VII hereof, are all applicable to the processing of data carried out by State instrumentalities. Likewise, and pursuant to article 23, they may also be applied articles 4, 5, 6, 7, and 8.

Article 22.- Data communication or transfer by a State instrumentality. State instrumentalities are authorised to communicate or transfer specific personal data, or all or part of their databases or sets of data, to other State

instrumentalities, provided the communication or transfer of said data is necessary to observe their legal duties and both entities act within the scope of their competencies. The communication or transfer of data shall be carried out for a specific processing matter, and the recipient State instrumentality may not use them for any other purposes.

Likewise, personal data or databases may be communicated or transferred among State instrumentalities, solely and exclusively whenever they are required for processing that is aimed at rendering benefits for the data subjects, avoiding duplication of errands for citizens, and iteration of requests for information or documents to those same data subjects.

The State instrumentality that is the data recipient may only keep such data for the time span necessary to carry out the specific processing for which they were requested, after which such data shall be deleted or anonymised. These data may be stored for a lengthier time span whenever the State instrumentality requires tending to complaints or challenges, perform control and follow-up tasks, or if they may be used as assurance of the decisions made.

For the purposes of communicating or transferring personal data to individuals or private entities, State instrumentalities shall require the consent from the data subject, unless the data communication or transfer were necessary to meet the duties of the State instrumentality in matters of monitoring or inspection.

Whenever the idea is to communicate or transfer personal data on account of a request to access the information formulated pursuant to article 10 in Law No. 20,285, State instrumentalities shall require the consent from the data subject, obtained in due time as set forth in article 20 of said law.

Regarding the communication of the data associated to criminal, civil, administrative, and disciplinary violations, article 25 shall apply.

State instrumentalities shall inform on a monthly basis and through their institutional websites any and all agreements executed with peers and with private entities regarding the transfer of personal data. This obligation shall be monitored and inspected by the Agency.

Article 23.- Exercise of data subject rights, procedure for administrative writ for the protection of constitutional rights, and complaint on illegality. The data subject may exercise before the State instrumentality the rights of access, rectification, and opposition that the law acknowledges to him/her. The data subject could also oppose to a specific processing whenever the latter breaches the provisions herein. The data subject may exercise the right to deletion in the cases set forth in the third paragraph of the preceding article.

State instrumentalities shall not admit the requests for access, rectification, opposition, deletion, or temporary blockage of the personal data in the following cases:

a) Whenever doing so prevents or hinders the performance of the monitoring and inspection, and investigative role, the duties of protection of victims and witnesses, and/or the penalizing duties of the State instrumentality, and

b) Whenever that affects the secret nature of the information, set forth by law.

The rights of the data subject shall be exercised pursuant to the procedure set forth in article 11 herein, addressing the highest authority in the State body.

Data subject may file a complaint before the Agency whenever the State instrumentality denies it, either expressly or tacitly, a request in which it exercises any of the rights he/she is acknowledged by law. The complaint shall abide by the rules provided in the procedure for administrative writ for the protection of constitutional rights set forth in article 41.

Article 24.- Special rules. The processing, communication, or transfer of personal data, carried out by State instrumentalities competent in matters listed below, shall be subjected exclusively to the special set of regulations set forth in this article:

a) Those carried out to prevent, investigate into, detect, or subject to trial any criminal infringements, or to enforce criminal sanctions, including protection and prevention activities in the face of threats and risks to public safety, and the protection of victims and witnesses.

b) Those on matters directly associated to national security, national defence, and a country's foreign policy.

c) Those carried out with the sole purpose of catering to an emergency situation or catastrophe, as declared pursuant to the law and only for as long as said declaration is valid.

d) Those protected by the rules on secrecy, reserve, or confidentiality, set forth in the corresponding laws. The data that, in abidance of a legal obligation, State instrumentalities need to transfer to a peer or to third parties -recipient having to, in such s case, process them observing the same obligation of secrecy, reserve, or confidentiality-, are also considered within this exception.

The relevant State instrumentalities may process, transfer, and communicate personal data in a lawful manner, provided it is done in order to meet its

legal duties, within the scope of its competencies, and in observance of the fundamental guarantees set forth in article 19, No. 4, of the Political Constitution of the Republic and the principles set forth in article third.

With a view to carrying out the processing of the transfers and communications of personal data for the purposes set forth in letters a), b), and c) above, State instrumentalities and their authorities shall be compelled to exchange information and to supply the personal data which they may be requested to such ends, provided they refer to processing carried out with a specific purpose authorised by law, or, whenever the foregoing is not possible, the requirement is a necessary and proportional measure.

The Personal Data Protection Agency may, after having heard from the relevant bodies, issue instructions to specify the manner in which to apply said guarantees and principles to the aforementioned cases, so as to ensure their being safeguarded and to enable due compliance of the legal duties of the relevant bodies.

Article 25.- Data associated to criminal violations, civil, administrative, and disciplinary offences. Personal data associated to the perpetration and penalties for criminal violations, and civil, administrative and disciplinary offences may only be processed by State instrumentalities to meet their legal duties, within the scope of their competencies, and in the cases expressly stated in the law.

Communications by State instrumentalities 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 associated to the perpetration of, and sentence for, criminal violations and civil, administrative or disciplinary offences, once the statute of limitations applies for the corresponding criminal, civil, administrative, or disciplinary action, or once the sentence or penalty applied has been met or applied the statute of limitations -which shall be declared or verified by the relevant State authorities- may not be informed or disclosed. The foregoing notwithstanding the incorporation, maintenance, and consultation of this information in the records kept by State instrumentalities as expressly provided by law, in the manner and for the time spans set forth in the law that establishes the relevant specific obligation. People working at State instrumentalities are compelled to observe secrecy as regards this information, which shall be kept as classified information.

Whenever the law provides that the information regarding the perpetration of and penalizing for criminal violations and civil, administrative, and disciplinary offences must be disclosed through inclusion in a penalties registry, or via

publication in a website of a State instrumentality, or by any other means of communication or dissemination, without setting a specific time span during which said information ought to be available, the following rules shall be followed:

a) Regarding criminal violations, publicity time spans shall be governed by the specific provisions that apply for this sort of infringements.

b) Regarding civil, administrative, and disciplinary offences, they shall be accessible to the public for a 5-year period.

It is hereby forbidden to run massive processing of personal data contained in electronic records of criminal violations, and of civil, administrative, and disciplinary offences kept by State instrumentalities. Pursuant to this law, failing to abide by the foregoing prohibition constitutes a very serious infringement.

Cases in which the information is requested by courts of law or by another State instrumentality, for the purposes of their legal duties and within the scope of their competency, are excepted from the prohibition, and the requesting entity shall keep due reserve of the relevant data.

Notwithstanding the third paragraph in this article, personal data associated to the perpetration of, and penalising for, criminal violations entails a classified nature and, excepting the legal provisions authorising their processing, they may not be informed or transferred to third parties by the State instrumentalities that have them.

Article 26.- Regulations. The conditions, modalities, and instruments to inform or transfer personal data among State instrumentalities and with individuals or private entities, shall be regulated by the rules issued by the Ministry General Secretariat of the Presidency and executed by the Ministry of Finance, as well as by the Ministry of Economics, Development and Tourism, after a report from the Agency. In these same regulations shall govern the personal data anonymization procedures, especially sensitive personal data.

Withal, these regulations shall not be applicable to the transfers in which there is participation of any of the bodies cited in Title VIII hereof.

Title V

On the international transfer of personal data

Article 27.- General rule on authorisation. If the requirements that,

pursuant to law, authorise the processing of data are met, the operations of international transfer of data are lawful in any of the following cases:

a) Whenever such transfer is carried out by a person, entity, or organization, from the State or the private sector, in abidance of the legal system of a country that offers suitable degrees of personal data protection, pursuant to article 28.

b) Whenever the transfer of data is sheltered by contractual clauses or clauses in other legal instruments executed between the party responsible for carrying out the transfer and the party responsible, or third party agent- that receives it, and the rights and guarantees of the data subjects are established therein along with the obligations of the parties responsible and of the third party agents and the means of control.

c) Whenever the party responsible that carries out the transfer and the party responsible or third party agent that receives it, adopt a binding and certified compliance or self-regulation model pursuant to the legislation applicable to each of them.

d) Whenever there is stated consent from the data subject to carry out a specific and particular international transfer of data.

e) Whenever they refer to specific banking, financial, or stock exchange transfers carried out pursuant to the laws that regulate this sort of transfers.

f) Whenever the transfer is carried out between companies or legal entities that belong to a same corporate group, affiliates, or companies subject to a same controller, pursuant to the Law on the Securities Market, provided all said companies operate under the same standards and policies in terms of personal data processing. The party responsible carrying out the data transfer shall assume the liability for any infringement to the binding corporate standards and policies incurred by any member of the corporate group. The party responsible may only be exempted from any liability whenever it may certify that the infringement is not attributable to the member of the corporate group.

g) Whenever data must be transferred to meet obligations acquired through standing international treaties or conventions ratified by Chile.

h) Whenever the transfer is necessary due to the application of cooperation conventions, information exchange, or supervision executed by State instrumentalities in compliance of their duties and in exercise of their competencies.

i) Whenever the data transfer carried out by an individual or body corporate,

be them from the public or private sector, has been expressly authorised by law and only for a specific purpose.

j) Whenever the transfer is carried out to render or request international judicial collaboration.

k) Whenever the transfer is necessary to enter into, or perform, an agreement between the data subject and the party responsible, or to execute any pre-contractual measures upon a request from the data subject.

l) Whenever it is necessary to adopt urgent measures in some medical or public health matter, towards the prevention or diagnose of illnesses, for medical treatments, or for the management of public health or healthcare services.

Article 28.- Rule to define suitable countries and other provisions applicable to international transfer of data. The understanding is that the legal system of a country has suitable degrees of data protection whenever it abides by standards similar or higher than those set forth herein. The Agency shall define, with good grounds, the countries that have suitable 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 provisions that acknowledge and guarantee the rights of data subjects, as well as the existence of jurisdictional or administrative State authority for control or protection of constitutional rights.

c) The imposition of information and security obligations to the parties responsible and third party agents of the data processing.

d) The definition of liabilities in the event of infringements.

The Agency shall make available to the interested parties, through its website, a list of suitable countries and templates for contractual clauses and other legal instruments for the international transfer of data.

Whenever none of the circumstances stated above take place, the Agency may authorise, upon a grounded resolution, the international transfer of data for a specific case, provided the party carrying out the transfer, and the recipient of the data, both grant suitable assurance as regards the protection of the rights of the individuals that are the data subject, and the security of the information transferred, pursuant to this law. The instruments, mechanisms, and clauses containing principles, rights and guarantees similar or more stringent than those set forth herein and, particularly, those

that grant enforceable rights and effective legal actions to data subjects, shall be deemed suitable guarantees. The Agency may set prerequisites for the transfer to take place, and may approve model clauses containing said guarantees to a cross-border data flow, all of which shall be available to the parties responsible.

The party responsible for data that carried out the international transfer of data shall be the one to certify before the Agency that said transfer was carried out pursuant to the provisions herein.

Article 29.- Monitoring and inspection. The Agency shall monitor and inspect the operations of international transfer of data, being entitled to make recommendations, adopt injunctive and precautionary measures, and, in specific cases, temporarily suspend the transfer of data.

Title VI

Supervisory Authority/Regulator on the Protection of Personal Data

Article 30.- Personal Data Protection Agency. The Personal Data Protection Agency is hereby created as an autonomous corporation under public law, of a technical, decentralized nature, with legal personality and own assets, which shall report to the President of the Republic through the Ministry of Economy, Development and Tourism.

Its purpose shall be as to ensure the effective protection of rights that guarantee the privacy of individuals and their personal data, pursuant to the provisions of this law, and to oversee compliance with its provisions.

Domicile of the Agency shall be specified by regulation, notwithstanding the domiciles that it may establish in other locations in the country.

Article 30 bis.- Duties and powers of the Agency. The Agency shall be entrusted with the following duties and powers:

a) To issue general and mandatory instructions and rules in order to regulate personal data processing operations consistent with the principles set forth in this law. 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 on personal data processing and that are necessary for the faithful compliance with the present law, providing the appropriate

mechanisms so that the interested parties may make comments thereon.

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

c) To oversee compliance with the provisions of this law, its regulations and the instructions and general rules issued in relation to the processing of personal data. To this end, it may require those who process personal data to submit any document, book or record and all the information necessary for the fulfilment of its oversight role.

d) To determine breaches and non-compliances incurred by those who process personal data, during their data processing operations, in relation to the principles and obligations set forth in this law, its regulations and the instructions and general rules issued by the Agency. To such effect, and on grounds, it may summon to testify, among others, the data subject, legal representatives, administrators, advisors and employees of whoever processes personal data, as well as any person who may have had participation or knowledge of any event that may be relevant to resolve a penalizing proceeding. The respective statements may also be taken by other means that ensure their faithfulness.

e) To exercise the penalizing power over natural or corporate bodies processing personal data in violation of this law, its regulations and the instructions and general rules issued by the Agency, enforcing the sanctions set forth in this law.

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

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

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

i) To provide technical assistance, when requested, to the National Congress, Judiciary, Office of the Comptroller General of the Republic, Public Prosecutor's Office, the Constitutional Court, Central Bank, Electoral Service, Electoral Courts and other special courts created by law, in the issuance and

implementation of the internal policies and rules of these bodies, so that their operations and personal data processing activities are carried out pursuant to the principles and obligations set forth in this law.

j) To interact and work with public bodies in the design and implementation of policies and actions aimed at ensuring the protection of personal data and its proper processing.

k) To enter into cooperation and collaboration agreements with public or private, national, foreign or international entities, with competence or related to the personal data sector. Prior consultation with the Ministry of Foreign Affairs shall be required when entering into agreements with international public entities, pursuant to 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 oversee models for prevention of breaches and compliance programs and to manage the National Registry of Penalties and Compliance.

n) To exercise such other duties and powers as may be entrusted thereto by law.

Should an Administration body be required to exercise the duties or powers granted to the Agency by this law, then 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. Upper Management of the Agency shall be vested in the Governing Board of the Agency, which shall exercise the following duties and powers:

a) To exercise the powers and execute the duties entrusted to the Agency by law.

b) To establish the Agency's internal operating regulations for the fulfilment of those duties entrusted thereto by law.

c) To establish the policies for planning, organizing, managing, overseeing, coordinating and controlling the Agency's operations, as well as those for the administration, acquisition and disposal of assets.

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

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

f) To prepare, within the first four-month period of each year, an annual public

account detailing the work carried out by the Agency in the immediately preceding year.

Article 30 quater.- Members of the Governing Board of the Agency. The Governing Board of the Agency shall be integrated by three board members, appointed by the President of the Republic, with the approval of the Senate, voted by two thirds of its members in office.

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

Candidates for board members shall be individuals of renowned professional or academic standing in the field of personal data protection.

The Governing Board of the Agency shall appoint its Chairman and Vice-Chairman from among its members, in accordance with the provisions of the Agency's by-laws. The offices of Chairman and Vice-Chairman shall be held for a term of three years or the time remaining on the Board as board members each case.

The board members shall serve 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 board member of the Agency's Governing Board requires exclusive time commitment.

The Agency's Governing Board shall take its decisions by a majority of its members and, in the event of a tie, its Chairman, or its Vice-Chairman in the absence of the latter, shall decide. The minimum quorum for a meeting shall be two board members. Regulations shall establish other necessary rules for its operation.

The Governing Board of the Agency shall hold ordinary meetings at least once a week, and extraordinary meetings when specially convened by its Chairman, either by himself or at the written request of two Board Members, in the manner and under the conditions determined by its internal operating regulations. Chairman may not refuse to issue the aforementioned call, and the respective meeting shall be held within two working days following the aforementioned request.

Article 30 quinquies.- Disqualifications and incompatibilities. The position of board member is incompatible with the exercise of any position or service, whether remunerated or not, rendered in the private sector. Likewise, it is incompatible with status as a member of the leadership of political parties, officials of the State Administration, and of any employment or service paid with fiscal or municipal funds, as well as with remunerated

or non-remunerated duties of advisor, director or employee of institutions, national or foreign autonomous bodies, State-owned 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 majority capital contributions or in equal proportion or, under the same conditions, representation or participation. Similarly, it is incompatible with any other remunerated or free service or employment in any branch of government.

The position of board member is compatible with the performance of academic positions in public or private institutions accredited by the State, up to a maximum of twelve hours per week.

The spouse or civil partner of any of the board members and their relatives up to and including the second degree of consanguinity may not be a board member or have a stake in the ownership of a company whose business purpose or line of business involves the collection, processing or communication of personal data.

In addition to the foregoing, it may not be appointed as a board member:

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 the 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 penalized, within the last five years, for a major or very major violation of the rules governing the processing of personal data and their protection.

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

All matters not expressly regulated in this article shall be governed by the provisions of Paragraph 2 of Title III of Decree with force of law No. 1-19,653, of 2000, of the Ministry General Secretariat of the Presidency, which establishes the consolidated, coordinated and systematized text of Law No. 18,575, Constitutional provisions for the General Terms of the State Administration.

Article 30 sexies.- Removal of board members and grounds for discharge. Board members shall be removed by the Supreme Court, at the request of the President of the Republic or the Chamber of Deputies by

resolution adopted by simple majority, or at the request of fifteen deputies, for inability, misconduct or gross negligence in the exercise of their duties. The Supreme Court shall hear the case in a plenary session specially convened for this purpose and, in order to agree on the removal, a majority of its members in office must vote in favour.

Apart from removal, the following shall be grounds for discharge from the office of board member:

a) Expiration of the term of office appointed.

b) Resignation before the President of the Republic.

c) Nomination to a popularly elected position.

d) Supervening disqualification or incompatibility, a circumstance to be determined by the majority of the board members, with the exclusion of the member affected.

In the event that one or more board members resign for any reason, a new board member shall be appointed by means of a proposal of the President of the Republic for the remaining term of office, subject to the same procedure set forth in Article 30 quater,

Should the board member who ceases to hold office by virtue of this article be the chairman or vice-chairman of the Governing Board of the Agency, a replacement shall be appointed in the manner provided for in article 30 quater, for the time remaining after the vacancy has arisen.

Article 30 septies.- Remuneration. Chairman of the Governing Board of the Agency shall receive a monthly gross remuneration equivalent to that of an Undersecretary of State, and shall be responsible for exercising the duties set forth in Article 30 nonies and other pertinent legal provisions.

Remuneration of the other board members shall be equivalent to 85% of the remuneration of the Chairman of the Governing Board of the Agency.

Article 30 octies.- Agency By-laws. The Agency's by-laws shall establish its operating rules. By-laws and their amendments shall be proposed by the Agency to the President of the Republic and their approval shall be provided for by means of a supreme decree issued through the Ministry of Economy, Development and Tourism.

Article 30h.- Duties and powers of the Chairman of the Governing Board of the Agency. The Chairman of the Agency's Governing Board shall be the Agency's head and shall represent the Agency both in and out of court. The Chairman

shall be in charge of the organization and administration of the Agency, as well as the oversight and hierarchical control over staff performance.

The Chairman of the Governing Board of the Agency shall be especially entrusted with the following Duties and powers:

a) To exercise the role of head of the entity.

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

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

d) To represent the Agency legally, in court and out of court.

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

f) To engage Agency's employees and to terminate their contracts, pursuant to the law.

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

h) To delegate specific powers or authorities to Agency officials.

i) To conduct the Agency's relations with public bodies and other agencies of the State and with individuals or entities subject to the Agency's oversight, as well as with international regulators of personal data.

j) To perform such other duties as may be so entrusted to it by the Agency's Governing Board.

In the absence of the Chairman of the Agency's Governing Board, the Vice-Chairman of the Governing Board shall undertake the duties and powers of the Chairman of the Agency's Governing Board.

Article 31.- Regulatory coordination with the Transparency Council. Should the Agency have to issue an instruction or rule of a general and mandatory nature that may impact the areas of competence of the Transparency Council, pursuant to the duties and powers set forth in Law No. 20,285, it will submit all the background information and request a report from the latter in order to avoid or prevent potential conflicts of rules and ensure coordination, cooperation and collaboration between the two 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 include the content of the opinion of the Transparency Council in the reasoning of the instruction or rule it issues Should the term expire and the report is not received, proceedings shall be taken as provided for in the second paragraph of Article 38 of Law No. 19,880.

In turn, in the event the Transparency Council must issue a general instruction that may clearly impact the areas of competence of the Agency, as per the duties and powers set forth under this law, the Transparency Council shall forward the background information and request a report from the Agency, the latter shall issue said report within thirty calendar days from the date on which the request was received. The Transparency Council shall include the content of the opinion of the Agency in the reasoning of the general instruction or rule it issues to such effect Should the term expire and the report is not received, proceedings shall be taken as provided for in the second paragraph of Article 38 of Law No. 19,880.

Article 32.- Agency staff and oversight. Individuals rendering services to the Agency shall be governed by the [Chilean] Labour Code.

Notwithstanding the foregoing, standards of integrity set forth in Law No. 20,880, on integrity in public service and prevention of conflicts of interest and under Title III of Decree with force of law No. 1-19,653, of 2000, of the Ministry General Secretariat of the Presidency, which establishes the consolidated, coordinated and systematized text of Law No. 18,575, Constitutional provisions for the General Terms of the State Administration shall be enforceable for this staff, and a clause to that effect shall be included in the respective contracts.

Individuals performing managerial duties in the Agency shall be recruited through public selection process carried out by the National Civil Service Office, on the basis of a shortlist of three candidates drawn up by the Upper Public Management Council for each case, pursuant to the rules governing the selection processes of the Upper Public Management under Law No. 19,882.

The Agency shall provide legal defence in case third parties bring legal actions against board members or the Agency's staff for formal acts or for actions or omissions in the performance of their duties. Said defence shall extend to all actions brought against them including those brought after they have ceased to hold office.

The defence referred to in the preceding paragraph shall not be applicable

in cases in which the formal acts, actions or omissions in question have constituted a cause for discharge attributable to the conduct of the respective official.

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

Likewise, the Agency shall be subject to the oversight of the Office of the Comptroller General of the Republic, as regards its staff and the examination and auditing of its accounts.

Resolutions of the Agency shall be exempt from the process of acknowledgment constitutionality by the Office of the Comptroller General of the Republic.

Article 32 bis.- On assets. Assets of the Agency shall consist of:

a) Contribution provided on an annual basis in the Public Sector Budget Law.

b) Movable and immovable property transferred to it or acquired by it for any reason and for the income received therefrom.

c) Donations accepted by the Agency. Donations shall not require filing legal certification/authorization referred to in Article 1401 of the [Chilean] Civil Code.

d) Inheritances and legacies accepted by the Agency, which shall always be done with the benefit of inventory. Such allocations shall be exempt from all taxes and from any levy or payment that may affect them.

e) Contributions from international cooperation.

Title VII

On infringements and their penalties, proceedings and liabilities

Article 33.- General liability regime. The party responsible for data, whether a natural or corporate body, under public or private law, which in its personal data processing operations infringes the principles set forth in Article 3 of this law, rights and obligations set forth in this law, shall be penalized pursuant to the provisions of the present Title.

First Paragraph

On liability, infringements and penalties applicable to natural or corporate bodies governed by private law

Article 34.- Minor, major and very major infringements. Infringements committed by parties responsible for data to the principles set forth in article 3°, as well as the rights and obligations set forth in this law, are classified, on the basis of their seriousness, as minor, major and very major.

Liabilities that may be incurred by a natural or corporate body for the infringements established under this law are deemed to be notwithstanding any other legal, civil or criminal liabilities that may correspond to it.

Article 34 bis.- Minor infringements. The following are considered minor infringements:

a) Total or partial non-compliance with the duty of information and transparency as set forth in Article 14 ter.

b) Lack of an updated and operative postal address, e-mail or equivalent electronic means of communication with the party responsible for data 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) Provide incomplete information in the registration or certification procedure of the model for the prevention of infringements.

g) 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.- Major infringements. The following are considered major 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 that 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) Omit to respond, respond delayed or deny the request with no reasonable 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 ter.- Very Major infringements. The following are considered major 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) Infringe the duty of secrecy or confidentiality of sensitive personal data and personal data related to the commission and penalties for criminal, civil, administrative and disciplinary offenses.

g) knowingly process, communicate or transfer sensitive personal data of children and adolescents in contravention of the rules set forth in this law.

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

g) Carry out massive processing of personal data contained in electronic records of criminal, civil, administrative and disciplinary breaches by state agencies, in the absence of legal authorization to that effect.

h) Knowingly carry out international data transfer operations in contravention of the rules set forth in this law.

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

f) Knowingly provide false, incomplete or clearly erroneous information in the registration or certification procedure of the model for the prevention of infringements

k) Failure to comply with the obligation set forth in Article 15 ter, where applicable.

Article 35.- Penalties. Penalties for infringements incurred by party responsible for data shall be as follows:

a) Minor infringements shall be penalized with a written warning or a fine of up to 100 unidades tributarias mensuales [UTM]

b) Major infringements shall be penalized with a fine of up to 5,000 unidades tributarias mensuales [UTM] or, in case of companies, a fine of up to the equivalent of 2% of the annual income from sales and services and other business activities for the last calendar year, with a maximum of 10,000 UTM.

b) Major infringements shall be penalized with a fine of up to 10,000 unidades

tributarias mensuales [UTM] or, in case of companies, a fine of up to the equivalent of 4% of the annual income from sales and services and other business activities for the last calendar year, with a maximum of 20,000 UTM.

The Agency shall indicate in each particular case the actions aimed at remedying the causes that gave rise to the penalty, which shall be adopted within a term not exceeding 60 days, otherwise a surcharge of 50% of the fine shall be imposed, notwithstanding the provisions of article 49. In the event of recidivism, pursuant to literal a) of the second paragraph of article 36, the Agency may apply a fine of up to three times the amount corresponding to the infringement committed.

Article 36.- Extenuating and aggravating circumstances of liability. Are considered extenuating circumstances:

1) Unilateral remedial actions taken by the party responsible and the remedial agreements reached with the data subjects affected.

2) Collaboration provided by the offender in the administrative inquiry carried out by the Agency.

3) Absence of previous penalties by the party responsible for data

4) Self-reporting before the Agency. Along with the self-reporting, the offender shall communicate the measures adopted for the termination of the facts that originated the infringement or the mitigation measures implemented, as appropriate.

5) Diligent performance of its duties of management and oversight for the protection of personal data subject to processing, which shall be verified with the certificate issued pursuant to the provisions of Article 51.

Are considered aggravating circumstances:

a) recidivism. Recidivism exists when the party responsible has been penalized on two or more occasions, in the last thirty months, for infringement of this law. Resolutions applying the respective penalties must be final or enforceable.

b) The continuing nature of the infringement.

c) Putting at risk the security of the rights and freedoms of data subjects in relation to their personal data.

Article 37.- Determination of Fines. For the purpose of determining the amounts of the fines set forth in this law, the Agency shall apply the following criteria in a reasonable manner:

1. Seriousness of the misconduct

2. The misconduct was committed with a lack of diligence or care in those case in which these elements are not considered as part of the infringement.

3. Damage caused by the infringement, especially the number of data subjects affected.

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

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

6. Economic capacity of the offender.

7. Penalties previously applied by the Agency under the same circumstances.

8. Extenuating and aggravating circumstances.

In case a misconduct gives rise to two or more infringements, or when one infringement constitutes a means to commit a second infringement, a single fine shall be imposed, based on the severity of the most serious infringement. Should there be two or more infringing misconducts, independent of each other, the penalties corresponding to each of them shall be accumulated.

Fines must be paid at the General Treasury of the Republic, through the in-person or digital means provided by the Treasury, within ten working days after the Agency's resolution becomes final. Payment voucher shall be submitted to the Agency within ten working days after the payment has been made.

Article 38.- Accessory penalties. Where fines are imposed for repeated very major 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 party responsible for data, for a period of up to thirty days. This suspension shall not affect the data storage by the party responsible.

The suspension ordered by the Agency as an accessory penalty may be partial or total, and may not be decreed when thereby affecting the rights of data subjects.

During this period the party responsible shall adopt the necessary actions in order to adjust its operations and activities to the requirements set forth in the resolution ordering the suspension.

Should the party responsible fail to comply with the provisions of the

temporary suspension resolution, this measure may be extended for indefinite successive periods of a maximum of thirty days, until such time as the party responsible complies with the order.

In case the suspension affects an entity subject to oversight by a public oversight entity, the Agency shall previously inform the corresponding regulatory authority, in order to protect the rights of the users of such entity.

Article 39.-National Registry of Penalties and Compliance The National Registry of Penalties and Compliance, to be managed by the Agency, is hereby created. Registry shall be public and access shall be free of charge. It shall be consulted and kept in electronic form.

This registry shall include those parties responsible for data penalized for infringing the rights and obligations set forth in this law, differentiated on the basis of the seriousness of the infringement. Furthermore, the misconduct penalized, the extenuating and aggravating circumstances of liability and the penalties imposed shall be stated. It shall also include those parties liable for adopting certified models for the prevention of infringements, currently in force.

Annotations in the registry shall be publicly accessible for a period of five years from the date on which the annotation was made.

Article 40.- Statute of limitations. Actions to prosecute liability for the infringements provided for in this law are subject to a four-year statute of limitations, counted from the occurrence of the event giving rise to the infringement.

In the case of continuous infringements, the statute of limitations for the referred actions shall be counted from the day on which the infringement ceased.

Statute of limitations is interrupted with the notification of the initiation of the corresponding administrative proceeding.

Penalties imposed for an infringement of this law shall be subject to the statute of limitations within three years, counted from the date on which the resolution imposing the penalty becomes enforceable.

Second Paragraph

On administrative procedures

Article 41.- Procedure for administrative writ for the protection of constitutional rights. The data subject may complain before the Agency

whenever the party responsible has denied a request made pursuant to article 11 of the present law, or has failed to respond to such request within the legal term set forth in said article.

The claim filed shall be processed under the following rules:

a) It shall be filed in writing, in physical or electronic format, within 15 business days from the date of receipt of the negative response from the party responsible for data or upon expiration of the deadline set by the party responsible for responding to the request made by the data subject. The claim shall specify the decision challenged in the event of rejection or failure to respond and be accompanied by all the background information on which the claim is grounded and indicate a postal address or an e-mail address or other equivalent electronic means where notifications shall be made.

b) Upon the filing of the claim, at motivated request of the data subject and except in justified cases, the Agency may suspend the processing of the personal data with respect to the data subject and which are the object of the claim, with prior hearing of the party responsible for data.

c) Upon receipt of the claim, the Agency shall determine, within the following 10 business days, whether it complies with the requirements set forth in the preceding paragraph in order to be accepted for processing. In the event the claim is not admitted, the Agency's decision shall be well founded and notified to the subject. In any case, the claim shall be deemed to have been accepted for processing if the Agency does not issue a decision within the aforementioned term.

d) Upon acceptance of the claim for processing, the Agency shall notify the party responsible for data, who shall be given 15 business days to respond to the claims, attaching all the background information it deems pertinent. Notifications to the party responsible shall be made to its postal address, e-mail address or other equivalent electronic means referred to in letter c) of Article 14 ter.

e) On expiration of this term, regardless of whether the party responsible for data has responded or not, and provided there are substantial, pertinent and controversial facts, the Agency may open an evidentiary term of 10 business days whereby the parties may submit all the means of proof they deem convenient.

f) The party responsible for data may accept the claim in its response, provided that, in such case, it must include the background information or testimonies that proves this circumstance. Verified the foregoing, the data subject shall be notified and shall have 10 days to assert his/her rights. On

expiry of the term, the Agency will proceed to file the records, prior application of the penalty and/or instruction to the party responsible for data, where appropriate.

g) The Agency shall be broadly empowered to request background information or reports that contribute to its decision. It may convene the parties to a hearing and urge them to reach a settlement. Opinions expressed by Agency officials at this hearing shall not disqualify them from continuing to hear the case in the event a settlement is not reached. Upon settlement, the case file will be closed.

h) Decision on the claim shall be grounded and rendered by the Agency. procedure for administrative writ for the protection of constitutional rights may not exceed 6 months.

i) Decision of the Agency not to accept a claim for processing as well as the decision resolving the claim may be judicially challenged within a term of 15 business days from its notification, through the procedure set forth in article 43.

Claims and requests for suspension of processing made in the event of refusal of a request for temporary blocking shall be resolved by the Agency within a maximum period of 3 business days, with no need to hear the parties beforehand.

Article 42.- Administrative procedure upon infringements of law. Assessment of the infringements committed by parties responsible for data for non-compliance or breach of the principles set forth in article 3°, rights and obligations established herein, as well as the application of the corresponding penalties, shall be subject to the following particular provisions:

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

b) The Agency may initiate a penalizing procedure, ex officio or upon request of a party, as a result of a supervision process or as a consequence of a claim filed by a data subject, by virtue of the procedure set forth in Articles 23 and 41 of the present Law. In the latter instance, the receipt of the claim must be evidenced. Along with the opening of the case, the Agency shall designate an official responsible for the investigation of the proceeding.

c) The Agency shall file charges against the party responsible for data, describing the events that constitute the infringement, principles and obligations not met or breach by such party responsible, legal provisions violated, and any other background information that might help support said claim.

d) Charges to the party responsible for data shall be notified at its postal address, e-mail address or other equivalent electronic means as indicated in

letter c) of article 14 ter.

e) The party responsible for data will be given a period of 15 business days to present his or her defence. On that occasion, the party responsible for data may submit all the background information he/she deems pertinent to discredit the facts alleged. Together with the discharges, the party responsible shall provide an e-mail address through which all other communications and notifications shall be made.

f) Upon receipt of the discharges or once the term granted for such purpose has expired, the Agency may open an evidentiary term of 10 days in the event substantial, pertinent and controversial facts exist.

g) The Agency shall allow the measures or evidentiary proceedings requested by the party responsible in its discharges, provided that they are pertinent and necessary. If rejected, the decision must be substantiated.

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

i) The Agency shall be broadly empowered to request background information or reports that contribute to its decision.

j) The decision bringing the penalizing procedure to an end must be well founded and resolve every matter raised in the file, ruling on each of the allegations and defences made by the party responsible for data and shall contain the sentence pronouncing the breach or violation of the principles, rights and obligations provided in the law by the party responsible or its acquittal, as applicable. Should the Agency consider that the infringement has been verified, it shall weigh the circumstances that aggravate or extenuate the offender's liability in the same decision and shall impose the corresponding penalty, pursuant to the seriousness of the infringement committed.

k) The decision stating the non-compliance or violation of the principles, rights and obligations under this law and thus enforcing the corresponding penalty shall be well-founded. This decision must indicate the administrative and judicial remedies available against said decision as provided for in this law, the bodies before which such remedies are to be filed and the deadlines for filing them. The decision of the Agency that resolves the proceedings for violation of the law shall be judicially challengeable pursuant to the following article.

l) The administrative procedure for violation of the law shall not exceed 6 months. Should more than 6 months have elapsed since the date of the

certification referred to in letter b) of this article and the Agency has not resolved the claim, the party concerned may file a complaint on illegality under the terms provided for in the following article.

Third Paragraph

On the judicial claim proceeding

Article 43.- On the judicial claim proceeding. The interested individuals or corporate entities who deem that an administrative act halts the procedure, or a final or end decision stemmed from the Agency, is illegal, may file a complaint on illegality before the Santiago Court of Appeals, or before an Appellate Court from the location where the party filing the claim is domiciled, whichever the latter deems fit. The complaint shall be filed within 15 business days following the notification of the challenged decision, under the following rules:

a) The claimant shall state accurately in his/her writ, the decision being challenged, the legal provision(s) alleged to have been infringed, the manner in which the infringement has occurred, and, if applicable, the reasons why the act causes the claimant grievance.

b) The Court may declare the claim inadmissible if the writ does not comply with the conditions set forth in letter a) above. Likewise, it may decree an injunction against further process when the execution of the challenged act may cause irreparable damage to the appellant.

c) Upon receipt of the claim, the Court shall request a report from the Agency, granting the latter a period of 10 days to that effect.

d) Upon answering (and commenting) within the term provided by the Court or having been deemed to have been answered (and commented) in default of appearance, the Court may open a period of evidence, if it deems it necessary, which shall be governed by the procedural rules set forth in the [Chilean] Code of Civil Procedure.

e) After expiration of the period of evidence, it shall be ordered to set the case for a hearing. The hearing of this case will enjoy preference for listing in the table.

f) Should the Court uphold the claim, it will decide in its ruling on the existence of a grievance and will order, as appropriate, the rectification of the challenged

act and the issuance of the respective decision, where appropriate.

g) In the case of claims against a decision that resolves a penalizing procedure, the Court may confirm or revoke the challenged decision, establish or dismiss the commission of the infraction, as applicable, and maintain, annul or modify the penalty imposed on the party responsible or its acquittal, as the case may be.

h) All matters not regulated by this article shall be governed by the rules set forth in the Organic Code of Courts and the Code of Civil Procedure, as appropriate.

Fourth Paragraph

On the liability of the State instrumentalities, of the authority or superior head of the body and of the officials thereof.

Article 44.- Administrative liability of the superior head of State instrumentalities. The superior head of a State instrumentality shall ensure that the respective body carries out its personal data processing operations and activities in compliance with the principles, rights and obligations set forth in Title IV of this law.

Likewise, State instrumentalities shall submit to the measures aimed at correcting or preventing infringements stated by the Agency or to the compliance or infringement prevention programs of Article 49.

Violations of the principles set forth in Article 3°, rights and obligations that State instrumentalities may commit are categorized in Articles 34 bis, 34 ter and 34 quater and shall be penalized by a fine of 20% to 50% of the monthly remuneration of the superior head of the offending State instrumentality. Amount of the fine shall be assessed taking into account the seriousness of the infringement, the nature of the data processed and the number of data subjects affected. Circumstances extenuating the offender's liability shall also be taken into consideration when assessing the penalty.

Should the State instrumentality persist with the violation, the superior head of the State instrumentality shall be subject to double the original penalty imposed and suspension from office for a period of 5 days.

In the case of sensitive personal data, the fine shall be 50% of the monthly remuneration of the superior head of the State instrumentality and the

suspension from office for up to 30 days.

Infringements committed by a State instrumentality in the processing of personal data shall be determined by the Agency pursuant to the procedure set forth in Article 42.

Upon the constitution of the infringement, the administrative penalties set forth in this article shall be applied by the Agency. Furthermore, the Office of the Comptroller General of the Republic, at the request of the Agency, may, pursuant to the provisions of its organic law, initiate administrative proceedings and propose the corresponding penalties.

The complaint on illegality set forth in Article 43 may be filed against the Agency's decisions.

Penalties provided for in this article shall be published on the website of the Agency and of the respective instrumentalities or bodies within 5 business days from the date on which the respective decision becomes final.

Article 45.- Liability of the official in breach. Notwithstanding the provisions of the preceding article, if it were determined, in the relevant administrative procedure, that there are individual liabilities of one or more officials from the State instrumentality, the Office of the Comptroller General of the Republic, upon a request from the Agency, shall launch a summary inquiry to determine the liability of each of those officials, or, if applicable, it shall do so in the administrative procedure already began. Penalties for offending officials shall be determined as provided for in the Administrative By-laws.

In the event the corresponding administrative procedure proves that any of the officials involved is liable for any of the very serious infringements set forth in Article 34 quater of this law, such behaviour shall be considered a serious violation of administrative integrity.

Article 46.- Duty of reserve and confidentiality for officials. Officials of State instrumentalities who process personal data and particularly those relating to sensitive personal data or data relating to the commission and penalization of criminal violations and civil, administrative and disciplinary offenses, must observe secrecy or confidentiality as regards the information they become aware of in the performance of their duties and refrain from using such information for a purpose other than that consistent with the statutory tasks of the respective State instrumentality 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 By-laws, it shall be considered that acts that constitute infringements of this provision

represent a serious violation of the principle of administrative integrity, notwithstanding any other penalties and liabilities that may apply.

Whenever, in compliance with a legal obligation, a State instrumentality communicates or transfers to another State instrumentality data protected by secrecy or confidentiality rules, the recipient State instrumentality and its officials shall process such data while maintaining the same obligation of secrecy or confidentiality.

Fifth paragraph

On civil liability

Article 47.- General rule. The party responsible for data shall compensate the property and non-property damage caused to the subject(s), in case its data processing operations violate the principles set forth in article 3°, rights and obligations provided for in this law and cause them any harm. The foregoing does not preclude 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 execution of the decision that favourably resolved the complaint filed with the Agency or the sentence is final and enforceable, in the case of having filed a complaint on illegality, and shall be processed pursuant to the rules governing the summary procedure set forth in Articles 680 et seq. of the Code of Civil Procedure.

Civil actions arising from a violation of this law shall be subject to the statute of limitations within 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.- Preventing infringements. Parties responsible for data, whether natural or corporate entities, either state or private, shall adopt actions aimed at preventing the commission of the infringements set forth in Articles 34 bis, 34 ter and 34 quater.

Article 49.- Infringement prevention model. Parties responsible for data may voluntarily adopt an infringement prevention model consisting of a compliance program.

The compliance program shall contain at least the following elements:

a) Appointment of a personal data protection officer.

b) Definition the means and authorities of the data protection officer.

c) Identification of the type of information processed by the entity, the territorial scope in which it operates, the category, class or types of data or databases it administers, and the profiling of data subject(s).

d) Identification of corporate the activities or processes, be them typical or occasional, which context triggers or increases the risk of perpetrating the violations set forth in articles 34 bis, 34 ter, and 34 quater.

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

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

g) The existence of internal administrative penalties, as well as procedures for reporting or penalizing those who fail to comply with the system for the prevention of infringements.

The internal regulation resulting from the implementation of the program, where appropriate, shall be expressly made an obligation in the employment or service contracts of all workers, employees and service providers of the entities acting as party responsible for data or third parties performing the processing, including the top executives thereof, or as an obligation of the internal regulations referred to in Articles 153 et seq. of the [Chilean] Labour Code. For the latter case, the publicity measures set forth in Article 156 of the same Code must be carried out.

Article 50.- Powers of the officer. The party responsible for data may appoint a personal data protection officer.

The data protection officer shall be appointed by the highest directive or administrative authority of the party responsible for data. The board of directors, a managing partner or the supreme corporate or service authority, as applicable, shall be deemed to be the highest management or administrative authority.

The data protection officer shall be autonomous from the administration in matters related to this law. The owner or the highest heads of micro, small and medium-sized companies may personally assume the duties of data

protection officer.

The data protection officer may perform other duties and roles, while maintaining independence in his or her duties. The party responsible shall ensure said duties and roles do not result in any sort of conflict of interests.

Companies or legal entities that belong to a same corporate group, affiliates, or companies subject to a same controller, pursuant to the Law on the Securities Market, may appoint a sole officer for data protection, 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 performance of his or her duties.

Data subjects may contact the data protection officer in relation to all issues concerning 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 with regard to the personal data he/she becomes aware of in the performance of his/her duties. Public officials who perform these duties and violate this duty of secret or confidentiality shall be penalized pursuant to the provisions of Articles 246 to 247 bis of the [Chilean] Penal Code. The party responsible shall be liable for violation of the duty of secret or confidentiality that his or her protection officer was required to comply with, notwithstanding any recourse actions that may be brought against him or her.

The party responsible for data shall ensure that the officer has sufficient means and authorities for the performance of his/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 party responsible for data, third party data processors or agents and dependents of the party responsible, with respect to the legal and regulatory provisions relating to the right to the protection of personal data and the regulation governing its processing.

b) To promote and participate in the policy issued by the party responsible for data with respect to the protection and processing of personal data.

c) To supervise compliance with this law and the policy issued by the party responsible, within the scope of its competence.

d) To ensure the ongoing training of persons involved in data processing operations.

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

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

g) To respond to queries and requests from data subjects.

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

Article 51 (52).- 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 said model.

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

A set of rules and 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 (53).- Validity of certificates. Certificates issued by the Agency shall be valid for 3 years. Notwithstanding the foregoing, they shall be null and void in the following cases:

a) By revocation by the Agency.

b) By decease of the party responsible for data in the case of natural individuals.

c) By dissolution of the body corporate.

d) By an enforceable judicial decision.

e) By voluntary cessation of the activity of the party responsible for data.

The termination of the validity of a certificate for any of the reasons mentioned above shall not be held against third parties until it is removed from the registry.

Article 53 (54).- Revoking the certification. The Agency may revoke the certification referred to in the preceding articles, provided that the party responsible does not comply with the provisions of this Paragraph. For this purpose, the Agency may request any information that may be necessary for the exercise of its duties.

The parties responsible may be exempted from providing the requested information provided that such information is covered by an obligation of secrecy or confidentiality, subject to proof of such circumstance.

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

To re-apply for a certificate that has been revoked by the Agency, the party responsible 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 (55).- General rule for the processing of personal data. The processing of personal data by 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 the other special courts created by law, is lawful when carried out for the fulfilment of their statutory tasks, within the scope of their competencies and, pursuant to the particular rules set forth in their respective organic laws and the provisions of Title IV of the present law applicable to State instrumentalities, save for the provisions of Article 14 quinquies and Articles 44 to 46, referring to the intervention of the Office of the Comptroller General of the Republic in the assessment of administrative liability and the enforcement 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 party responsible 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.

Article 55 (56).- 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 1.- Amendments to Laws No. 19,628, on protection of personal data, and No. 20,285, on access to public information, and Decree with force of law 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 2.- The regulations referred to in the present law shall be issued within 6 months following the publication of this law in the Official Gazette.

Article 3.- Within 60 days prior to the entry into force of the amendments to Law No.19,628, contained in Article 1 of this Law, the Civil Registry and Identification Office shall eliminate the registry of personal databases as provided for in the existing Article 22 of Law No. 19,628.

Article 4.- The first appointment of board members of the Governing Board of the Personal Data Protection Agency and of the president and vice-president of the Governing Board of the Agency shall be carried out within 60 days prior to the entry into force of the present 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.

Nonetheless, board members shall only assume their positions upon the entry into force of this law, pursuant to the provisions of the first interim article.

The Agency's by-laws shall be presented to the President of the Republic, pursuant to Article 30 octies hereof, within 90 days following the entry into force of the present law.

Article 5.- State instrumentalities who decide 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 6.- 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 Decree with force of law 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 establishes rules on the protection of consumers' rights, is replaced by the following:

"Article 15 bis.- The provisions contained in Articles 2 bis letter b) and 58 bis shall be applicable with respect to the personal data of consumers, within the framework of consumer relations".

/Carey

CHILEAN LAW 19,628 ON **PERSONAL DATA PROTECTION**