BILL

NEW REGULATION:
PERSONAL DATA LAW

After seven years of processing, last August 26, the Congress approved the bill that regulates the protection and processing of Personal Data, creating the Agency for the Protection of Personal Data, corresponding to bulletins No. 11,092-07 and 11,144-07 (hereinafter, the "Bill"). This initiative implies a profound reform of Law No. 19,628, previously known as the *"Law on the Protection of Private Life"*. Therefore, preventive constitutional review by the Constitutional Court is still pending, as well as its subsequent promulgation and publication for it to enter into force.

Due to the significant impact that this Bill will have in our country, as it establishes restrictions, obligations, and penalties applicable to the processing of Personal Data, in addition to changing the culture regarding how this data is shared and managed, Guerrero Olivos will publish a series of informative newsletters detailing the scope of the Bill, structured by areas of application. In this first issue, we will present a general summary of the most relevant aspects regulated by the Bill.

1 SCOPE OF APPLICATION:

The processing of Personal Data will be governed by the new law in the following four scenarios:

1.1 When the Controller or agent is established or incorporated in national territory.

1.2 When the Controller or agent, regardless of their place of establishment or incorporation, conducts operations on behalf of a Controller established or incorporated in Chile.

1.3 When the Controller or agent is not established in Chile but offers goods or services to data subjects located in Chile.

1.4 When the processing of Personal Data is carried out by a Controller who, while not established in Chile, is subject to national legislation due to a contract or international law provisions.

2 DEFINITIONS:

The Bill provides more exhaustive definitions of several terms already contained in Law No. 19,628, deleting some and adding new definitions. The most relevant ones are mentioned below:

2.1 Personal Data: *"Any information linked or related to an identified or identifiable natural person. An identifiable person is considered to be anyone whose identity can be determined, directly or indirectly, in particular by means of one or more identifiers, such as name, identification number, or the analysis of elements specific to the physical, physiological, genetic, psychological, economic, cultural, or social identity of that person."*

2.2 Sensitive Personal Data: *"Those personal data that refer to the physical or moral characteristics of individuals, or to facts or circumstances of their private life or intimacy, revealing their ethnic or racial origin, political, trade union, or guild affiliation, socioeconomic status, ideological or philosophical convictions, religious beliefs, health data, human biological profile, biometric data, sexual life information, sexual orientation, and gender identity."*

2.3 Consent: *"Any expression of free, specific, unequivocal, and informed will, granted through a declaration or a clear affirmative action, by which the data subject, their legal representative, or agent, as appropriate, authorizes the processing of personal data concerning them."*

2.4 Public Access Sources: *"All those databases or sets of personal data whose access or consultation can be lawfully carried out by any person, such as the Official Gazette, media, or public records provided by law. The processing of personal data from publicly accessible sources will be subject to the provisions of this law."*

2.5 Data Controller or Controller: *"Any individual or legal person, public or private, who determines the purposes and means of processing personal data, regardless of whether the data is processed directly by them or through a third party or agent."*

3 PRINCIPLES:

The Bill establishes that the processing of Personal Data must be governed by the following principles:

3.1 Lawfulness and Loyalty: The Controller must bear the burden of proving the lawfulness of the processing.

3.2 Purpose: Data must be collected for specific, explicit, and lawful purposes, and processing must be limited to fulfilling those purposes.

3.3 Proportionality: Data processing must be limited to what is necessary, adequate, and relevant in relation to the purposes of the processing.

3.4 Data Quality: Personal Data must be accurate, complete, up-to-date, and pertinent in relation to its origin and the purposes of the processing.

3.5 Accountability: The entity processing Personal Data will be legally responsible for complying with these principles and the obligations and duties established in this law.

3.6 Security: The Controller must ensure appropriate security standards, protecting Personal Data from unauthorized or unlawful processing, loss, leakage, damage, or destruction.

3.7 Transparency and Information: The Controller must provide the data subject with all the necessary information to exercise their rights.

3.8 Confidentiality: The Controller of Personal Data and those who have access to it must maintain confidentiality, and the Controller must take appropriate measures for this purpose.

4 RIGHTS OF THE DATA SUBJECT:

The Bill establishes a series of rights for the data subjects (individuals to whom the data belongs); rights that are personal, non-transferable, and non-waivable, and cannot be limited by any act or agreement. These rights are:

4.1 Access: The right to request and obtain from the Controller confirmation of whether their Personal Data is being processed, to access it if applicable, and to receive information about its content and origin, purpose, identity of recipients, and the duration of the processing, among other details.

4.2 Rectification: The right to request and obtain from the Controller modifications or updates to their Personal Data when it is being processed and is inaccurate, outdated, or incomplete.

4.3 Deletion: The right to request and obtain from the Controller the deletion or removal of their Personal Data, for example, if it is no longer necessary for the intended purpose or if Consent has been revoked.

4.4 Opposition: The right to request and obtain from the Controller the termination of specific data processing based on the legal grounds provided by law. For example, if the lawful basis of the processing is solely the Controller's legitimate interest, if the processing is exclusively for marketing purposes, or if its only legal foundation is that the data was obtained from a public access source. Additionally, the Bill includes the right to object to processing consisting of automated decisions, including profiling, that produces legal effects or significantly affects the data subject.

4.5 Portability: The right to request and obtain from the Controller a copy of their Personal Data in a structured, generic, and commonly used electronic format that allows for interoperability across different systems, as well as to communicate or transfer them to another Data Controller, provided the processing is automated and based on the Consent of the data subject. The data subject may even request that their data be transmitted directly from Controller to Controller.

5 SOURCES OF LEGALITY FOR DATA PROCESSING

5.1 The general rule is the Consent of the data subject: Consent must be free, informed, and specific as to its purpose or purposes. It must be expressed in advance and unequivocally through a verbal, written declaration, or by an equivalent technological means or affirmative action that clearly demonstrates the data subject's will.

This Consent can be revoked by the data subject at any time and without cause through means equivalent or similar to those already mentioned.

5.2 Other lawfulness sources for Data Processing: In the absence of the data subject's Consent, other sources of legality include:

(i) Processing of data related to financial, economic, banking, or commercial obligations, and conducted in accordance with the rules of Title III (which regulates the processing of this type of data).

(ii) When the processing of data is necessary to comply with a legal obligation or as provided by law.

(iii) When data processing is necessary for the execution or performance of a contract between the parties.

(iv) When the processing satisfies the legitimate interest of the Controller or a third party, provided it does not affect the rights and freedoms of the data subject.

(v) When necessary for the exercise or defense of rights before the courts of law and public authorities.

It is the responsibility of the Controller to demonstrate the legality of the processing.

It is important to highlight that the processing of Sensitive Personal Data, biometric data, and other special categories (such as data pertaining to children and adolescents, for historical, statistical, or scientific purposes, as well as geolocation data) is subject to specific and different regulations.

6 OBLIGATIONS AND DUTIES OF THE DATA CONTROLLER:

The Data Controller has the following obligations and duties:

6.1 Obligations:

(i) Inform and provide the data subject with the information that demonstrates the legality of the data processing being carried out, and promptly supply such information when requested.

(ii) Ensure that Personal Data is collected from lawful sources, for specific, explicit, and lawful purposes, and that its processing is limited to fulfilling these purposes.

(iii) Communicate or transfer accurate, complete, and up-to-date information.

(iv) Delete or anonymize the Personal Data of the data subject when obtained for the execution of pre-contractual measures.

(v) Comply with the other duties, principles, and obligations governing the processing of Personal Data as stipulated in this law.

6.2 Duties:

(i) Secrecy or confidentiality: The obligation to maintain secrecy or confidentiality regarding the Personal Data of a data subject, unless the data subject has made it publicly known.

(ii) Information and transparency: Duty to provide and maintain permanently available to the public, on their website or any other equivalent information medium, certain information, such as the policy on the processing of Personal Data, the identification of the Controller and their legal representative, categories or types of data processed, among others.

(iii) Protection by Design and by Default: Duty to apply appropriate technical and organizational measures by design prior to and during the processing of Personal Data.

(iv) Adoption of security measures: The duty to adopt the necessary measures to ensure compliance with the principle of security.

(v) Report breaches of security measures: Duty to report to the Agency for Personal Data (mentioned in the following section), by the most expedient means possible and without undue delay, any breaches of security measures that result in destruction, leakage, loss, or accidental or unlawful alteration of the Personal Data being processed or unauthorized disclosure or access to such data when there is a reasonable risk to the rights and freedoms of the data subjects.

7 CREATION OF THE AGENCY FOR THE PROTECTION OF PERSONAL DATA:

The law contemplates the creation of the Agency for the Protection of Personal Data (the "Agency"), which will be an autonomous public corporation, of a technical and decentralized nature, with legal personality and its own assets, whose primary objective will be to ensure the effective protection of the rights that guarantee individuals' privacy and their Personal Data. Therefore, its work will be essential for the efficacy of the law.

Among its key functions and powers are:

7.1 Issue mandatory rules on the processing of Personal Data after public consultation.

7.2 Applying and interpreting laws and regulations on the protection of Personal Data.

7.3 To supervise compliance with the provisions contained in the law.

7.4 To determine infractions and apply penalties.

7.5 To resolve claims from data subjects and develop outreach programs on the protection of Personal Data.

7.6 Collaborate with national and international entities by means of agreements and certify models for the prevention of infringements.

8 MODEL FOR PREVENTING VIOLATIONS:

Data Controllers may voluntarily adopt a model for preventing violations ("Prevention Model"), consisting of a compliance program which, if certified by the Agency, will serve as a mitigating factor for liability.

The Prevention Model must contain at least the following elements:

8.1 Designation of a Data Protection Officer.

8.2 Definition of means and powers of the Data Protection Officer.

8.3 Identification of the type of information the entity processes, the territorial scope in which it operates, the category, class, or types of Data or databases it manages, and the characterization of the data subjects.

8.4 Identification of the usual or sporadic activities or processes of the entity in which the risk of committing violations may be generated or increased.

8.5 Establishment of protocols, rules, and specific procedures that allow individuals involved in the indicated activities or processes mentioned above to plan and execute their tasks in a manner that prevents the occurrence of the referenced violations.

8.6 Internal reporting mechanisms for compliance with the provisions of this law and reporting mechanisms to the Agency.

8.7 Existence of internal administrative sanctions and procedures for reporting or disciplining individuals who violate the prevention system.

9 LIABILITY REGIME:

Data Controllers shall adopt a proactive and responsible posture to ensure that Data processing is carried out in a way that prevents or mitigates possible damages. Although there is a catalog of infringements to guide data subjects, the Agency will be in charge of defining the limits through regulatory standards and their interpretation, which will demand a continuous review of the criteria adopted.

In view of the abovementioned, the text of the Bill classifies infringements according to their seriousness, into minor, serious and very serious, while fines are determined by virtue of their classification, reoccurrence and the existence of mitigating or aggravating circumstances.

Thus, the penalties for violations committed by Data Controllers will be as follows:

a) Minor Violations: Written warning or fine of up to 5,000 UTM (Monthly Tax Units) (approximately equivalent to USD 357,158.23 . Examples of minor violations are infraction of the duty of information and transparency, not specifying a means of communication with the Data Controller, not responding to a request from a data subject, or any other violation not classified as serious.

b) Serious Violations: Fine of up to 10,000 UTM (approximately equivalent to USD 714,337.99). Examples of serious violations include processing Personal Data without the data owners' Consent or a lawful basis for doing so, violating confidentiality obligations, processing data of children and adolescents in violation of the law, etc.

c) Very Serious Violations: Fine of up to 20,000 UTM (approximately equivalent to USD 1,428,675.99). Examples of very serious violations include fraudulent data processing, maliciously using Data for purposes other than those consented to, deliberately omitting to report security breaches, etc.

In each case, the Agency will indicate the measures to remedy the causes that led to the penalty, and if the defect is not remedied within 60 days, a surcharge of up to 50% of the imposed fine will be added.

Finally, in the event of a repeat offense, a fine of up to three times the amount assigned may be applied, or between 2% (serious infringements) or 4% (very serious infringements) of the annual income from sales and services and other activities of the business in the last calendar year, whichever is more severe. However, it should be noted that this sanction only applies to larger companies, i.e., those not covered by Law 20,146.

The law establishes a catalog of mitigating and aggravating circumstances within the sanctioning system and includes a special administrative procedure for determining violations of the law, as well as an appeal for illegality before the Court of Appeals of Santiago or where the claimant is domiciled, in case of disagreement with the resolution of the administrative procedure, as well as in other circumstances established by law.

10 EFFECTIVE DATE

According to the first transitional article of the Bill, its entry into force will be on the first day of the twenty-fourth month following its publication in the Official Gazette.

contact

Juan Enrique Allard
jeallard@guerrero.cl

Rocío García de la Pastora
rgarciadelapastora@guerrero.cl

Pedro Pellegrini
ppellegrini@guerrero.cl

Tomás Garnham
tgarnham@guerrero.cl

Alejandra Leiton
aleiton@guerrero.cl

Valentina Mora
vmora@guerrero.cl

Diego Morandé
dmorande@guerrero.cl

Antonia Paredes
aparedes@guerrero.cl

María José Rodríguez
mjrodriguez@guerrero.cl

Joaquín Valenzuela
jvalenzuelac@guerrero.cl

Personal Data