24 de julio de 2024

Joint Committee approved the final text of bill which amend Law N° 19,628 on Protection of Private Life

Carey y Cía. Ltda.
Isidora Goyenechea 2800, Piso 43
Las Condes, Santiago, Chile.
www.carey.cl

On July 24, 2024, the joint committee approved what should be the final draft of the bill that amends Chilean Data Protection Law N° 19,628 (the "Law").

After this stage, the draft of the Law needs to be approved by both the Senate and the Chamber of Deputies. Upon approval, it will be sent to the President of the Republic for presidential approval and eventually will be subject to review by the Constitutional Court.

The purpose of the Law is to update the regulatory framework regarding the protection and processing of personal data, in line with international standards on the handling of personal data, inspired by the General Data Protection Regulation (GDPR) of the European Union, to increase the standards of protection and to face the challenges of the digital economy, seeking a balance between the privacy of individuals and the free flow of information.

In this way, the new Law involves the implementation of relevant aspects and changes regarding personal data protection, among which we highlight the below:

I. *Data Protection Agency*

The Law establishes the creation of the Data Protection Agency (the "Agency"), which will ensure the effective protection of the privacy and personal data of individuals and will supervise the observance of the Law.

In particular, the Agency will have i) **regulatory** powers, such as issuing instructions and general rules, applying and interpreting legal and regulatory rules, proposing rules to ensure the protection of personal data; ii) **supervisory** powers, as regards compliance with the provisions of the Law by data controllers, and in resolving requests and claims made by data subjects; and iii) **sanctioning** powers, by exercising the power to impose penalties and determining the infringements and breaches incurred by data controllers.

II. *Scope of Application*

The Law applies to any natural or legal person, including public bodies, that processes personal data, except for processing carried out in the exercise of the freedom to express opinions and to inform, as well as to processing carried out by natural persons in connection with their personal activities.

Regarding the **territorial scope**, the Law will apply to all processing of personal data carried out by those "**controllers**" (defined as "*any natural or legal person, public or private, who decides about the purposes and means of the processing of personal data*") or "**data processors**" (i.e. "*the natural or legal person who processes personal data, on behalf of the data controller*") (i) established in the national territory; (ii) who carry out personal data processing operations on behalf of a controller established in the national territory; and (iii) whose data processing operations are intended to offer goods or services to data subjects located in Chile.

In this sense, it is important to point out that the data controller corresponding to legal persons **not incorporated in Chile**, must indicate in writing and before the Agency (as defined above), a valid and operative e-mail address of a natural or legal person, capable of acting on their behalf so that the data subject may exercise its rights and communicate with the controller, and where the corresponding communications and administrative notifications may be validly made.

III. *Principles applicable to personal data processing*

The Law introduces several principles to comply with when processing personal data. Among such principles, there are:

1. **Lawfulness and faithfulness**: processing of personal data must be lawful and faithful, and the controller has the burden of proving it.
2. **Purpose**: personal data must be collected for specific, explicit and lawful purposes, to which the processing must be limited.
3. **Proportionality**: processing must be limited to personal data which are necessary, adequate and relevant in relation to the purposes of the processing.
4. **Quality**: personal data must be accurate, complete, current and relevant in relation to the origin and the purposes of the processing.
5. **Confidentiality**: data controllers and those who have access to personal data must keep secrecy or confidentiality regarding them.
6. **Liability**: data controllers will be legally responsible for Compliance with the principles, obligations and duties contained in the Law.

IV. *General rule of processing and legal basis*

The Law also expands the catalogue of legal basis for the processing of personal data, which will be allowed in the following cases:

1. When the data subject grants his/her consent, which must be free, informed and specific as to its purposes. In this regard, the consent is presumed not to have been freely given when the data controller obtains it in the context of the execution of a contract or the provision of a service where such collection is not necessary.
2. Regarding data related to economic, financial, banking or commercial obligations, and the processing is performed complying with the provisions of the corresponding chapter of the Law;
3. When the processing is necessary for the fulfillment of a legal obligation;
4. When the processing is necessary for the execution of an agreement between the controller and the data subject;
5. When the processing is necessary for the satisfaction of legitimate interests of the data controller or of a third party;
6. When the processing is necessary for the formulation, exercise or defense of a right before the courts of law or public bodies; and
7. When established by the law.

V. *Data subjects' rights*

The Law establishes that all individuals, acting alone or represented, shall have the personal, non-transferable and non-waivable rights of i) access; ii) rectification; iii) cancellation; iv) objecting; v) objecting to automated individual decisions; vi) portability; and vii) restriction (blocking) of their personal data.

1. **Right of access**: data subjects will have the right to request that the data controller provide them with i) confirmation of whether their data is being processed by the controller; ii) the content of the data that is being processed and their source; iii) what is the purpose of the processing; iv) which are the recipients of the data in case of transfer; v) the time of processing, among others.
2. **Right of rectification**: data subjects will have the right to request that the data controller modify their personal data when inaccurate, outdated or incomplete.
3. **Right of cancellation**: data controllers, when required by the data subject, must delete his/her personal data under different scenarios.
4. **Right to object**: data subjects will have the right to object to specific or particular processing carried out by the data controller, when (i) the basis of legal basis is the satisfaction of legitimate interests; (ii) the purposes of the processing are exclusively marketing or direct marketing of goods; and (iii) the processing is carried out solely on the basis of having obtained the data from a publicly available source.
5. **Right to object to automated individual decisions:** data subjects will have the right to object to and not be subject to decisions based on automated processing of their personal data, except under specific circumstances.
6. **Right of portability**: data subjects will have the right to request and obtain from the data controller a copy of their personal data under certain circumstances.
7. **Right of blocking**: data subjects will have the right to request temporary suspension of any processing of their personal data under certain circumstances.

VI. *Duties of the data controller*

The data controller, in addition to the corresponding obligations which derive from the enforcement of data subjects' rights, will be subject to the following obligations, among others:

1. **Duty of secrecy or confidentiality**: the data controller shall maintain secrecy or confidentiality regarding the personal data of the data subject, except when the latter has made them public, and this obligation will subsist even after the relationship between both parties has ended.
2. **Duty of information or transparency**: the controller shall provide and keep permanently available to the public certain information regarding its privacy policies and the processing performed.
3. **Duty of Protection by design and by default**: the controller must implement appropriate technical and organizational measures by design, prior to and during the processing of personal data. They must also ensure, by default, that only personal data that is specific and strictly necessary for such activity is processed.
4. **Duty to adopt security measures**: the data controller must adopt the necessary measures to safeguard compliance with the security principle, and thus guarantee the confidentiality, integrity, availability and resilience of the data processing systems.
5. **Duty to report breaches of security measures**: the data controller will have the obligation to report to the Agency any breaches to the security measures that cause the accidental or illicit destruction, leak, loss or alteration of the data, or the unauthorized communication or access to the same.
6. **Duty to perform a Data Protection Impact Assessment (DPIA)**: The Law, under certain circumstance, establishes the obligation to perform a DPIA, which consists of a risk analysis that evaluates possible harm to the rights of data subjects, and concludes with the issuance of a report that identifies the risks and determines what measures need to be taken to either eliminate or minimize

those risks.

7. **Regulating the processing of data with the data processor**: when the data controller processes data through a third party (data processor), such processing shall be governed by the contract entered into between the data controller and the processor, which must regulate certain terms indicated in the Law.

VII. *Personal Data International Transfer*

The Law establishes specific scenarios under which international transfers are allowed, including the following:

1. When the transfer is made to a person, entity or public or private organization, subject to the legal system of a **country that provides adequate levels of protection of personal data** (the Agency will be the one to determine which countries provide adequate levels of protection).
2. When the transfer of personal data is covered by **contractual clauses** or other legal instruments entered into between the controller making the transfer and the controller or data processor receiving it, establishing adequate guarantees for the protection of the personal data transferred.
3. When the two parties involved in the transfer adopt a **compliance model or certification mechanism**, establishing adequate guarantees for the protection of the personal data transferred.
4. When there is **express consent of the data subject** to carry out a specific and determined international data transfer.
5. When it refers to specific **bank, financial or stock exchange transfers**.
6. When the transfer is necessary for the execution or enforcement of a **contract between the data subject and the data controller**, or for the execution of pre-contractual measures adopted at the request of the data subject.

VIII. *Special categories of personal data*

The Law establishes a general rule for the processing of sensitive data (i.e. data referring "*to the physical or moral characteristics of persons or to facts or circumstances of their private life or intimacy, revealing ethnic or racial origin, political, union or trade union affiliation, socioeconomic situation, ideological or philosophical convictions, religious beliefs, data relating to health, human biological profile, biometric data, and information relating to sex life, sexual orientation and gender identity of a natural person*") subjecting the processing of such data to the consent of the data subject, with some exceptions, and regulating different subcategories of sensitive data, such as those relating to health and the human biological profile, and biometric data.

On the other hand, the Law introduces, regulating their processing, new special categories of (i) personal data of children and adolescents, (ii) personal data for historical, statistical, scientific and study or research purposes, and (iii) geolocation data, specifically.

IX. *Infringements and corresponding sanctions*

The Law sets forth various penalties applicable to the infringement of the established obligations, which are classified into 3 categories: minor, serious and very serious.

By way of example, the law will consider as a minor infringement the total or partial breach of the duty of information and transparency, as a serious infringement the processing of personal data without a lawful basis or for a purpose other than that for which it was collected, and as a very serious infringement the processing of personal data in a fraudulent manner.

As for the applicable penalties, the Law provides for the imposition of fines for tax benefits, depending on the type of infringement incurred by the controller:

1. **Minor infringements:** Fine of up to 5,000 UTM (approx. USD 348,000);
2. **Serious infringements:** Fine 10,000 UTM (approx. USD 696,000); and
3. **Very serious infringements:** Fine 20,000 UTM (approx. USD 1,392,000).

X. *Data Protection Officer and Infringement Prevention Model*

The law introduces the concept of Infringement Prevention Model consisting of compliance programs that the controller may voluntarily adopt as a mechanism to prevent infringements to the Law.

The Law establishes the minimum requirements of an Infringement Prevention Model and regulates its certification and registration process in a National Registry of Sanctions and Compliance, administered by the Agency. It should be noted that compliance by the controller with the duties of management and supervision of the Infringement Prevention Model certified by the Agency may constitute a mitigating circumstance.

Unlike the regulations of other jurisdictions, under the Law there will be no obligation for the controller to have a Data Protection Officer ("DPO"), a figure within the operational structure of an entity that fulfills the function of informing and advising the entity with respect to compliance with the personal data protection regulations. However, it will be imperative to have a DPO if an Infringement Prevention Model is adopted.

XI. *Entry into force*

The Law will enter into force after 24 months from its publication in the Official Gazette.

In the following days, we will be updating the information available on the specialized data protection law website available here: protecciondedatos.carey.cl/en/

AUTORES: *José Ignacio Mercado, Stefano De Cristofaro, Iván Meleda.*