PERSONAL DATA PROTECTION LAW

The purpose of this document is to present an executive summary with the main changes that the new Law brings with it and to highlight the importance of starting the process of adapting to this new regulation as soon as possible.

Purpose of the Law and scope of application

The **purpose of the Law** is to regulate the form and conditions in which the processing and protection of the personal data of natural persons is carried out.

It applies to all processing of personal data carried out by a natural or legal person, including public bodies.

Not applicable:

(i) To the processing of data that is carried out in the exercise of the freedoms to express opinions and to inform regulated by the laws referred to in Article 19, No. 12 of the Political Constitution.

(i) The processing of data carried out by natural persons in relation to their personal activities.

As for the **territorial scope of application**, it applies to:

- A data controller or data processor established or constituted in national territory.
- A representative, regardless of where they are, who processes personal data on behalf of a data controller established or constituted in national territory.
- A data controller or data processor not established or constituted in national territory, but whose personal data processing operations are intended to offer goods or services to data subject who are located in Chile, or to monitor their behavior, including their analysis, tracking, profiling or prediction of behavior.
- A data controller who, not being established in national territory, is applicable to national legislation due to a contract or international law.

Key Concepts

Personal data: any information linked to or referring to an identified or identifiable natural person. Any person whose identity can be determined, directly or indirectly, in particular by means of one or more identifiers, such as name, identity card number, analysis of elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person, shall be considered identifiable. In determining whether a person is identifiable, all objective means and factors that could reasonably be used for such identification at the time of processing should be considered.

Andrés Bello 2687, piso 24. Las Condes, Santiago - Chile I Tel +56 2 3210 0030 I www.magliona.cl

Sensitive personal data: this status will include personal data that refer to the physical or moral characteristics of individuals or to facts or circumstances of their private life or intimacy, which reveal ethnic or racial origin, political, trade union affiliation, socio-economic situation, ideological or philosophical convictions, religious beliefs, data relating to health, human biological profile, biometric data, and information relating to the sex life, sexual orientation and gender identity of a natural person.

Data controller: any natural or legal person, public or private, who decides on the purposes and means of the processing of personal data, regardless of whether the data is processed directly by it or through a data processor.

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

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

Principles

Guiding principles that must be observed by all those who process personal data and throughout its life cycle:

- **Principle of lawfulness and loyalty:** personal data can only be processed lawfully and fairly.
- **Principle of purpose:** personal data must be processed for specific, explicit and lawful purposes.
- **Principle of proportionality:** limiting personal data to those that are necessary, appropriate and relevant in relation to the purposes of the processing.
- **Principle of quality:** personal data must be accurate, complete, current and relevant in relation to its origin and the purposes of the processing.
- **Principle of responsibility:** those who process personal data will be legally responsible for compliance with the principles, obligations and duties of the Law.
- **Principle of security:** the controller must ensure adequate levels of security, protecting personal data against unauthorized or unlawful processing, and against loss, leakage, accidental damage or destruction.
- **Principle of transparency and information:** the data controller must provide the data subject with all the information that is necessary for the exercise of the rights established by law, including the policies and practices on the processing of personal data.
- **Principle of confidentiality:** the data controller and those who have access to personal data must keep them secret or confidential.

Legal bases for personal data processing

Reasons for which the processing of personal data is carried out and whose lawfulness must be accredited by the controller:

- When the data subject gives his/her consent.
- When the processing refers to data relating to obligations of an economic, financial, banking or commercial nature and is carried out in accordance with the rules of Title III of the law, including data referring to the socio-economic situation of the data subject.
- When processing is necessary for the execution or compliance with a legal obligation or provided for by law.
- When data processing is necessary for the conclusion or execution of a contract between the data subject and the data controller, or for the execution of pre-contractual measures.
- When processing is necessary for the satisfaction of the legitimate interests of the controller or a third party, provided that this does not affect the rights and freedoms of the data subject (the data subject may always demand to be informed about the processing of personal data that affects him or her and the legitimate interest on the basis of which such processing is carried out).
- When the processing of data is necessary for the formulation, exercise or defence of a right before the courts of justice or public bodies.

Rights of data subjects

Those rights that assist the data holders of personal data and that they may exercise before the data controllers:

- Access (Art. 5)
- Rectification (Art. 6°)
- Suppression (Art. 7)
- Opposition (Art. 8)
- Not to be subject to automated individual decisions (Art.8 bis)
- Block (Art. 8. Ter)
- Data portability (Art. 9)

It is relevant to consider that **data controllers must implement technological mechanisms and tools that allow the data subject to exercise their rights in an expeditious, agile, and effective manner.** The means provided by the data controller must be simple in their operation.

New responsibilities and obligations

The data controller has the following **obligations**:

- Inform and make available to the data subject the background information that proves the lawfulness of the data processing carried out.

- Ensure that personal data is collected from lawful sources of access for specific, explicit and lawful purposes, and that its processing is limited to the fulfilment of these purposes.
- Communicate or transfer, in accordance with the provisions of this law, accurate, complete and current information.
- Delete or anonymize the data subject's personal data when they were obtained for the execution of pre-contractual measures.
- To comply with the other duties, principles and obligations.

Data controller that does not have a domicile in Chile: and that processes the data of people residing in the national territory, must indicate and keep updated and operational, an email or other means of contact suitable for receiving communications from the data subjects and the Agency.

Regarding duties:
- Duty of secrecy or confidentiality.
- Duty of information and transparency.
- Duty of protection by design and by default.
- Duty to adopt security measures.
- Duty to report violations of security measures.

In the case of data processing through a third-party agent or data processor, the considerations contained in Article 15 bis must be complied with and taken into account. Such processing will be governed by the contract entered into between the controller and the processor which must contain the special elements indicated in said regulation.

In addition, when it is likely that a type of processing, due to its nature, scope, context, technology used or purposes, may produce a high risk to the rights of the data subjects of the personal data, the **data controller must carry out**, prior to the start of the processing operations, **an assessment of the impact on the protection of personal data.**

New specialised control body and sanctioning regime

From the perspective of the control body and the enforceability of the rights of individuals in matters of personal data, this new Law advances from a judicial logic to an administrative one, where the body in charge of overseeing this new regulatory standard will be the **Personal Data Protection Agency**, **an administrative body of a technical nature, with regulatory, interpretive, supervisory and sanctioning powers.**

With regard to the **sanctioning regime**, in the event of non-compliance with the Law, the Agency may:
- Impose fines of up to 100 UTM in case of minor infractions; up to 5,000 UTM in the case of serious infringements; and up to 10,000 UTM (**USD750.000**) in the case of very serious infractions;

- Triple fines in case of repeat offenses;
- such fines can reach up to 2% or 4% of the annual income of large companies in the event of repeated serious or very serious infringements (with ceilings of 10,000 and 20,000 UTM – **USD1.450.000**), respectively;
- to provide for the suspension of data processing for up to 30 days as an accessory sanction;
- to administer the National Registry of Sanctions and Compliance (whose entries will be publicly accessible for 5 years) in which the sanctioned perpetrators and the respective sanctions will be recorded.

For its part, one of the **main novelties** brought about by the new Law, unlike other regulatory models at the regional and global level, is the possibility of voluntarily adopting an **infringement prevention model**, which includes the implementation of a compliance program that will also include the appointment of a **Personal Data Protection Officer.**

The adoption of this model for the prevention of infractions may be certified by the Agency and, in such a case, used as a mitigating circumstance in the event of a possible violation of the law, implying a **reduction in the amount of the fine** to be imposed.

Final Comments

The Law will enter into force within 24 months after its publication in the Official Gazette. However, comparative experience (e.g. European Union; Brazil) has shown that even with "vacancy periods" of this type, organizations in both the public and private sectors **are unable to adapt their internal procedures and policies**, as they are extensive processes that involve significant economic outlays and, especially, a cultural change in the organizational structure of companies.

At Magliona Abogados we actively participated in the legislative discussion of the bill during its more than 7 years of processing in the National Congress, understanding its **importance for the development of the digital ecosystem of our country**, and during which it was promoted to adequately balance the free flow of information, the promotion of innovation and socio-economic development in a responsible way and respectful of the fundamental rights of people.

Therefore, we understand that adapting to these new requirements can be a significant challenge. Faced with this scenario, **we have a specialized team with extensive experience** in advising and complying with personal data protection, and other related areas of equal relevance and interrelated, such as cybersecurity, prevention, mitigation and response to cybercrime, as well as the challenges that in labor matters and consumer rights, as well as other regulated sectors (e.g. telecommunications; banking and finance; fintech), may imply cross-cutting regulations such as this.

Our perspective is that organizations can efficiently use the vacancy period to design a **fluid adaptation and migration** from the current regulations on the protection of personal data to the standards of the new Law, integrating the requirements of special regulations or sectors and taking advantage of the efforts aimed at implementing other related regulatory frameworks in the field of cybersecurity and cybercrime.

Andrés Bello 2687
Piso 24 Las Condes
Santiago
Chile

Tel: +56 2 3210 0030
Fax: +56 2 2 377 9451
Email: cmagliona@magliona.cl
Web: www.magliona.cl