# DATA PROTECTION LAWS OF THE WORLD

Chile

# CHILE

*Last modified 28 January 2023*

## LAW

Protection of Personal Data is regulated under various laws in Chile.

### Constitution of the Republic of Chile, Art. 19 N° 4

The Chilean constitution establishes the individual’s right to (i) respect and protection of private life, (ii) honor of the person and his/her family, and (iii) protection of his/her personal data. Any individual who, as a result of an arbitrary or illegal act or omission, suffers a “privation, disturbance or threat” to these rights may file a Constitutional Protective Action (“*Recurso de protección*”).

### Law 19,628/1999 'On the protection of private life', commonly referred to as 'Personal Data Protection Law' (hereinafter, the 'PDPL')

The PDPL generally defines and regulates the processing of personal data in public and private databases and is thus the primary body of rules on the processing of personal data not governed by sectoral provisions (for example contained in the laws mentioned below).

Generally, the PDPL stipulates that personal data may only be processed if the processing is (i) permitted by law (*eg*, labor law, health care law, etc.) or (ii) based on the data subject’s prior informed, written consent. There are only a few narrow exceptions to this principle (*eg*, certain publicly accessible data, or purely internal data processing for certain purposes). In addition, the PDPL contains special regulations on the processing of personal data relating to economic, banking, and financial obligations.

The PDPL law also provides data subjects the right to access, rectify, delete, block and object to processing of personal data in certain cases.

### Decree with Force of Law N° 3/19978, 'General Law of Banks'

Article 154 of this law establishes the confidentiality of an individual’s transactions with and through banks. The law distinguishes transactions covered by secrecy, which in principle are subject to an absolute prohibition of disclosure, and transactions covered by reserve, which may only be disclosed where a legitimate interest exists and if it cannot be foreseen that the knowledge of the disclosed data may cause financial damage to the customer.

### Law 20,575/2012 establishing the 'purpose principle' for the processing of personal data of an economic, financial, banking or commercial nature

This law establishes several rules that apply to the processing of personal data referring to financial, economic, banking or commercial information, such as:

- Limited disclosures: Such data shall only be communicated to established commercial entities for the purpose of a commercial risk assessment in a credit granting process, and to entities that take part in this evaluation.
- Prohibition on requesting such type of data in the context of processes for personnel selection, pre-school, school or higher education admission, emergency medical care or application for public office.
- Providers of economic, financial, banking or commercial databases must have a system for recording the name of any person requesting database information, the reason, date and time of the request and the person responsible for delivering or transferring the information. Data subjects have the right to request access to their commercial information every four months and free of charge.
- Providers of the database must implement the principles of legitimacy, access and objection, data quality, purpose, proportionality, transparency, non-discrimination, use limitation and security in personal data processing, and designate a contact person for data subjects.

### Law 19,223/1993 regulating certain computer crimes

This law establishes criminal sanctions for certain specific conduct related to the theft, destruction, obstruction, modification and illegal access and disclosure of information contained in data processing systems. It does not, however, refer specifically to personal data.

### Law 20,584/2012 regulating the rights and duties of individuals in the context of healthcare

This law sets forth that all information contained in patient files or documentations of medical treatments are sensitive data, and establishes the obligation of healthcare professionals to maintain patient data confidential and to comply with the principle of purpose limitation. This law also includes certain specific cases in which such data can be submitted, partially or totally, to the data subject and to other individuals or entities.

### Law 21521/2023 promotes competition and financial inclusion through innovation and technology in the provision of financial services, FinTech law (takes effect on February 3rd, 2023)

The law’s objective is to establish a broad framework to facilitate the provision of financial services using technology means. The law delegates regulatory authority to the Financial Market Commission ("**CMF**").

The following principles will guide the law: financial inclusion and innovation; competition promotion; financial client protection; adequate data protection; integrity and financial stability preservation; and prevention of money laundering and funding of drug trafficking and terrorism.

### Bill to Create a Consolidated Debt Registry (Bulletin 14743-03)

The draft bill establishes the right to be forgotten in financial concerns where there are no valid grounds to keep people's personal financial data after its purpose has been completed.  

The bill is in the first constitutional stage in the chamber of deputies, and we will be monitoring its progress over the coming year.

### Bill regulating the protection and processing of personal data and creating the Agency for the Protection of Personal Data (Bulletin 11,144-07, consolidated with Bulletin 11,092-07)

This draft law aims to modernize the PDPL and adapt it to international standards. The most important stipulations are:

- the introduction of further legal bases for the processing of personal data in addition to consent (such as performance of a contract and legitimate interest), and additional requirements for processing sensitive data, depending on the category of data concerned.
- various basic principles, such as lawfulness, purpose limitation, proportionality, data quality, accountability, security, transparency and information, and confidentiality.
- regulations on international data transfers.
- information requirements.

- special obligations when using data processors.
- provisions on data protection by design and default and security measures.
- reporting obligations in the event of data breaches.
- introduction of the right to portability.
- the creation of a data protection authority with the competence to impose administrative fines.

The bill is under debate at the second constitutional stage in the chamber of deputies and conclusion of the legislative procedure is expected for this year.

### Bill creating a Cybersecurity and Critical Information Infrastructure Framework Law (Bulletin 14847-06)  

This law aims to create a harmonized regulatory framework for the strengthening of cybersecurity, both operational and regulatory and addresses essential service providers. It creates a governing body, which is in charge of deciding who the declared essential service providers will be. Declared essential service providers must implement certain technological, organizational, and informational security measures to prevent, report, and resolve cybersecurity events, manage risks, and contain and reduce the impact on operational continuity, confidentiality, and service integrity.

The bill is at the second constitutional stage in the senate.

## DEFINITIONS

### Definition of personal data

The PDPL defines **personal data** as any information concerning identified or identifiable natural persons.

### Definition of sensitive data

**Sensitive data** are defined very broadly as personal data relating to the physical or moral characteristics of persons or to facts or circumstances of their private or intimate life, such as personal habits, racial origin, ideologies or political opinions, religious beliefs or convictions, physical or mental health conditions, and sexual life.

### Definition of controller and data processing

The PDLP defines the **controller** ('responsible for the register or database') as the private individual or legal entity, or the respective public body, which is responsible for decisions related to the processing of personal data.

**Data processing** is defined as any operation or complex of operations or technical procedures, of automated or non-automated nature, that allow to collect, store, record, organize, elaborate, select, extract, confront, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use them in any other way.

## NATIONAL DATA PROTECTION AUTHORITY

In Chile, there is no specific authority dedicated to overseeing matters related to data protection concerning processing activities performed by private persons or entities exists. Law 20,285/2008 on access to public information provides that the Transparency Council (*Consejo para la Transparencia*, the control body that ensures compliance with the aforementioned law which provides the rights to transparency and access to information of the state administration), shall ensure proper compliance with the data protection law by the organs of the state administration; however, the Transparency Council does not have powers to impose fines.

Since December 24, 2021, due to a provision in the newly adopted so-called Pro-Consumer Law (Law 21,398/2021), the consumer protection agency SERNAC has the competency to monitor compliance with the provisions of the data protection law in consumer matters. The SERNAC cannot impose fines but may initiate and participate in judicial proceedings and collective voluntary proceedings. This is the first time that private controllers’ processing of (consumer) personal data has been subject to regulatory control.

A special data protection authority is to be created by the above-mentioned legislative project (Bill that regulates the protection and processing of personal data and creates the Agency for the Protection of Personal Data (Bulletin 11,144-07, consolidated with Bulletin 11,092-07). However, as noted, there is no clear timeline for when to expect this bill to pass.

## REGISTRATION

Public databases must be registered in the Civil Registry and Identification Service (*Servicio de Registro Civil e Identificación*). There is no obligation to register private databases.

## DATA PROTECTION OFFICERS

The PDPL does not require the appointment of a Data Protection Officer.

## COLLECTION & PROCESSING

According to the PDPL, personal data may be processed in the following cases:

- With informed, prior and written consent given by the data subject
- If authorized by legal provisions
- If the personal data comes from publicly accessible sources, and the data:
    - are of financial, banking or commercial nature, or
    - are contained in lists related to a category of persons that merely indicate background information such as the individuals´ membership in that category, his/her profession or activity, educational qualifications, address or date of birth, or
    - are required for direct response commercial communications or direct marketing or sale of goods or services

- Furthermore, personal data may be processed without the data subject’s consent if they are processed by private entities for their exclusive use, or that of their associated or affiliated entities use, for statistical, pricing or other purposes of general benefit to them. In practice, this exception is not of significant importance.

## TRANSFER

Transfer of personal data is considered a processing activity, so all of the aforementioned rules are applicable, including the requirement to rely on a legal basis (usually consent). The PDPL does not provide or require any special provisions for the international transfer of personal data.

## SECURITY

The PDPL does not establish specific measures that need to be adopted for the security of the personal data processed. It only stipulates that the controller is required to take care of the data with due diligence, being liable in case of damages.

All individuals involved in the processing of personal data (other than from publicly accessible sources) have to comply with confidentiality obligations, even after they end their work in this field.

## BREACH NOTIFICATION

There is no obligation to report a data breach.

## ENFORCEMENT

Since there is no special data protection authority in Chile, data protection violations must be challenged with a Constitutional Protective Action obased on an alleged violation of the constitutionally guaranteed right to protection of personal data, or with an action before the ordinary civil courts. In addition, the PDPL provides for a special type of action in the event that a controller fails to respond in a timely manner to a request to assert data subject rights ('*Habeas Data*').

With the entry into force of the Pro-Consumer Law (see in the section on Authority), and the competency thereby granted to the consumer protection agency SERNAC, consumers can lodge complaints alleging the violation of the data protection law to this authority. The SERNAC cannot impose fines, but may initiate and participate in judicial proceedings and collective voluntary proceedings.

## ELECTRONIC MARKETING

Private entities are allowed to create and maintain databases for purposes of sending marketing and promotional emails, provided that the requirements mentioned in the 'Collection and Processing' section have been fulfilled.

However, any person may require that his/her information be deleted for such purposes, either permanently or temporarily.

The Chilean Consumer Protection Act (Law 19,496/1997 on the protection of consumer rights) defines 'advertising' as the communication that the provider of goods or services send to the public by any means, in order to inform and motivate the purchase goods or services. It also indicates that all promotional or advertising communication must indicate an expeditious way in which the recipients can request the suspension of the promotional communication (opt-out). After a consumer has exercised his opt out right, the sending of new communications is prohibited. In case of promotional or advertising communication sent by e-mail, the communication must also indicate the subject matter or theme and the identity of the sender.

## ONLINE PRIVACY

There are no specific laws governing online privacy or cookies.

## KEY CONTACTS

**DLA Piper Chile**
www.dlapiper.com/en-cl

Matías Zegers
Partner
DLA Piper Chile
T +56 2 2798 2604
mzegers@dlapiper.cl

Jorge Timmermann
Partner
DLA Piper Chile
T +56 2 2798 2608
jtimmermann@dlapiper.cl

Carla Illanes
Counsel
DLA Piper Chile
T +56 2 2798 2620
carla.illanes@dlapiper.cl

Juan Cristóbal Ríos
Associate
DLA Piper Chile
T +56 2 2798 2688
juancristobal.rios@dlapiper.cl

## DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.