CHILE

LAW

Personal Data Protection is regulated in different laws.

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

This law establishes individuals’ constitutional right to the respect and protection of public and private life, and the honor of the person and his / her family. Also, due to an amendment in 2018, it includes the protection of personal data. Any person who, as a result of an arbitrary or illegal act or omission, suffers a “privation, disturbance or threat” to this right may file a Constitutional Protective Action.

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

This law mainly defines and regulates the processing of personal information in public and private databases and thus constitutes the main and most important body of rules on the processing of personal data which are not governed by special provisions.

As a general principle, the law stipulates that personal data may only be processed on the basis of the prior informed written consent of the data subject, with only a few narrow exceptions (e.g. in the case of certain publicly accessible data or purely internal data processing for certain purposes).

This law also regulates the rights of data subjects to access, rectification, deletion or blocking and objection in certain cases. In 2011, Law 20.521/2011 introduced an amendment to this law, according to which credit risk predictions or assessments related to late payments or contested items that are not based solely on objective data are forbidden.

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

This law establishes in its article 154 the confidentiality of transactions that individuals conduct 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 are subject to a significant limitation on the possibility of disclosing the transaction (a disclosure may only be made to persons that can demonstrate a legitimate interest and only if it cannot be foreseen that the knowledge of the disclosed facts may cause property damage to the customer).

**Law 20,575/2012 that establishes the 'purpose principle' in the processing of personal data for commercial risk assessment for the credit granting process**

This law establishes several rules that apply to the processing of personal data referring to financial, economic, banking or commercial information:
Limited disclosures: This type of data shall only be communicated to established commercial entities, and only for the purpose of a commercial risk assessment in a credit granting process. It can also be communicated to entities that take part in this evaluation, and only for the aforementioned purpose.

Prohibition of requesting this type of data in the context of processes for personnel selection, preschool, school or higher education admission, emergency medical care or application for public office.

Access and opposition right for data subjects: Holders of commercial information have the right to request access to their information every four months and free of charge.

Obligation of the databases holders of implementing the principles of Information, Legitimacy, Data quality, Proportionality, Transparency, Non-discrimination, Use limitation and security in personal data processing, and designation of a contact person for data subjects.

**Law 20,285/2008 on access to public information (and its Regulation, Decree 13/2009)**

This law regulates the principle of transparency of the public service, the right of access to information held by any State Administration organism, the procedures for the exercise and protection of such right, and exceptions to the disclosure of information.

According to this law, the State Administration bodies are obliged to keep a public register with information about the structure of the body, certain finances, and access to services, among others. The register will not include sensitive personal data. The Regulation furtherly details the provisions set forth in this law.

**Law 19,223/1993 that defines certain Computer Crimes**

This law establishes criminal sanctions for certain specific conducts related to the theft, destruction, obstruction, modification and illegal access and disclosure of information contained in data processing systems.

**Law 20,584/2012 that regulates 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 when such data can be delivered, partially or totally, to the data subject and to other individuals or entities.

**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)**

This draft law aims to modernize the data protection law (the PDPL, see above) and adapt it to international standards. In particular, the introduction of further legal bases in addition to consent, various basic principles which must be observed when processing personal data, regulations on international data transfers and the introduction of a data protection authority are planned. The bill is currently in the first constitutional stage in the senate and it is not yet foreseeable when the law will be passed.

**DEFINITIONS**

**Definition of personal data**

The only legal definition of the concept is found in the PDPL, in which personal data is defined as any information concerning identified or identifiable natural persons.

**Definition of sensitive data**

Under the PDPL and the Regulation of Law 20,285/2008 on access to public information, sensitive data means 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 and political opinions
• Religious beliefs or convictions
• Physical or mental health conditions, and
• Sexual life.

NATIONAL DATA PROTECTION AUTHORITY

In Chile, there does not exist an authority dedicated to overseeing matters related to data protection with regard to processing activities performed by private persons or entities. Issues under the PDPL are generally resolved by Chilean ordinary trial courts.

However, Law 20,285/2008 on access to public information created the Transparency Council (Consejo para la Transparencia), an autonomous public body responsible for:

• Promoting transparency in public institutions
• Overseeing compliance with transparency and information disclosure standards and rules, and
• Guaranteeing the right of access to information held by public bodies by all individuals.

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

Under the PDPL, a responsible person for the registry or database should be appointed, corresponding to the natural or legal person or the public entity, as the case may be, which is in charge of the database and is responsible for decisions related to the processing of personal data. The responsible person is obliged to make these decisions with due diligence, being liable for the damages that could occur.

COLLECTION & PROCESSING

The processing of personal data is defined as any operation, complex of operations or technical procedures, whether automated or not, that allows the:

• Collection
• Storage
• Recording
• Organization
• Elaboration
• Selection
• Extraction
• Comparison
• Interconnection
• Dissociation
• Communication
• Assignment
• Transfer
• Transmission
• Cancellation, or
• Any other use of personal data.

In general terms, personal data may be processed in the following cases:

• With informed, prior and written consent given by the data subject
• In cases expressly authorized by law
• When said data may be collected from publicly accessible sources, and the data:
  ○ Has an economic, financial, banking or commercial nature
  ○ Is obtained from lists related to a specific category of people, which only disclose information such as the allegiance of such individual to such specific group, his / her profession or activity, educational degrees, address and date of birth
  ○ Is required for direct response to commercial communications or marketing, or direct sale of goods or services
  ○ Is treated by private entities only for their exclusive internal use, or for their associated or affiliated entities use, for statistical, pricing or other general benefit purposes
  ○ In cases of data processing carried out by public bodies, whenever dealing with matters within their competence, subject to the other general rules established in the PDPL.

TRANSFER

Transfer of data is considered a personal data processing activity, so all of the aforementioned rules are also applicable, including the consent requirements.

SECURITY

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

Regarding the use of personal data all individuals involved in the processing activities shall comply with confidentiality obligations, even after they end their contractual relationship.

For automated transmission procedures, the responsible person must, at all times, ensure that the rights of the data subjects are safeguarded and the transmission is related to the tasks and purposes of the organizations involved. Also, in case of a request for personal data through an electronic network, the following information must be recorded:

• The inquirer’s identity
• The motive and purpose of the request, and
• The specific data being transferred.

BREACH NOTIFICATION

There is no obligation to report a data breach.

ENFORCEMENT

The data subject has the right to require that the responsible person provide information on:

• What data is held
• Its source and recipients
• The purpose of processing, and
• Detailed information on any person or entity to which the data is regularly sent

The data subject may also request that any incorrect or incomplete record of personal data is modified.

The data subject can request the deletion of his / her personal data, as well as revoke his / her consent to data processing.

The rights of the data subject to information, modification, cancellation or blocking of his / her personal data cannot be contractually waived or limited. Also, requests for the exercise of said rights can only be denied when the responsible person can show that they will affect:

• The due exercise of the faculties of the public body requested (as the case may be)
• The duty of confidentiality
• National security, or
National interests.

In the cases mentioned above, if the responsible person does not reply within two business days to a data subject’s request, the data subject can file a complaint before the relevant local trial court. Along with requesting a specific performance, the affected individual can also claim damages.

The responsible person shall indemnify the data subject for the pecuniary and moral damages caused by the undue processing of the data, and must delete, modify or block the data as required by the data subject or, if applicable, as ordered by the court.

The court must reasonably determine the amount of damages, and may impose fines up to USD 3,300.

Additionally, if the data subject considers that his / her constitutional right to protection of personal data has been affected or threatened, he / she can also file a Constitutional Protective Action before the relevant Court of Appeals, requesting the cessation of the offensive action or omission.

Finally, in accordance with the provisions of Law 19,223/1993 that defines certain Computer Crimes, criminal sanctions (imprisonment and fines) may be imposed for breaching information processing systems and/or revealing any information contained therein.

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 in this case, either permanently or temporarily.

The Chilean Consumer Protection Act defines marketing as the communication that the provider of goods or services sends to the public by any means, in order to inform and motivate the purchase or contract for goods or services. It also indicates that all marketing practices must comply with the following:

- Terms and conditions and / or characteristics of the offered goods and services shall be accurate
- An ‘expedited mean to request’ the suspension of any further communications (opt-out) shall be included in such communications
- Every marketing email must indicate that it is an advertisement, and include the identity of the sender and a valid email address to which an opt-out request may be sent.

ONLINE PRIVACY

There are no specific laws governing online privacy or cookies.

KEY CONTACTS

Albagli Zaliasnik
www.az.cl/

Felipe Bahamondez
Partner
DLA Piper (Chile)
T +56 2 2798 2602
fbahamondez@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.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.