CÁMARA
CHILENO BRITÁNICA
DE COMERCIO

Doing Business in Chile
Guide 2025

DATA PRIVACY AND TECHNOLOGY LAW

Executive Summary

In today's rapidly evolving digital landscape, the role of law is more crucial than ever. With technology advancing at a rapid pace, our lives, work, and interactions are being continuously reshaped. This dynamic environment presents both opportunities and challenges, making it essential to have strong legal frameworks in place. These frameworks not only need to keep pace with technological innovation but also ensure the protection of individuals, businesses, and societies from new threats that arise in our increasingly digital and interconnected world.

Chile is presently experiencing significant shifts in data protection, aiming to enhance its data privacy standards and establish itself as a regional leader with robust regulations conducive to the transfer and handling of personal data. There's a renewed focus on data privacy and safeguarding personal information, leading to extensive discussions among local authorities and amendments to various legal frameworks.

In the wake of the European General Data Protection Regulation (GDPR), Chile has intensified its focus on data privacy. The National Congress is currently deliberating on a new data protection bill, which proposes the creation of a dedicated Data Protection Agency. Soon to be introduced, this legislation will impose increased obligations on organizations handling personal data and will grant individuals enhanced rights concerning the protection of their private information.

We have seen an increasing interest in reshaping and developing new regulations to mitigate some of the most common risks regarding our cyberspace. New Information Technology and Cybersecurity laws have been enacted, aiming to establish clear guidelines for protecting digital infrastructure, safeguarding sensitive information, and mitigating the risks associated with cybercrime in all its forms.

In this report we will be reviewing the primary regulations that set out Chile's legal framework regarding Data Privacy, IT, and Cybersecurity.

Main Regulation

In 2018, Chile took a significant step by constitutionally recognizing the right to privacy, highlighting its importance within our legal framework. While this recognition did not entail detailed regulations, it highlighted the growing political and legal attention to data privacy in our country. Moreover, it paved the way for unprecedented legislative efforts aimed at developing updated regulations for protecting personal data, as exemplified by the forthcoming data protection bill discussed in the following pages.

Currently, the processing of personal data in Chile is primarily regulated by Law No. 19.628, originally enacted in 1999. This legislation applies to all activities involving the processing of personal data, whether conducted by public or private entities, with certain exemptions related to freedom of expression and information. Personal data is defined as any information concerning identified or identifiable natural persons. Additionally, data processing is defined as any operation or set of operations, whether automated or not, that involves the collection, storage, recording, organization, creation, selection, extraction, comparison, interconnection, dissociation, communication, provision, transfer, transmission, or deletion of personal data, or any other use of such data.

Another relevant law, though not solely focused on personal data protection, is Law 19.496, also known as the "Consumer Protection Law." Recent amendments to this law have introduced provisions concerning data privacy, especially in consumer-provider relationships regarding personal data.

Recent changes to the Consumer Protection Law extend class action procedures to cases involving consumer-provider relations and infractions related to personal data. Additionally, these amendments grant SERNAC (the National Consumer Service) authority to oversee consumer personal information, enabling them to penalize violations of data privacy provisions within the law.

Mandatory Obligations.

Chile tightly regulates the handling of personal data, requiring lawful authorization or consent from the data owner. Consent must be documented in writing, with full disclosure of the intended use of their personal information, and they retain the right to withdraw consent at any time. However, the law outlines some specific exceptions which allow data processing without explicit consent.

The law mandates that personal data can only be processed for the initially stated purposes, unless obtained from public sources. The entity responsible for data management, known as the controller, must fulfill specific obligations. These include promptly deleting personal data lacking legitimate processing grounds upon request, rectifying inaccuracies, and limiting processing when data accuracy is in doubt. The controller is accountable for lawful data processing, with

breaches subject to fines and potential legal compensation for damages incurred, as well as for potential harm to corporate reputation.

Data owners possess specific rights regarding their personal information. Specifically, they have the right to request information about the purposes of their stored data, as well as the identification of the individuals or entities to whom the data is transmitted. They also have the right to request the deletion of their data if it is stored without legal justification.

To summarize, under Chilean legislation, the processing of personal data must comply with the following conditions:

- There must be a clear legal justification for processing sensitive data, which include: if it is authorized by law; if the data owner gives their consent; or if it is necessary for the owner to gain health benefits.
- However, under certain circumstances, the processing of personal data (excluding sensitive data) can be done without authorization. Such situations include data from publicly available sources; economic, financial, banking, and commercial data; group listings; commercial communications for the sale of goods and services; and when it is made by private entities for their own exclusive use.
- The data owner who has given their explicit consent must be duly informed about the intended use of their data, and with whom it will be shared. Their consent must be given in writing, which can be revoked at any time.
- Personal data can only be processed according to the specific purposes which were stated unless it was collected from publicly available sources.
- Any individual that is responsible for processing personal data must maintain the confidentiality of said data. They must execute the following actions: if the storage of the data has no legal basis it must be deleted or removed; if the data is inaccurate, incomplete, or incorrect it must be corrected; and if its accuracy or validity is in doubt it must be processed with caution.

Expectations for the forthcoming Data Privacy regulation.

Chile's National Congress is deliberating on a new data protection bill which is in its final stages before entering into Law. This legislation will impose heightened responsibilities on companies and other entities which handle personal data. It will empower individuals with various rights pertaining to safeguarding their private information. The updated privacy framework is likely to enter into force during 2024.

The new data protection bill will have implications for for all entities that process personal data. The obligations and responsibilities of those who handle the data are significantly increased.

The following are the most relevant modifications included in the bill:

- It introduces new grounds for lawfully processing personal data. It also imposes stricter criteria for obtaining valid consent from data owners.
- It imposes additional obligations on data controllers, including the requirement to collect data from lawful sources for specific, explicit, and lawful purposes. It also mandates that data processing be limited to the fulfillment of these purposes, requires the maintenance of accessible records on processing activities, mandates the adoption of privacy measures by design and by default, and necessitates the reporting of security breaches.
- It will mandate that the data owner must receive essential information regarding the way the data will be processed, including details such as the identification of the data controller, contact information, types of data processed, description of data subjects, intended recipients, processing purposes, security measures, and the rights of data owners.
- It includes new express regulation for the international transfer of personal data.

A new Personal Data Protection Agency will be established, which will be responsible for supervising and ensuring compliance with the principles, rights and obligations established in the law; resolving any requests and claims made by the data owner against the data controller; investigating and determining infringements made by data controllers, and if necessary, applying sanctions; and adopting preventive or corrective measures.

The Agency will have two specific instruments which it an employ in the case of (i), if a data controller refuses or fails to respond, and (ii), if there is a clear infringement of the law. A system of penalties is established for each type of infringement, according to its significance, with associated fines up to 20,000 UTM (US$ 1,326,659 approx.).

TECHNOLOGY LAW

Due to the increasing complexity and risks of new technology and the threats to system and data security, Chile has created a dynamic legal landscape to address the challenges of cybersecurity and cybercrime. It has created new and innovative laws to increase trust, promote innovation, and safeguard fundamental rights in an increasingly interconnected world.

IT Law

Law 21.459, known as the "IT Law" or "Cybercrime Law," which was initiated in 2018, is a significant milestone in Chile's legal framework concerning information technology (IT) and cybersecurity. By aligning its legislation with the standards established by the Budapest Convention, to which Chile subscribed in 2017, Chile demonstrates a commitment to combating cybercrime and enhancing cybersecurity measures in line with international best practices.

The IT Law entered into full force in June 2022. It defines the specific behaviors qualifying as "cybercrimes," establish their respective sanctions, and regulates specific aggravating and mitigating circumstances related to these behaviors. It

also contains a series of provisions regarding the criminal procedures and the investigation of these crimes, granting new powers to the authorities to pursue these crimes.

The law considers the following to be cybercrimes:

- Interference with the normal function of an IT system through the introduction, transmission, damage, alteration, or suppression of computer data.
- Illicit access to an IT system without authorization, especially when security measures are deliberately bypassed.
- Unauthorized interception, interruption, or interference with nonpublic information transmission within an IT system using technical means.
- Attacks on the integrity of informatic data, which involve unlawfully altering, damaging, or deleting informatic data, resulting in severe harm to the data owner.
- Forgery by unlawfully introducing, altering, damaging, or erasing informatic data with the intent for them to be identified as authentic or to generate authentic documents.
- Receipt of stolen informatic data, which includes selling, transferring, or storing such data.
- Fraudulently manipulating an informatic system by introducing, altering, damaging, or deleting informatic data with the intention of causing damages and seeking profit.
- Device abuse, which encompasses the provision or acquisition of one or more devices specifically designed or adapted for committing cybercrimes.

The IT Law in Chile incorporates special mitigating circumstances related to the crimes mentioned earlier, such as cooperating with investigations. Additionally, it outlines two aggravating circumstances. The first involves abusing a position of trust, such as administering or safeguarding an informatic system. The second pertains to exploiting the vulnerability or trust of children, teenagers, or elders to commit any of the listed crimes.

The IT Law also expands Chile's Criminal Process Code to include specific provisions for investigating cybercrimes. This grants authorities extensive powers to pursue and prosecute such offenses effectively.

Cyber-security

Significant advances in the application and modernization of laws related to cybersecurity have been made since the beginning of 2023. Notably, on December 12th, 2023, the National Congress approved the 'Framework Law on Cybersecurity and Critical Information Infrastructure.' This approval came shortly after the publication of the National Cybersecurity Policy, which delineated Chile's governmental strategies for addressing cybersecurity challenges within the country.

This new Framework Law on Cybersecurity and Critical Information Infrastructure aims to establish a general institutional framework. It includes the principles and general regulations to allow for the structuring, regulation, and coordination of cybersecurity procedures between government agencies, and between these agencies and private entities. It also aims to establish minimum requirements for the prevention, containment, resolution, and response to cybersecurity incidents; define the powers and obligations of government agencies and the duties of private institutions; and outline the mechanisms for control, supervision, and accountability in case of infractions.

This law is currently in its final stages of processing pending presidential enactment.

The most relevant aspects of this project include:

Establishment of guiding principles to be observed by both government agencies and private entities relating to: damage control, cooperation with authority, coordination, cybersecurity, responsible response, computer security, rationality, security and privacy by default and by design.

1. Scope of Application. - This law applies to providers of essential services and vital operations, including those provided by government agencies, public service concessions and private operators engaged in the following activities:

- Generation, transmission, or distribution of electricity.
- Transportation, storage, or distribution of fuels.
- Provision of potable water or sanitation.
- Telecommunications.
- Digital infrastructure, digital services, and information technology services managed by third parties.
- Land, air, rail, or maritime transportation, as well as the operation of their respective infrastructure.
- Banking, financial services, and payment methods.
- Administration of social security benefits.
- Postal and courier services.

- Institutional provision of health services by entities such as hospitals, clinics, medical centers, and medical offices.
- Production and/or research of pharmaceutical products.

2. General Duties to Prevent, Report, and Resolve Cybersecurity Incidents. - The institutions obligated by this law must continuously apply measures to prevent, report, and resolve cybersecurity incidents. These measures may be of a technological, organizational, physical, or informational nature, as appropriate. This includes, among other measures:

- Implementation of protocols and standards required by the National Cybersecurity Agency.
- Implementation of appropriate security measures according to the industry sector involved.
- The duty to report incidents to the relevant authority.

3. Creation of The National Cybersecurity Agency. - This Agency is created with the purpose of advising the President of the Republic on cybersecurity matters, collaborating in the protection of national interests in cyberspace, coordinating the actions of institutions with competencies in cybersecurity, ensuring the protection, promotion, and respect of the right to computer security, and coordinating and supervising the actions of government agencies in cybersecurity matters.

Among its faculties are:

- Requiring entities obligated by the Law to provide truthful, sufficient, and timely information to potential affected parties about cybersecurity incidents or cyberattacks that have impacted their services.
- Requiring entities obligated by the Law to provide records of activities related to networks and computer systems that allow for a detailed understanding of cybersecurity incidents that may have occurred.
- Requiring, in certain cases, access to networks and computer systems of entities obligated by the Law.
- Monitoring compliance with the provisions of this law and its regulations.

4. Offenses and Penalties. The Agency will have the authority to oversee, adjudicate, and penalize offenses through administrative procedures outlined by the Law. Offenses established by the Law are categorized as minor, serious, and very serious.

The penalties associated with these offenses are as follows:

- Up to 5,000 UTM (US$ 323.240,00 approx.), or up to 10,000 UTM (US$ 646.480,00 approx.) if it concerns an operator of vital importance, for minor offenses.
- Up to 10,000 UTM (US$ 646.480,00 approx.), or up to 20,000 UTM (US$ 1,326,659 approx.) if it concerns an operator of vital importance, for serious offenses.

- Up to 20,000 UTM (US$ 1.326,659 approx.), or up to 40,000 UTM (US$ 2.585,921 approx.) if it concerns an operator of vital importance, for very serious offenses.

CONCLUSSIONS

Chile is experiencing a notable shift in its legal framework concerning data privacy, cybersecurity, and technology. This transformation indicates a recognition of the changing digital landscape and the necessity to update regulations accordingly.

Current regulations on personal data processing dating back to 1999, are expected to be replaced by a new data protection bill that introduces more stringent requirements for data controllers, expands data subjects' control over their rights, and creates a new supervisory and enforcement authority. Additionally, new laws on information technology and cybersecurity have been enacted to protect digital infrastructure, sensitive information, and mitigate cybercrime risks.

The significance of these legal developments is hugely important. Given the dynamic nature of technology and data privacy, the necessity to be well-versed in the evolving regulatory landscape is crucial to effectively conduct business in our country.

In essence, Chile's legal transformation underscores the country's commitment to adapting to the realities of the digital age, prioritizing data privacy, and enhancing cybersecurity measures. These developments signal a progressive approach towards protecting individual rights and fostering a secure digital environment conducive to innovation and growth.