Global Data and Cyber Handbook - Chile

Key Data & Cybersecurity Laws

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# How are data and cybersecurity laws/regulations implemented?

*Last review date: 29 December 2023*

☒ omnibus – all personal data  
☒ sector-specific — e.g., financial institutions, governmental bodies

In addition to the general principle regarding the protection of privacy and personal data contained in the Chilean Constitution and the general data privacy framework set forth in Act 19,628 (Chilean Data Privacy Act or DPA), there are several other provisions on data privacy scattered throughout various bodies of law, including, e.g., the Chilean Labor Code, the Chilean Sanitary Code, Decree with the Force of Law No. 1 issued by the Chilean Ministry of Health in 2006 regarding health insurance, Act 19,799 on electronic signatures, Decree Law 3,500 issued by the Labor and Social Security Ministry in 1980 regarding the pension system, Decree with the Force of Law No. 3 issued by the Chilean Finance Ministry in 1997 regarding banks, the Updated Compilation of Rules issued by the Chilean Commission for the Financial Market, etc.

☒ constitutional

# What are the key data privacy laws and regulations?

*Last review date: 1 January 2025*

[Act 19,628](https://www.leychile.cl/Navegar?idNorma=141599) (Chilean Data Privacy Act or DPA), as amended.

Importantly, Act N°21,719 amended Act 19,628 with a comprehensive reform. The rules of Act N°21,719 will come into force on 13 December 2026.

# What are the key cybersecurity laws and regulations?

*Last review date: 1 January 2025*

Act N°21,663 ("**Cybersecurity Act**") enacted on 8 April 2024 established a general framework of cybersecurity regulation. The Cybersecurity Act mandated the creation the National Cybersecurity Agency. On 24 December 2024, the presidential decree for the creation of the National Cybersecurity Agency was enacted and the first head of the agency was appointed.

In addition, some cybersecurity matters are currently regulated by specific laws and regulations, the main ones being the following:

**Laws:**

Law No. 21,459 on computer crimes: Published in June 2022, the law outlines a series of computer crimes such as attack to the integrity of a computer system, illicit access, illicit interception, attack to the integrity of computer data, computer forgery, reception of computer data, computer fraud and abuse of devices, for which different penalties and/or fines are contemplated, according to their severity.

Law No. 21,180 on Digital Transformation of the State: This law requires electronic platforms used by government agencies to comply with security, interoperability, interconnection and cybersecurity standards.

Law No. 18,168, General Telecommunications Law: This law protects the confidentiality and integrity of information by classifying crimes of unauthorized interception.

**Decrees:**

Supreme Decrees have been issued approving technical standards. For example, Supreme Decree No. 83 of 2005 approved the technical standards for State Administration Bodies on the security and confidentiality of electronic documents and Supreme Decree No. 1 of 2015 approved the technical standards for their systems and websites.

Decree No. 273, recently issued by the Ministry of Interior in December 2022, establishes the obligation of the State Administration Bodies to report cybersecurity incidents affecting them as soon as they ascertain their occurrence.

**Sectoral Regulations:**

Undersecretary of Telecommunications: Exempt Resolution No. 1,318 of August 2020 approving technical standards on general cybersecurity fundamentals for the design, installation and operation of networks and systems used for the provision of telecommunications services.

Superintendence of Pensions: in December 2020, Title XVIII, called "Security and Cybersecurity Management System of Pension Fund Administrators" was added to Book V of the Compendium of Pension System Regulations

Financial Market Commission:*Comisión para el Mercado Financiero* (CMF): In December 2020, the CMF issued a regulation for the management of information security and cybersecurity, which establishes guidelines and best practices for compliance by banks, banking support companies and payment card issuers and operators. Another regulation was issued in September 2021 addressing the operational risk management and cybersecurity for insurance companies, which, among other things, contemplates the obligation to report cybersecurity incidents to the CMF.

# What are the key laws and regulations relating to non-personal data?

*Last review date: 1 January 2025*

Non-personal data is not covered by Data Protection Laws in Chile. However, the cybersecurity laws listed above do apply to personal and non-personal data.

# Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 1 January 2025*

The reform to the Data Protection Act  ("**Reform**") was enacted and published on 13 December 2024. The Reform will not come into force immediately but will take effect 24 months later, on 13 December 2026. This transition period gives companies two years to adapt to the new obligations. During this time, the new Data Protection Agency will also be established and staffed.

The main aspects of the Reform are the following:

It establishes new principles regulating the use of personal data (largely following the Organisation for Economic Co-operation and Development (OECD)'s privacy principles).

It establishes new data subject rights (including, for instance, the right to request that no decision that significantly affects the data subject be adopted exclusively on the basis of automated processing of their data, with certain exceptions) and new obligations for data controllers/owners (including, e.g., the duty to adopt security measures and breach notification obligations).

It contains more specific consent requirements and exceptions and defines consent as a free, specific, unambiguous (i.e., affirmative) and informed manifestation of will.

It creates special categories of personal data, which are subject to special rules (children's data, data used for historical, statistical, scientific and other purposes, and geolocation data) and regulates in greater detail the concept of sensitive data (including new types of sensitive data such as data regarding the data subject's biological profile or biometric data).

It regulates cross-border data transfers (which are not specifically regulated under current data privacy legislation) and establishes the requirements for such transfers to be made lawfully.

It creates a Personal Data Protection Agency (*Agencia de Protección de Datos Personales*), which will have the ability to monitor and punish breaches and apply fines of up to 5,000 *Unidades Tributarias Mensuales* or UTM (approximately USD 320,000).

It creates a National Compliance and Sanctions Registry and establishes new procedures for the enforcement of data privacy regulations. It establishes the possibility for data controllers/owners to reduce their exposure by adopting a breach prevention program certified by the Personal Data Protection Agency.

On 4 January 2023, the Fintech Law was enacted. This law aims to regulate various Fintech activities, including crowdfunding, open finance systems, alternative transactional technologies, financial instruments intermediation, investment advisory, credit advisory, crypto-asset transfers, and financial instrument custody. Providers of these services will be required to obtain a license from the *Comisión para el Mercado Financiero* (CMF) and will be considered as regulated financial entities.

Regarding the ongoing discussions in Congress about the reform to the DPA, it is crucial to highlight that the Fintech Law introduces a transitory regime with severe sanctions related to personal data. In contrast, the DPA does not specify a catalog for conduct of the same severity. Those who repeatedly engage in any of these actions within a 24-month period will be prohibited from registering in the Registry of Information-based Service Providers maintained by the CMF or participating in the open finance system as payment initiators.

The Chilean Cybersecurity Act entered into force in January 2025, with the first head of the Cyber Security Agency appointed. Starting in March 2025, the first companies will be notified to adopt the higher standards required for Critical Importance Operators, as defined in the Cybersecurity Act.

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.