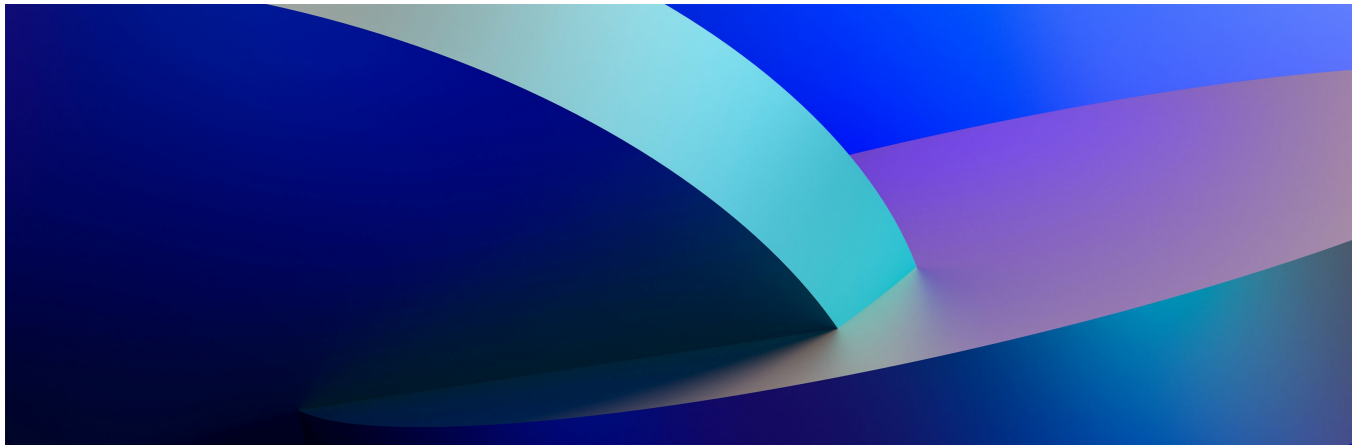




Data protection and cybersecurity laws in Chile

Data protection

1. Local data protection laws and scope

Chile's current data protection regime is governed by Law No. 19.628 on the Protection of Private Life, which remains in force and fully applicable until November 30, 2026.

However, on December 13, 2024, Chile enacted Law No. 21.719 on the Protection of Personal Data, a comprehensive reform that modernizes the legal framework, brings it closer to international standards (such as the GDPR) and establishes a dedicated Data Protection Authority. This new law will enter into force on December 1, 2026.

Other legal provisions that regulate some aspects of personal data processing include:

- The Chilean Constitution, in its article 19 No. 4 and No. 5, which enshrine the right to privacy, as well as the protection of personal data, and also;
- Law 19.496 (Consumer Protection Law) that establishes the regulation regarding unsolicited commercial marketing communications for consumers.

2. Data protection authority

The *Agencia de Protección de Datos Personales* (APDP) will act as the supervisory authority in Chile, with regulatory, investigative and sanctioning powers.

While the APDP has been created by Law No. 21.719, it is not yet operational. Until its formal implementation, Chile remains without a functioning authority in charge of overseeing data protection compliance.

3. Anticipated changes to local laws

The reform is no longer pending: Law No. 21.719 has been enacted. Its main features include:

- A modernized legal definition of personal data and sensitive data, aligned with international standards;

- Expanded lawful bases for processing: consent, legal obligations, contract performance, vital interests, public interest, and legitimate interest;
- Establishment of the APDP as a fully empowered supervisory authority;
- Regulation of international data transfers based on adequacy decisions, safeguards (standard clauses, binding corporate rules), or informed consent;
- A structured catalogue of infringements with fines of up to 20,000 UTM, or 2% to 4% of annual revenue for large enterprises in case of repeated violations;
- Introduction of a formal complaint mechanism before the APDP, with judicial review before the Court of Appeals.

4. Sanctions & non-compliance

Sanctions in Chile are now administrative rather than solely judicial. The new framework distinguishes between minor, serious and very serious infringements, with fines of up to 5,000, 10,000 and 20,000 UTM, respectively.

In addition, for large enterprises, repeated infringements may give rise to fines of up to 2% or 4% of annual revenues, whichever amount is greater. This marks an important difference with the former regime, where only civil courts could impose sanctions through civil court proceedings.

5. Registration / notification / authorisation

Controllers and processors must keep a register of processing activities, detailing the categories of data, purposes, lawful basis, transfers, and security measures. Controllers must also document the lawful basis relied upon for each processing activity.

6. Main obligations and processing requirements

Data processing:

According to the New CDLP the processing of all data shall be carried out:

- In a manner consistent with the law;
- For the purposes permitted by the legal system; and
- With attention to the full exercise of the fundamental rights of the data subject.

Consent of the data subject: Article 12 of the law establishes that the processing of personal data is permitted only when subject expressly consents or authorises it.

The consent of the data subject must be freely given, informed, and specific as to its purpose or purposes. Consent must also be given in advance and unequivocally, by means of a verbal, written or equivalent electronic statement, or by an affirmative act that clearly indicates the data subject's will.

Article 3 of the law establishes the principles on which the entity responsible for processing personal data must act. The principles are:

Article 3(a): Principles of lawfulness and fairness. Personal data may only be processed in a lawful and fair manner.

Article 3(b): Principle of purpose. Personal data must be collected for specific, explicit and lawful purposes. The processing of personal data must be limited to the fulfilment of these purposes.

Article 3(c): Principle of proportionality. The personal data processed must be strictly limited to what is necessary, appropriate and relevant in relation to the purposes of the processing.

Article 3(d): Principle of quality. Personal data must be accurate, complete, up-to-date and relevant in

relation to its source and the purposes for which it is processed.

Article 3(e): Principle of responsibility. Those who process personal data shall be legally responsible for complying with the principles contained in this article and with the obligations and duties under the law.

Article 3(f): Principle of security. When processing personal data, the controller must ensure adequate security standards, protecting it against unauthorized or unlawful processing, and against loss, leakage, accidental damage or destruction. Security measures must be appropriate and proportionate with the processing to be carried out and the nature of the data.

Article 3(g): Principle of transparency and information. The controller must provide the data subject with all the information necessary for the exercise of the rights established by this law, including policies and practices regarding the processing of personal data, which must also be permanently accessible and available to any interested party in a precise, clear, unambiguous and free manner.

Article 3(h): Principle of confidentiality. The controller of personal data and those who have access to it must maintain secrecy or confidentiality regarding such data. The controller shall establish appropriate controls and measures to preserve secrecy or confidentiality. This obligation shall remain in force even after the relationship with the data subject has ended.

Sensitive data: Article 16 of the law prescribes that sensitive personal data, defined as any information regarding characteristics of a physical or moral nature of an individual or facts or circumstances of his private life, such as personal habits, racial or ethnic origin, ideologies and political opinions, religious beliefs or convictions, physical or mental health and sexual life, cannot be processed unless:

- The data subject expressly consents to said processing;
- Without consent when:
 - the processing refers to sensitive personal data that the subject has made manifestly public and its processing is related to the purposes for which it was published;
 - the processing is based on a legitimate interest pursued by a legal entity governed by public or private law that does not pursue profit-making purposes and certain conditions are met;
 - the processing of the data subject's personal data is essential to safeguard the life, health or physical or mental integrity of the data subject or another person;
 - the data processing is necessary for the establishment, exercise, or defence of legal claims before courts of law or administrative entities;
 - data processing is necessary for the exercise of rights and the fulfilment of obligations of the data controller or data subject, in the field of employment or social security, and is carried out within the framework of the law; and
 - the processing of sensitive personal data is expressly authorized or mandated by law.

7. Data subject rights

Law No. 21.719 establishes a comprehensive set of rights for data subjects, which are personal, non-transferable, non-waivable, and may not be contractually limited. These rights may also be exercised by the data subject's legal representative or, in the event of death, by their heirs (subject to certain restrictions). The rights include:

Right of Access:

Data subjects have the right to know whether their personal data is being processed, access it, and receive information about its origin, purposes, recipients, retention period, and, in the case of automated decisions, the logic involved and potential effects.

Right to Rectification:

This right allows individuals to request the correction, update, or completion of their personal data when it is inaccurate, outdated, or incomplete. The data controller must suspend processing until the data is rectified.

Right to Erasure (“Right to be Forgotten”):

Individuals can request the deletion of their data when it is no longer necessary, consent has been withdrawn, data has been unlawfully processed, or deletion is required by law or judicial decision, subject to certain legal exceptions.

Right to Object:

Data subjects may object to the processing of their data on compelling personal grounds or when it is used for direct marketing purposes, unless the controller can demonstrate overriding legitimate reasons for the processing.

Right Not to Be Subject to Automated Decisions:

This right ensures individuals are not subject to decisions based solely on automated processing (including profiling) that produce legal effects or significantly affect them, except in certain lawful circumstances with appropriate safeguards.

Right to Data Portability:

Subjects can request a copy of their data in a structured, commonly used, and machine-readable format and transfer it to another controller, provided the processing is based on consent and conducted through automated means.

Right to Restriction of Processing (Blocking):

Data subjects may request the restriction of processing (i.e., blocking) in specific situations, such as when data accuracy is contested, the processing is unlawful but erasure is not desired, or the data is no longer needed but required for legal claims.

8. Processing by third parties

Under Law No. 21.719, personal data may be processed by a third party acting as a *data processor* (“encargado del tratamiento”) on behalf of a *data controller* (“responsable del tratamiento”), provided that such processing is carried out under the controller’s instructions and responsibility. The relationship must be governed by a written agreement that clearly defines the scope, purpose, and duration of the processing, as well as the obligations of the processor to ensure data security, confidentiality, and compliance with the law. The processor must not use the data for its own purposes and must return or delete the data once the processing is complete or upon the controller’s request. Subprocessing is only allowed with prior written authorization.

9. Transfers out of country

Article 27 of the law establishes that, provided the requirements authorizing data processing are met, international data transfer operations are lawful in any of the following cases:

- When the transfer is made to a person, entity, or public or private organization subject to the legal system of a country that provides adequate levels of personal data protection, as determined by the APDP;
- When the transfer of data is covered by contractual clauses, binding corporate rules, or other legal

instruments signed between the controller making the transfer and the controller or third-party agent receiving it, and these establish adequate safeguards; and

- When the controller making the transfer and the controller or third-party agent receiving it adopt a compliance model or certification mechanism and these establish adequate protection.

In the absence of an adequacy decision or appropriate safeguards, a specific and non-routine transfer may be made if one of the following conditions is met:

- The data subject has given express and informed consent;
- The transfer relates to specific banking, financial, or stock market operations governed by applicable sectoral laws;
- The transfer is necessary to comply with obligations arising from international treaties or agreements ratified by the Chilean State.
- The transfer is required under cooperation, information exchange, or supervision agreements signed by public bodies to carry out their functions;
- The transfer is expressly authorized by law for a specific purpose;
- The transfer is necessary for purposes of international judicial cooperation;
- The transfer is required for the conclusion or performance of a contract with the data subject; or
- The transfer is necessary for urgent medical or health-related measures, such as disease prevention or treatment, or the management of health services.

The APDP may also authorize specific transfers when sufficient guarantees are demonstrated, and it may issue recommendations, suspend transfers, or impose measures to safeguard the rights of data subjects.

10. Data Protection Officer

Not mandatory. Article 49 of the CDPL establishes that data controllers may voluntarily adopt an *infringement prevention model* (*modelo de prevención de infracciones*) consisting of a compliance program. This program must include, among other elements, the designation of a Personal Data Protection Officer (PDPO), who will be responsible for overseeing the controller's compliance with data protection obligations.

11. Security

Under article 14 *quinquies*, data controllers must implement appropriate technical and organizational measures to comply with the *security principle*. These measures must ensure the confidentiality, integrity, availability and resilience of the data processing systems and services. They should be proportionate to the nature and volume of data processed and must prevent unauthorized access, alteration, destruction, loss, or unlawful processing.

12. Breach notification

Under Article 14 *sexies* of the CDPL, data controllers must report personal data breaches to the ADPD without undue delay when there is a reasonable risk to the rights and freedoms of data subjects. If the breach involves sensitive data, information about children under 14, or data related to financial or commercial obligations, controllers must also notify the affected data subjects in clear language. These obligations are without prejudice to any additional notification duties under other laws.

13. Direct marketing

Direct marketing is governed by Law No. 19.496 on Consumer Protection, which establishes that unsolicited commercial communications sent via email must clearly identify their commercial purpose and include a valid email address to allow recipients to opt out of future communications. Once the

recipient requests to opt out, any further unsolicited emails are prohibited by law. The law is applicable to communications sent to individuals for consumer purposes.

14. Cookies and adtech

The New CDPL does not directly regulate the use of cookies or similar technologies. However, their use may still be subject to general data protection principles, such as transparency, purpose limitation and consent, particularly when cookies process personal data.

15. Risk scale

Low

16. Useful links

- <https://www.bcn.cl/leychile/navegar?idNorma=1209272> (New Chilean Data Protection Law)
- <https://www.bcn.cl/leychile/navegar?idNorma=61438%C2%A0> (National Consumer Law)
- <https://www.bcn.cl/leychile/navegar?idNorma=242302%20> (Chilean Constitution)

No official code of conduct has been published yet but regulatory guidelines may be issued by the Data Protection Agency in the future.

Cybersecurity

1. Local cybersecurity laws and scope

The Cybersecurity Framework Law No. 21.663, published in April 2024, establishes a comprehensive legal and institutional framework for cybersecurity architecture. The law creates the National Cybersecurity Agency (*Agencia Nacional de Ciberseguridad*, ANCI), a new public authority tasked with overseeing the implementation of cybersecurity policies, issuing technical standards, coordinating incident responses and imposing sanctions.

The law aligns with international standards and applies to both public and private entities managing Critical Information Infrastructure (CII) or essential services, based on their risk exposure and strategic relevance.

In addition to Law No. 21.663, several other laws govern aspects of cybersecurity and information protection in Chile:

- **Law No. 20.285 (2008)** - Law on Access to Public Information
- **Law No. 17.336 (2004)** - Intellectual Property Law
- **Law No. 19.927 (2004)** - Law amending criminal codes regarding child pornography
- **Law No. 19.880 (2003)** - Administrative Procedure Law for acts of State administration
- **Law No. 19.799 (2002)** - Law on Electronic Documents, Electronic Signatures, and Certification Services
- **Law No. 20.478 (2010)** - Law on Recovery and Continuity in Critical and Emergency Conditions of Public Telecommunications
- **Law No. 21.459 (2022) - Cybercrime Law**, which modernizes the criminal legal framework for addressing digital crimes, including unauthorized access, system interference and data breaches

2. Anticipated changes to local laws

The full implementation of Cybersecurity Framework Law No. 21.663 depends on future regulations to be issued by the ANCI. These will cover technical standards, risk management protocols, and classification criteria for Critical Information Infrastructure (CII). Meanwhile, Decree No. 295 (2025) has already established binding rules on cybersecurity incident reporting, applicable to both public and

private entities.

3. Application

The law applies to public and private entities operating CII or essential services. Applicability is based on risk and strategic relevance, not sector.

4. Authority

National Cybersecurity Agency (ANCI)

5. Key obligations

Obligations for agencies subject to the law:

- Implementation of technical and organizational measures. Obligated organizations must implement a cybersecurity management system that includes: i) Information security policies; ii) Periodic risk assessments; iii) Technical and operational controls; iv) Vulnerability management; and v) Digital supply chain protection.
- Incident reporting: One of the core obligations is the mandatory reporting of cybersecurity incidents to the National CSIRT.
- Continuity and recovery plans: Entities must have documented and updated plans in place to: i) Ensure operational continuity in the event of disruptive events; ii) Restore services in a secure and orderly manner; and iii) Assess damage and prevent the incident from recurring.
- Audits and monitoring: Entities will be subject to periodic technical audits.
- Training and awareness: All organizations must regularly train their staff in cybersecurity, best practices, incident management and the safe use of information systems.

6. Sanctions & non-compliance

The law provides a graduated penalty system for non-compliance, with fines of up to 40,000 UTM depending on the severity of the infringement (minor, serious, or very serious). Enforcement will be led by the ANCI, including its power to supervise, classify and sanction entities subject to the law.

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

Chile has a national Computer Security Incident Response Team (CSIRT), officially known as: CSIRT of the Government of Chile (CSIRT Nacional)

As of April 2024, the National CSIRT operates under the newly created National Cybersecurity Agency, established by Law No. 21.663.

It serves public institutions and plays a coordinating role for national and international cybersecurity incidents.

Its core functions include:

- Monitoring cyber threats nationwide.
- Coordinating responses to incidents affecting public services and critical infrastructure.
- Collaborating with sector-specific CSIRTs (defense, finance, energy, etc.).
- Issuing alerts, vulnerability reports, and technical guidelines.
- Sharing threat intelligence with international networks.

8. National cybersecurity incident management structure

The National CSIRT forms part of a centralized structure, coordinated by the ANCI, responsible for

incident response, oversight, and strategic coordination across sectors.

9. Other cybersecurity initiatives

No.

10. Useful links

New Cybercrime Law Status:

- <https://www.bcn.cl/leychile/navegar?idNorma=1202434>
- <https://www.csirt.gob.cl/>
- <https://www.bcn.cl/leychile/navegar?idNorma=1211466>

Authors



Diego Rodríguez, LL.M.

Partner

left_cms