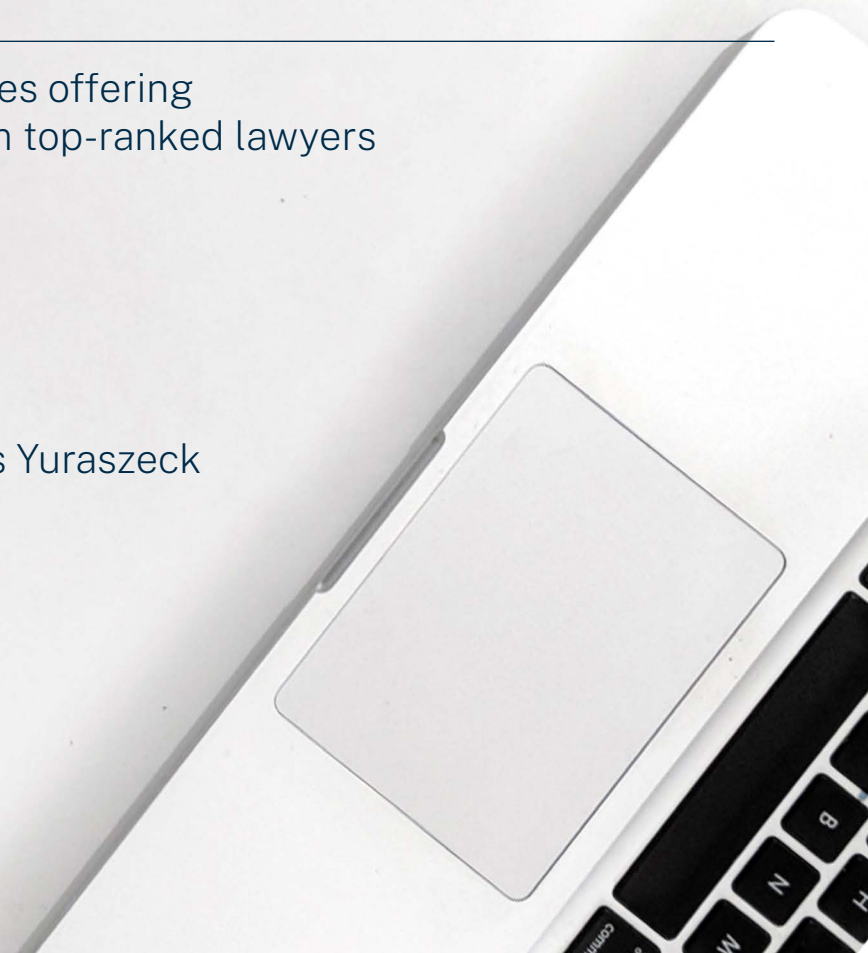
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers



Chile: Law & Practice

Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

CHILE

Law and Practice

Contributed by:
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

Contents

1. Basic National Regime p.6
1.1 Laws p.6
1.2 Regulators p.6
1.3 Administration and Enforcement Process p.8
1.4 Multilateral and Subnational Issues p.8
1.5 Major NGOs and Self-Regulatory Organisations p.8
1.6 System Characteristics p.9
1.7 Key Developments p.9
1.8 Significant Pending Changes, Hot Topics and Issues p.10

2. Fundamental Laws p.11
2.1 Omnibus Laws and General Requirements p.11
2.2 Sectoral and Special Issues p.13
2.3 Online Marketing p.15
2.4 Workplace Privacy p.15
2.5 Enforcement and Litigation p.16

3. Law Enforcement and National Security Access and Surveillance p.17
3.1 Laws and Standards for Access to Data for Serious Crimes p.17
3.2 Laws and Standards for Access to Data for National Security Purposes p.17
3.3 Invoking Foreign Government Obligations p.17
3.4 Key Privacy Issues, Conflicts and Public Debates p.17

4. International Considerations p.18
4.1 Restrictions on International Data Issues p.18
4.2 Mechanisms or Derogations That Apply to International Data Transfers p.18
4.3 Government Notifications and Approvals p.19
4.4 Data Localisation Requirements p.19
4.5 Sharing Technical Details p.19
4.6 Limitations and Considerations p.19
4.7 “Blocking” Statutes p.19

5. Emerging Digital and Technology Issues p.20
5.1 Addressing Current Issues in Law p.20
5.2 "Digital Governance" or Fair Data Practice Review Boards p.21
5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation p.21
5.4 Due Diligence p.21
5.5 Public Disclosure p.21
5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI) p.22
5.7 Other Significant Issues p.23

Magliona Abogados specialises in corporate matters, tax services, complex business litigation and finance structures, telecommunications, technology law, intellectual property, and government relations and public policy, including corporate structuring, due diligence planning, M&A, financial assistance, syndicated loans, liability restructuring and leasing. It has expertise in licensing and software development agreements, technological platforms, franchises, data protection and computer crime, as well as the distribution, production and financing of film and television. The firm's clients encompass a wide range of enterprises, both local and multinational, engaged in banking and finance, technology and software, leasing and insurance. It also counsels public agencies and companies in the movie industry, as well as other diverse fields.

Authors

Claudio Magliona is the founding partner of Magliona Abogados. He has a wealth of experience in data protection, IP and TMT, and an extensive practice in corporate and finance, technology law, telecommunications, intellectual property and entertainment law, including corporate structures, M&A, financing, licensing and software development agreements, franchising, data protection, prevention of computer crimes, and film distribution, production and financing. Claudio also handles government relations and policy matters. He has spoken at numerous conferences around Latin America and has been quoted in several publications. He is also the author of numerous publications on technology and law, data protection, IP and film financing.

Nicolás Yuraszeck is a partner at Magliona Abogados who focuses on new technologies, IP and telecommunications law, with special expertise in public policies and government relations. Before joining Magliona Abogados in 2014, Nicolás worked as an attorney adviser at the National Council for Culture and the Arts between 2012 and 2014. He has a master's degree in technology and law from the Universidad de Chile.

Carlos Araya is a director at Magliona Abogados. He joined the firm in 2013 and focuses his practice on civil and commercial matters, with special expertise in licensing and IP litigation, trade marks and telecommunications law. He studied private law at postgraduate level at the Universidad Adolfo Ibáñez and has a diploma in IP from the Pontificia Universidad Católica de Chile. He has a master's degree in Media, Entertainment, Technology, and Sports Law and Policy from the University of California, Los Angeles (UCLA).

Magliona Abogados

Andrés Bello 2687
Piso 24, Las Condes
Santiago
Chile

Tel: +56 2 3210 0030
Fax: +56 2 2 377 9451
Email: contacto@magliona.cl
Web: www.magliona.cl

MAGLIONA
ABOGADOS

1. Basic National Regime

1.1 Laws

The Chilean legal framework for data protection can be found in Article 19, No 4 of the Political Constitution of the Republic of Chile, which guarantees that the processing and protection of personal data will be carried out in the manner, and under the conditions, laid down by law. In addition, Chile has a dedicated data protection law, Law No 19,628 on Privacy Protection (the "Law"), which was published in the official gazette on 28 August 1999. The current Law is not based on any international instrument on privacy or data protection (such as the OECD Guidelines, Directive 95/46/EC, the EU General Data Protection Regulation or the European Convention on Human Rights and Fundamental Freedoms).

Furthermore, on 28 October 2021, the Ministry of Science, Technology, Knowledge and Innovation of Chile launched the National Artificial Intelligence Policy (the "Policy") along with an Action Plan. The Policy has three areas of focus:

- development of enabling factors;
- use and development of technology; and
- ethical and safety aspects.

The initiative seeks to lay the foundations to promote the development of AI in Chile; however, it does not promote substantial regulatory changes, but rather corresponds to a series of objectives that Chile would like to achieve.

1.2 Regulators

Currently, and in general, the main data privacy regulators are the civil courts under the Law. In Chile, there is no data protection regulator, that is, there is no specific public body created for this purpose as yet.

However, other entities have powers in matters of personal data protection, the main ones being the following.

Consumer Rights

Currently, the National Consumer Service ("SERNAC") is the control body in matters of protection of personal data in the context of consumer relations, until a specialised data protection body is formed.

Although it does not have sanctioning powers, SERNAC can exercise its powers to file individual or class actions before the courts, supervise, inspect, investigate, and issue interpretative circulars that are mandatory for SERNAC officials when applying the regulation and the Law (eg, at the time of audit). See **5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)**.

Public Sector

The Council for Transparency is responsible for ensuring compliance with the Law by the organs of state administration. The council has issued the Recommendations on Protection of Personal Data by the Organs of the State Administration, the Guide on Protection of Personal Data for Public Institutions (2021) and Resolution No 489/2022, which approved the Procedure for Processing Requests for the Exercise of ARCO Rights (the right of access, rectification, cancellation and opposition of the personal data of each holder) made before the Council for Transparency.

Financial Sector

The Financial Market Commission ("CMF") is the control body in the financial sector and has regulatory and supervisory powers in matters of personal data protection, information security and cybersecurity.

Under Chapters 18-5, on information about debtors from financial institutions, and Chapters 20-6, and following the Updated Compilation of Standards ("RAN") of the CMF on business continuity, information security and outsourcing of services, financial institutions must have an internal policy on security and management of debtor information ("PISMID"), which must follow international principles and best practices on personal data processing.

Law No 21,521, known as the "Fintech Law", was also recently published to "[promote] competition and financial inclusion through innovation and technology in the provision of financial services". The Fintech Law mandates the CMF to dictate the cybersecurity and personal data protection standards that financial institutions participating in the future Open Finance System must comply with (see **1.7 Key Developments**). Finally, according to the Bill on Personal Data Protection (Bill No 11.144-07 or the "Bill"), which is currently being discussed in the National Congress, the planned future agency for data protection in Chile will be an independent Personal Data Protection Agency. If the Bill is approved by the National Congress, all the general competencies in matters of protection of personal data will fall under this new national agency, meaning that SERNAC, for example, will eventually only maintain its power to file individual or class actions before the courts in this matter (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

Artificial Intelligence

There is no regulator with express powers to regulate AI. However, the current institutional ecosystem of AI governance is spearheaded by the Ministry of Science and the Interministerial Council for Science, Technology, Knowledge and Innovation. In this sense, the different ministries that make up the institutional ecosystem could potentially exercise their regulatory powers in the field of AI.

In this regard, the Chilean Ministry of Science and the Digital Government Division published a Circular Letter (the "Letter") in mid-December 2023 with "Recommended Guidelines for the Use of AI by State Agencies", which will be implemented during 2024. The Letter contains recommendations related to human-centred AI guidelines; transparency and explainability; and privacy and data use.

Notwithstanding the above, it should be noted that at the sectoral level there have been incipient advances in the regulation of AI, for example:

Financial sector

The CMF issued General Rule No 494 complementary to Law No 21,521 or the Fintech Law, relating to investment advisers. Thus, in the case of consultancies that use computer processes without human intervention, investment advisers must develop and implement policies, procedures and controls to ensure compliance with established requirements, among them, that the algorithms are designed and implemented in such a way that the results are always consistent and related to the needs and expectations expressed by the client; that the results cannot be altered by human intervention; and that the client is aware of the fact that the result emanates from an algorithm with these characteristics.

For its part, in August 2023, the CMF arranged public consultations for four regulatory proposals on corporate governance and comprehensive risk management requirements, and a regulatory proposal that establishes a cross-cutting framework for operational risk management,

applicable to a series of regulated entities. The regulation would oblige these entities to develop and implement policies and procedures for the approval, evaluation and control of trading algorithms that ensure that transactions are carried out in the interest and protection of customers.

In this sense, for the protection of consumers, obliged entities would be required to have trained personnel who understand algorithmic trading, and the algorithms would have to be tested in order to verify their correct functioning and to ensure that they do not imply a risk to the integrity of the market, among other requirements.

Health sector

Decree No 6/2022 of the Ministry of Health established the "Regulation on actions related to healthcare carried out remotely" and is applicable to both public and private health providers. Health providers will be able to carry out health actions or services through technological tools such as applications, robotics, artificial intelligence, and the internet of things (IoT), among others, to the extent that the nature of the actions or benefits allow, and ensure that the quality of care, the autonomy of the patient's will, and the security and confidentiality of people's data are guaranteed. Technical standards dictated by the Ministry of Health would guarantee the safety of these tools and types of remote services.

Finally, it should be noted that the future National Agency for the Protection of Personal Data will also have competencies in the field of AI, due to the fact that the Bill specifically includes the right to object to automated decision-making. For more information, see **2.1 Omnibus Laws and General Requirements**.

1.3 Administration and Enforcement Process

There is currently no privacy regulator or data protection authority in Chile, although there is a legal action (habeas data) that data subjects may exercise in the event of a breach of data.

However, the Bill that will update the Law is in its final stages of legislative processing. If the Bill is approved by the National Congress in 2024, the entity that will be in charge of enforcing the Law will be the new Personal Data Protection Agency, which will be able to impose fines, supervise and audit. The compliance system proposed by the Bill is similar to the European standard represented by the General Data Protection Regulation (GDPR) of the EU.

1.4 Multilateral and Subnational Issues

The Law is more than 20 years old – it is outdated and currently does not comply with international standards, except regarding the purpose principle. These are the reasons behind the Bill, which aims to update the Law to raise its levels of protection to EU GDPR standards and, in this case, to allow Chile the possibility of being recognised as an "adequate country" for the international transfer of personal data by the European Commission, by virtue of the provisions of Article 45 of the GDPR.

1.5 Major NGOs and Self-Regulatory Organisations

Datos Protegidos and *Derechos Digitales* are two well-known NGOs in data protection matters. Both are dedicated to raising awareness of the importance of protecting personal data by creating various instructions on the subject.

Another important organisation in this area is the new Chapter of the Internet Society in Chile ("ISOC Chile"). The Chilean Chapter has quickly

managed to insert itself among the main national NGOs involved in the protection of personal data and new technology matters.

In the field of AI, one of the most relevant NGOs is the Public Observatory for Transparency and Algorithmic Inclusion ("OptIA"). During the year, OptIA has participated in multiple activities and has collaborated in the discussion of public policies related to AI.

1.6 System Characteristics

Chile is working on the Bill that will modify the current Law, adapting it to be in line with EU standards (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

Thus, the Bill will propose a regulatory system quite similar to the EU Omnibus Model. However, the compliance system of the Bill will have its own particular characteristics, including:

- differentiated application of the regulations, especially for small and medium-sized enterprises;
- the adoption of an infringement prevention model, including the adoption of a compliance program and the appointment of a data protection officer;
- no legal requirement to keep a record of data processing activities; and
- the presence of the "accountability principle" in some obligations of the data controllers (ie, active transparency to demonstrate the legality of the processing), although this is not expressly enshrined in the Bill as it currently stands in the legislative process.

For more information on the content of the Bill and the characteristics of its system, see **2.1 Omnibus Laws and General Requirements**.

Similarities between the current Law and other international data protection legislation include the fact that Chile has a special category for sensitive data and that Chile has recognised the purpose principle in data processing.

1.7 Key Developments

Key developments in the past 12 months include the following.

- Law No 21.521, or the Fintech Law, which "promotes competition and financial inclusion through innovation and technology in the provision of financial services", is in the process of being gradually implemented and complementary regulations will be issued by the CMF until mid-2024. This law regulates new fintech services and creates an open financial system.
- The Advisory Commission Against Mis/Disinformation was formed, led by the Minister of Science, Technology, Knowledge and Innovation. The Commission was composed of experts and civil society organisations, and its purpose was to advise the government and to have a consultative status. The Commission published two reports during 2023: the first, to diagnose the phenomenon of mis/disinformation in Chile and the world, and the second, to provide public or regulatory policy recommendations to confront the phenomenon of mis/disinformation through digital platforms and promote digital literacy.
- The National Cybersecurity Policy 2023–2028 was published. This is of the utmost relevance, since it determines the approach that the state and its institutions will adopt to cybersecurity until 2028, in terms of public and regulatory policies. It is noteworthy that the Policy specifically adopts the promotion of local industry in cybersecurity and even

gives it preference in public procurement processes.
- The technical standard on information security and cybersecurity of Law No 21,180 on Digital Transformation of the State was published in the official gazette. The technical standard established that the organs of state administration must prepare and adopt an information security and cybersecurity policy that includes, among other things, measures to safeguard and protect the personal data and information that they process, transmit, interoperate, or store in their electronic platforms or databases, to comply with current regulations on data protection and any new regulations. The policy described should consider measures that allow privacy by design.
- In October 2023, UNESCO, the Development Bank of Latin America and the Caribbean (CAF) and the Ministry of Science, Technology, Knowledge and Innovation of Chile organised the first Forum on the Ethics of Artificial Intelligence in Latin America and the Caribbean, which seeks to install a regional council to implement UNESCO's Recommendation on the Ethics of AI. A ministerial summit was also held, in which 20 nations of the region participated and together signed the Declaration of Santiago to promote ethical Artificial Intelligence in Latin America and the Caribbean.
- In December 2023, the National Congress approved the Framework Law on Cybersecurity and Critical Information Infrastructure, which will come into force during 2024 after its publication in the official gazette. The Act is inspired by the European Union's Network and Information Security Directives 1 and 2, and identifies a list of essential services and a procedure for classifying private institutions as operators of vital importance. In addition, it creates the National Cybersecurity Agency and the National Computer Security Incident Response Team (CSIRT).

1.8 Significant Pending Changes, Hot Topics and Issues

In the next 12 months, the following developments are expected.

- The Bill on Personal Data Protection is in its third constitutional stage and is currently under discussion in the National Congress, very close to the end of its legislative processing. The Bill is expected to be a law of the republic in 2024 and will update Law No 19.628 on Privacy Protection. The precepts of the Bill are consistent with the GDPR and also seek to create a Personal Data Protection Agency.
- In the context of a National Data Policy, during 2024 the Digital Government Division will seek to develop strategic data governance to implement more efficient public policies and provide a better quality of state digital services. Thus, the approval of the National Data Strategy and the formation of a Technical Committee on Interoperability and Data Management are expected.
- The CMF must issue general rules, under the Fintech Law, which will establish the standards of information security, cybersecurity and protection of personal data with which the participating financial institutions of the future open financial system must comply. According to the gradual implementation schedule, the complementary rules should be issued during 2024.
- The AI Bill will continue to be discussed in the National Congress. The Bill takes inspiration from the EU's Artificial Intelligence Act of 2021, and identifies high-risk and unacceptable-risk AI systems, as well as the different requirements and authorisation procedure for

developing and using these systems. However, it is likely that the Bill will be amended in light of the changes made to the Artificial Intelligence Act in 2023. For its part, the government announced that a new Bill on AI, inspired by the latest version of the EU AI Act (2024), will be submitted to the National Congress in the first half of 2024.
- Chile's Ministry of Science and the Digital Government Division published a Circular Letter with "Recommended Guidelines for the Use of AI by State Agencies", which will be implemented during 2024. The Circular Letter contains recommendations related to human-centred AI guidelines; transparency and explainability; and privacy and data use.
- During 2024, the implementation process of the new Framework Law on Cybersecurity and Critical Information Infrastructure will begin. The Law is inspired by the Networks and Information Security Directives 1 and 2 of the European Union, as well as international legislation, such as that of Estonia on cybersecurity. In this sense, the new law will be applicable to public and private entities that are classified as providers of essential services and operators of vital importance by virtue of the regulations.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The Law does not currently require the appointment of privacy or data protection officers.

The processing of personal data may only be carried out if authorised by the Law, authorised by other laws or with the express consent of the data subject. If the Law authorises it, however, there is no need for the express consent of the data subject. The Law authorises the processing of personal data as follows:

- when the data comes from or is collected from publicly accessible sources;
- for the exclusive use of private legal entities, their associates and the entities to which they are affiliated, for statistical, pricing or other purposes of general benefit to the former;
- by public bodies, within their competence and subject to the provisions of the Law; and
- sensitive data, when the treatment is necessary for the determination or granting of health benefits to data subjects.

Currently, there is no exception regarding fulfilment of contract.

The Law features no application of "privacy by design" or "by default" concepts; does not require privacy, fairness or legitimate impact analyses to be conducted; and does not include the need to adopt internal or external privacy policies.

However, the Bill does include, among other elements similar to those found in the EU's GDPR:

- the appointment of a data protection officer in the context of the implementation of an infringement prevention model;
- privacy by design and by default;
- personal data protection impact assessments;
- the duty of active transparency and the adoption and transparency of the privacy policy; and
- the right of personal data subjects to object to and not be subject to decisions based on the automated processing of their personal data, including profiling, which has legal effects on them or significantly affects them.

The latter would not apply: (i) where the decision is necessary for the conclusion or performance of a contract between the data subject and the data controller; (ii) where the data subject has given prior and express consent in the manner prescribed by law; and (iii) when provided for by law, to the extent that the law provides for the use of safeguards for the rights and freedoms of the data subject.

It includes as ancillary rights the right to information and transparency; the right to an explanation; the right to human intervention; the right to express one's point of view and to request a review of the decision.

Data Subject Access Rights

In order to exercise their right to access data held about them, data subjects must address the person responsible for the data registry or bank, claiming their right to access their data. This right to access may refer to:

- the origins of the data (how this data was collected);
- the addressee of the data;
- the purpose of the storage of the data; and
- the identity of the persons or agencies to whom the data is regularly transmitted.

Access to information about personal data must be free of charge. This right to access cannot be limited by means of any act or agreement, except for the following matters: government agency, national security, or the national interest.

Data subjects also have the right of rectification if the personal data is erroneous, inexact, equivocal, or incomplete, and that situation is evidenced.

Data subjects have the right of deletion of personal data if its storage lacks legal grounds or those grounds have expired; or if the subject has voluntarily provided their personal data, and it is used for commercial communications; or if they do not want it to continue appearing in the respective registry, either definitively or temporarily.

Data subjects may oppose or object to the use of personal data for the purposes of advertising, market research or opinion polls. If the person responsible for the personal data registry or bank fails to respond to a request within two business days, or refuses a request on grounds other than the security of the nation or the national interest, the data subject will have the right to appeal before the civil court with jurisdiction over the domicile of the party responsible for the data registry or the bank, requesting protection of their right of access or the other rights granted by the Law.

For its part, the Bill, this time following the logic of the GDPR, will also establish the rights of access, rectification, deletion, opposition and portability of data, the contents and scope of which will be strengthened compared to the current law in force.

Anonymisation/Pseudonymisation

The Law contains a definition of the dissociation process, which refers to all personal data processing by which the information obtained cannot be related to an identified or identifiable individual.

Big Data

There are no additional specific restrictions, other than those expressly established in the Law, on big data analysis, algorithms, AI and the like. The general requirements are that consent

must be obtained in writing and that the person providing the data must be informed about the purpose of the storage of their personal data and whether the data will be communicated to the public or not. The authorisation, as with any other authorisation, can be obtained electronically.

Injury or Harm

The Law does not create actionable "harm" regarding data breaches, it only establishes a legal action (habeas data) that the data subject may exercise before the general courts, when the data subject requires information, modification, cancellation or blocking of personal data, and the person responsible for the personal data registry or bank does not provide a proper answer within two days. Therefore, the habeas data does not come from a harm but from specific reasons indicated in the law. If the damage comes from causes other than those indicated in the Law, the data subject may file an action for injunctive relief, before a court, in order to stop the act causing the harm (see **1.3 Administration and Enforcement Process**).

2.2 Sectoral and Special Issues

According to the Law, "sensitive data" means personal data that refers 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, beliefs or religious convictions, conditions of physical or mental health, and their sex life.

Financial Data

There is no definition of financial data, although there are some rules regarding financial data. If the financial data may be deemed as personal data, authorisation will not be necessary if the data comes, or is collected, from sources available to the public. Financial data may not be processed in the following cases:

- five years or more after the respective obligation was enforceable;
- in the case of debts incurred during a period of unemployment;
- in the case of data relating to obligations that have been paid or extinguished by other legal means; and
- in the case of debts relating to electricity, water, telephone, gas and highways.

Health Data

Health data is deemed as sensitive data. It may not be subject to processing, unless the data subject authorises it, or it is necessary for the determination or granting of health benefits.

For its part, the Bill establishes that data relating to the health of the data subject as well as that relating to the biological profile of the data subject, such as genetic, proteomic or metabolic data, may only be processed for specific purposes established in the Bill, and with the consent of the data subject.

Similarly, the Bill expressly regulates biometric data within the category of sensitive data. Biometric data may only be processed with the consent of the data subject and when the data controller provides certain additional information to the data subject before starting the data processing.

Communications Data

There is currently no definition of communications data in the Law. However, in Chile there is constitutional protection of the inviolability of private communications.

Voice Telephony and Text Messaging

There is currently no definition of voice telephony and text messaging in the Law. However, providers that direct promotional or marketing communications to consumers via mail, fax, telephone calls or messaging services must indicate an expedited way the addressees may request the suspension of this material.

Content of Electronic Communications

There is currently no definition of electronic communications in the Law. However, in Chile there is constitutional protection for the inviolability of private communications.

Other Issues

There is currently no definition of children's or students' data in the Law. Although the general rules of the Law therefore apply to this kind of data, the Bill establishes special rules for the processing of the personal data of children and adolescents. According to the Bill, the processing of personal data concerning children and adolescents can only be carried out in the best interests of the children and adolescents and respect for their progressive autonomy.

There is also currently no definition of employment data in the Law, so the general rules of the Law apply to this kind of data.

Internet, streaming and video issues

Browsing and viewing data is not regulated under Chilean law. If cookies gather personal data, they may be deemed as data processing, hence companies that place cookies will require the consent of the data subject. Location data is not regulated in Chile, although the Bill regulates such data. Tracking technology is not regulated in Chile. However, there is a law mandating that, when motor vehicle insurance policies are taken out, the insurers must include, at no extra charge, the delivery of GPS devices, which will be installed and activated exclusively by the vehicle owner.

In copyright matters, internet service providers are not obliged to compensate the damage attributable to third-party copyright infringements committed through systems or networks controlled or operated by a service provider, provided that the service provider complies with the specific conditions requested; internet service providers may only be subject to the remedies established in the Copyright Act, which in all cases requires a previous resolution issued by a court. In addition, internet service providers must forward to their users the infringement notices sent by copyright holders. Service providers fulfil their obligation by simply forwarding infringement notices, and are not compelled to take content down, or authorised to provide their users' personal data to copyright holders without a court resolution.

Hate speech

Hate speech is somewhat regulated in Chile. Article 31 of Act No 19,733 on freedom of opinion and information and the exercise of journalism imposes a fine on anyone who, by any means of social communication, promotes hatred or hostility towards persons on the grounds of their race, sex, religion or nationality.

Data Subject Rights

The Law provides data subjects with a variety of rights.

Right of access

Data subjects have the right to demand information about data held about themselves, its origin and addressee, the purpose of its storage and the identity of the persons or agencies to whom their data is regularly transmitted. Neverthe-

less, no information may be requested when it prevents or hinders proper compliance with the supervisory functions of a government agency or if it affects the confidentiality or secrecy established in legal or regulatory provisions, the security of the nation or the national interest.

Right of modification

If personal data is erroneous, inexact, equivocal or incomplete, and that situation has been evidenced, the data subject has the right to have it amended.

Right of blocking

A data subject may request the blocking of personal data when that individual has voluntarily provided their personal data or when it is used for commercial communications and the subject does not want to continue to appear in the respective registry, either definitively or temporarily.

Right of cancellation or elimination

Notwithstanding legal exceptions, the data subject may also demand that data be eliminated if its storage lacks legal grounds or those grounds have expired, when the data subject has voluntarily provided their personal data and it is used for commercial communications or they do not want it to continue appearing in the respective registry, either definitively or temporarily.

Right to free copy

The modification or elimination of personal data is absolutely free of charge, and a copy of the pertinent part of the registry that has been changed must also be provided at the subject's request. If new modifications or eliminations of data are made, the data subjects may obtain a copy of the updated registry without cost, as long as at least six months have passed since the last time they made use of this right.

Right of opposition

The data subject may oppose the use of their personal data for the purposes of advertising, market research or opinion polls.

Right to be forgotten (or of deletion or erasure)

There is no legal recognition of the right to be forgotten in the Law.

Data access and portability

The Bill includes the right to data portability, whereby the data subject may request and obtain a copy of their personal data from a data controller and communicate or transfer it to another data controller.

2.3 Online Marketing

Law No 19,496 on the Protection of Consumer Rights contains a provision regarding marketing through email. Every promotional or advertising communication sent by email must indicate its subject, the identification of the sender and a valid email address to which the recipient can address their request for the suspension of the advertising communication, which will remain banned from then on.

Providers that direct promotional or marketing communications to consumers via mail, fax, telephone calls or messaging services must indicate an expedited way the addressees may request the suspension of the communications.

Regarding data privacy, this practice requires consent from the data subject, unless the data comes from sources available to the public.

2.4 Workplace Privacy

The Political Constitution of the Republic of Chile guarantees the respect and protection of the privacy and honour of a person and their family at a

constitutional level. Such constitutional protection extends to workers. The same protection is guaranteed in Article 5 of the Chilean Labour Code.

According to the Labour Department of Chile, employers may regulate the conditions, frequency and timeliness of use of the company's emails, but may not, under any circumstances, have access to the private email correspondence sent and received by employees. This would violate the fundamental rights granted by the Political Constitution of the Republic of Chile.

If there is a breach of a worker's privacy, and that worker is part of a union, the union may apply some pressure on the employer to fulfil the Law.

All means to control workers – including cybersecurity tools – must comply with respect for the fundamental rights granted by the Political Constitution of the Republic of Chile, the right to privacy, a private life and the honour of workers. Therefore, control mechanisms are only allowed if they fulfil the following requirements:

- they must necessarily be incorporated in the normative text that the law establishes for the effect, that is, the Internal Regulations of Hygiene and Safety of the company, dictated in conformity with the law;
- they may only be carried out by suitable means consistent with the nature of the employment relationship;
- the application of control mechanisms must be general, and the impersonality of the measure must be guaranteed (ie, it must not be discriminatory); and
- the dignity of the worker must be respected.

There is no discovery system in Chile.

There are no additional requirements related to AI.

2.5 Enforcement and Litigation

Data protection enforcement is addressed by general courts with general powers. A summary court procedure is established by the Law if the person responsible for the personal data registry or bank fails to respond to a request for access, modification, elimination or blocking of personal data within two business days or refuses a request on grounds other than the security of the nation or the national interest.

Breaches of data protection caused by improper processing of data may eventually lead to fines determined by the Law (USD70 to USD700, and USD700 to USD3,490 approximately). Fines are determined in a summary court procedure. The Law establishes a general rule under which both non-monetary and monetary damages that result from wilful misconduct or negligence in the processing of personal data will be compensated. In those cases, the amount of compensation will be established reasonably by the civil judge, considering the circumstances of the case and the relevance of the facts. See **1.3 Administration and Enforcement Process**.

Private Litigation

The same standards used for public litigation also apply to private litigation for alleged privacy or data protection violations.

Eventually, SERNAC could use its powers in matters of personal data protection and file individual or class actions before the courts. These powers will be maintained even if the Bill is approved by the National Congress (see **1.2 Regulators**).

Finally, the Bill, if approved by the National Congress, will establish a sanctioning model that includes:

- minor, serious and very serious infractions;
- fines imposed by the Personal Data Protection Agency depending on the seriousness of the infringement;
- in the event of recidivism, the fine may be tripled;
- mitigating and aggravating circumstances;
- complementary sanctions, ie, suspension of data processing operations and activities carried out by the data controller;
- the National Registry of Sanctions and Compliance; and
- infringement prevention models.

In addition, in its current state of legislative processing, the Bill contemplates the extraterritorial application of the regulations, as does the GDPR.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Personal data processing by a government agency may only be carried out for matters within its scope of jurisdiction, subject to the aforesaid rules (see **2. Fundamental Laws**). Under those conditions, the consent of the subject is not necessary. Government agencies that process personal data about sentences for felonies, administrative infractions or disciplinary failures may not communicate them after the statute of limitations applicable to the criminal or administrative action, sanction or penalty has elapsed, or after the sanction or penalty has been served.

Regarding the privacy of a data subject who commits a serious crime, personal data about their crime may not be communicated after the penalty has been served. An exception would be when such information is requested by the courts of justice or other public bodies within the scope of their competence, with the requirement that such information should remain confidential.

In addition, there is the Regulation on Interception of Communications and Storage of Communication Data (Decree No 142 of 2005). For the purposes of carrying out the interceptions and recordings decreed, the telecommunications service providers will comply with them, within the period and in the manner established in the respective office issued by the court hearing the case. See **3.4 Key Privacy Issues, Conflicts and Public Debates**.

Finally, it should be noted that Chile, as a member of the OECD, adheres to the Declaration on Government Access to Personal Data Held by Private Sector Entities.

3.2 Laws and Standards for Access to Data for National Security Purposes

See **3.1 Laws and Standards for Access to Data for Serious Crimes** for information about data processing by government agencies.

3.3 Invoking Foreign Government Obligations

Organisations in Chile may not invoke a foreign government access request as a legitimate basis to collect and transfer personal data.

3.4 Key Privacy Issues, Conflicts and Public Debates

There was some debate regarding a new Regulation on Interception of Telephone Communications and Other Forms of Telecommunication,

and Retention of Communication Data. This regulation sought to replace the current Regulation on Interception of Communications and Storage of Communication Data (Decree No 142 of 2005), which regulates the obligation contained in the Code of Criminal Procedure to store the IP addresses of internet users for at least one year. The new regulation ordered telecommunications companies to store the communication data related to any type of communication carried out in Chile for a minimum of two years, also requiring additional data such as the history of internet connections and the geolocation of customers. However, the new regulation was rejected by the Chilean comptroller on the grounds that various provisions of the regulation regulate matters of law exceeding the rules of the Code of Criminal Procedure that are invoked as its basis.

4. International Considerations

4.1 Restrictions on International Data Issues

At present, the Law does not contain a specific provision in respect of international data transfers. However, the transfer of personal data outside the jurisdiction may be deemed as a use of data, for which authorisation and other requirements established by the Law would therefore be required.

However, the Bill has a chapter dedicated to the international transfer of personal data, contemplating a wide catalogue of cases that would allow data to be implemented dynamically.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

The general rules regarding data processing according to the Chilean Law also apply to international data transfers, particularly those regarding the authorisation or consent of the data subject, the purpose principle (personal data may only be used for the purposes for which it has been collected, and those purposes should be permitted by the Chilean legal system) and the informing of users of the potential communication of the data to the public. In addition, the fundamental rights of the data subject must be respected.

For its part, the Bill, following the same logic as the GDPR, establishes that subject to the requirements that confer legality on data processing, international data transfer operations are lawful in specific cases, such as:

- when the data controller who makes the transfer and the data controller or processor who receives it, adopt a compliance model or binding and certified self-regulation according to the applicable legislation for each of them;
- when the transfer is made to a person, entity or public or private organisation, subject to the legal system of a country that provides adequate levels of protection of personal data;
- when the transfer of data is covered by contractual clauses or other legal instruments signed between the data controller responsible for making the transfer and the data controller or processor who receives it, and they establish the rights and guarantees of the data subjects, the obligations of the controllers and processors, and the means of control;
- when the data subject has given express consent to carry out a specific and determined international data transfer; and
- when data must be transferred to comply with obligations acquired in international treaties or conventions that have been ratified by the Chilean state and are in force.

4.3 Government Notifications and Approvals

No government notifications or approvals are required to transfer data internationally.

According to the Bill, it is not necessary to request authorisation from the Data Protection Agency to carry out an international transfer of data, except when some of the specific requirements under which it is legal to carry out this type of activity have not been met.

4.4 Data Localisation Requirements

Currently, the Law does not establish data localisation requirements.

However, under Chapter 20-7 of the Updated Compilation of Standards ("RAN") on the outsourcing of services by financial institutions (especially banks), the data, technological platforms, and applications to be used in the outsourcing of services must be located at specific processing sites, and in the case of processing abroad, in a defined and known jurisdiction. In addition to jurisdiction, the city where the data centres operate is also required to be known.

For the purposes of contracting any type of service through the modality called cloud computing, the board of directors of a financial institution must pronounce annually on the risk tolerance that the financial institution is willing to assume in this type of outsourcing. This pronouncement must consider an analysis of the data to be stored or processed under this modality and its location.

Without prejudice to the due fulfilment of the different requirements contained in Chapter 20-7, financial institutions may outsource their non-critical services to the public or private cloud. If the financial institution evaluates the contracting of a cloud service for an activity considered strategic or critical, this may also be carried out in public or private cloud mode. However, in these cases, the financial institution must carry out an enhanced due diligence of the provider and the service.

4.5 Sharing Technical Details

No details of software code, encryption or algorithms or similar technical details need to be shared with the government.

However, in the field of public procurement, Decree No 273/2022 of the Undersecretary of the Interior establishes the obligation for heads of service to require, with respect to public procurement contracts concluded after the Decree came into force, that state ICT service providers share information on threats and vulnerabilities that may affect the networks, platforms and computer systems of the organs of state administration. The mitigation measures applied, as well as the information security policies and practices incorporated in the services provided must also be included in the shared information.

In the same sense, entities providing services to state bodies may have to comply with certain clauses of public procurement contracts that establish the duty to inform and make their algorithms transparent, etc.

4.6 Limitations and Considerations

When dealing with foreign government data requests, organisations involved in collecting or transferring data have to comply with the requirements established by the Law for data processing.

4.7 "Blocking" Statutes

There are no blocking statutes in Chile.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Big Data Analytics

There are currently no laws in Chile regarding big data analytics, but in the Bill, there is a mention of this topic. The Bill requires that this secondary use of personal data be based on a compatible purpose, that there must be a contractual relationship with the holder that justifies this differentiated use, or that the holder must have renewed their consent.

Automated Decision-Making

The Law establishes that data processing may be conducted through an automated process, and it also establishes that a person responsible for a register or personal database may establish an automated procedure for transmission, provided that the rights of the data subjects are safeguarded, and the transmission is related to the tasks and purposes of the bodies involved.

For its part, the Bill includes the right of personal data subjects to object and not to be subject to decisions based on the automated processing of their personal data, including profiling, that produces legal effects on them or significantly affects them.

Profiling or Micro-targeting

Profiling or micro-targeting is not regulated in the Law, although the Bill contains provisions on this matter. Thus, the Bill includes, in its current state of legislative processing, a section dedicated to automated individual decision-making, including profiling. According to the Bill, data subjects will therefore have the right to oppose and not be subject to decisions based on the automated processing of their personal data, including profiling, which produces legal effects on them or significantly affects them.

Artificial Intelligence

In terms of AI, the Chilean government has issued the first National Artificial Intelligence Policy along with an Action Plan.

Likewise, the Policy began its updating process during 2023, to include the socio-cultural and ethical scope or effects of AI. In this regard, the updating process is being accompanied by UNESCO, as Chile is the first country in the region to apply UNESCO's Readiness Assessment Methodology (RAM), a tool that allows assessing how prepared the country is for the ethical implementation of artificial intelligence (AI), in line with the update of its national AI policy.

Finally, it should be noted that the Ministry of Science and the Digital Government Division published the Circular Letter on "Recommended Guidelines for the Use of AI by State Agencies".

A draft law on AI, inspired by the European Union's Artificial Intelligence Act of 2021, is currently in the legislative process. The bill is in its first constitutional stage in the National Congress and has received comments from multiple stakeholders. For its part, the government announced that a new draft law on AI, inspired by the latest version of the EU AI Act (2024), will be submitted to the National Congress in the first half of 2024.

Internet of Things

Currently, the internet of things (IoT) is not regulated in Chile. However, Decree No 6/2022 of the Ministry of Health establishes the "Regulation on actions related to health care carried out remotely" which recognises that health providers may perform health actions or benefits through

technological tools such as applications, robotics, AI, IoT, among others, to the extent that the nature of the actions or benefits admit it and guarantee the quality of care, the autonomy of the patient's will, and the security and confidentiality of people's data.

Facial Recognition and Biometric Data

Neither facial recognition nor biometric data are regulated in Chile. However, either might be deemed as sensitive data and therefore the rules for sensitive data apply, and the Bill considers that as well. This has been confirmed by the Standards and Regulations Unit of the Council for Transparency.

Drones

The General Directorate of Civil Aeronautics ("DGAC") has issued DAN-151, a regulation on the use of drones in Chile. The regulation establishes restrictions regarding the areas in which drones can be used, the altitude at which drones can fly, requirements to operate drones and an express reference that the operation of drones may not violate the rights of others in terms of privacy and intimacy. In addition, the DGAC issued DAN-137 on aerial work, which expressly provides for a special regulation for "drone swarm" shows under the control of an AI system.

Disinformation

Regarding disinformation, there are attempts to legislate on the regulation of hate speech, fake news, misinformation, illegal information, etc. So far, several bills that seek to regulate these matters are being processed in the National Congress, although with little chance of being approved, following what is regulated in the EU Digital Services Law and other international regulatory or legal bodies (eg, the *Netzwerkdurchsetzungsgesetz* – NetzDG of Germany).

Dark Patterns in E-Commerce

Regarding electronic commerce, the Report on the Results of the Survey of Dark Patterns in Electronic Commerce, published by SERNAC, shows the results of the dark pattern survey in a sample of the companies participating in Cyber Monday in November 2020. The objective of this survey is to find out which are the dark patterns that are most used in Chilean electronic commerce and how they affect people's purchasing decisions.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Organisations in Chile do not establish protocols for digital governance.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

There do not appear to have been any significant audits regarding data protection violations.

See the section on Private Litigation in **2.5 Enforcement and Litigation**, for more on this topic.

5.4 Due Diligence

Regarding data protection, it is important to comply with the Law and other rules that may be applicable to personal data and, in particular, to begin to prepare institutions for the imminent approval of the Personal Data Protection Bill, which will raise standards to EU GDPR levels.

5.5 Public Disclosure

No privacy/data protection-specific laws mandate the public disclosure of an organisation's cybersecurity arrangements. For more on this topic, see **4.5 Sharing Technical Details**.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

SERNAC is currently the authority in control of matters to do with personal data protection in the context of consumer relations by virtue of Law No 21,398, the Pro-Consumer Law, until a body specialised in data protection and with powers in this area is formed.

SERNAC can exercise its powers in this area (although it does not have sanctioning powers) in that it is able to present class actions before the courts, supervise, carry out mediations and request reports, and issue interpretative circulars that are mandatory only for officials of the National Consumer Service.

Interpretative Circulars

The following are examples of these circulars that also deal with matters related to personal data protection.

Interpretative circular on good practices in electronic commerce

This establishes the following principles of electronic contracting:

- The principle of effective and comprehensive protection, according to which suppliers must ensure that the consumer has, throughout the contractual term, effective and complete protection, the standard of which may not be lower than the level of protection afforded in other forms of trade.
- The principle of transparency in information, according to which each supplier must provide consumers with visible and truthful information on the identity of the supplier and its national contact details; on the characteristics of the products and/or services it offers and markets; and also on the electronic transaction process.
- The principle of legality, according to which the offer and contracting of goods or services with consumers and the after-sales service of the electronic provider must respect the legal regulations in force in the applicable jurisdiction.
- The principle of informed consent, according to which electronic suppliers must inform the consumer about the general and particular conditions of a contract and about the goods or services. This means that, when consumers give their consent, they have adequate knowledge in relation to the nature of the contract concluded, the goods or services it covers, and their rights and obligations.
- The principle of the binding force of the contract, according to which electronic suppliers who have accepted a purchase order must fulfil the contract in a faithful and timely manner, using all the means at their disposal to do so.
- The principle of professionalism, according to which electronic suppliers must behave professionally in the exercise of electronic commerce, offering quality goods and services, to which they have access and are in a position to provide or procure effectively.
- The principle of good faith, according to which suppliers must act in a fair and transparent manner towards consumers, avoiding all conduct that misrepresents or maliciously conceals information, or that is intended to confuse the consumer.

In addition, the circular establishes that all companies must inform in a timely, visible manner and with the possibility of storing information about the terms and conditions. SERNAC interprets the terms and conditions as standard form contracts that must include the provider's privacy policy.

Interpretative circular on the criteria of equity in the stipulations contained in standard form contracts referring to the collection and processing of the personal data of consumers

SERNAC may control and supervise, through its officials, the clauses that are established in the terms and conditions of the providers, and especially in their privacy policies, in the following aspects:

- control of form – the transparency of the privacy policy and of any stipulation or condition related to the processing of personal data;
- clauses that contemplate the modification, suspension, or unilateral termination of the contractual relationship;
- clauses that charge the consumer for the effects of any deficiencies, omissions or errors;
- clauses that establish absolute limitations of liability towards the consumer; and
- clauses that contravene contractual good faith.

Interpretative circular on consumer protection against the use of artificial intelligence systems

This circular includes a series of interpretative rules that aim to establish the meaning and scope of the regulations on the protection of consumer rights and protection of personal data that the SERNAC is responsible for monitoring, in the face of the risks derived from AI systems in the framework of a consumer relationship:

- delivery of truthful, timely and transparent information;
- safeguarding freedom of choice;
- consumer safety;
- prohibition of all arbitrary discrimination; and
- protection of consumers' personal data.

The Electronic Commerce Regulation

The Electronic Commerce Regulation came into force in 2022 and is applicable to sellers who offer goods or services on electronic commerce platforms in exchange for a price or fee, and to operators of electronic commerce platforms that offer the products or services of third parties.

In the regulation, electronic commerce platforms are understood as any website or platform, accessible through electronic means, which allows sellers to offer products or services, and consumers to acquire or contract them, as appropriate. The following are not considered to be electronic commerce platforms: internet sites or online payment service platforms; those where consumers cannot purchase the products or contract the services offered, regardless of whether or not the payment is made through the website or platform; those on which only advertising is displayed; and those on which the consumer is redirected to the websites or platforms of sellers.

With regard to consent, the regulation establishes that consent will not be deemed to have been given if the consumer has not previously had clear, understandable and unambiguous access to the general conditions of the contract and the possibility of storing or printing them.

In addition, the regulation establishes that silence does not constitute acceptance in acts of consumption, and that merely visiting an e-commerce platform does not impose any obligation on the consumer, unless they have unequivocally accepted the terms and conditions offered by the user or platform operator.

5.7 Other Significant Issues

There are no other major issues regarding data protection and privacy in Chile.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com