



The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Chile: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection and cyber security laws and regulations that may occur in Chile.

This Q&A is part of the global guide to Data Protection & Cyber Security. For a full list of jurisdictional Q&As visit <http://www.inhouselawyer.co.uk/practice-areas/data-protection-cyber-security/>



Country Author: Ecija Otero

The Legal 500



Macarena Lopez, Head of IT & IP Area

mlopez@ecija.com



Gerardo Otero

gotero@ecija.com

1. Please provide an overview of the legal framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the laws enforced)?

- The legal framework governing privacy can be found in article 19 No. 4 of the Political Constitution of the Republic of Chile, which guarantees the respect and protection of privacy and honor of the person and his/ her family. Article 19 No. 4 of the Chilean Constitution, was amended by Law No. 21,096, establishing the Right to Protection of Personal Data; and precisely recognizes the protection of personal data within the scope of the constitutional guarantee of the protection of private life and honour, stating that the treatment and protection of this data will be subject to the forms and conditions

established by law.

- Furthermore, Chile has a data protection law, Law No. 19,628 on Privacy Protection (“Data Privacy Act”); regulates the treatment of personal information in public and private databases or bank register. Though, regarding the public segment, there are some special rules about the public data base or bank by public agencies, restricted rights for holders of personal data stored or processed by public entities, and under the scope of its functions.
- Law No. 19,496, which comprehends provisions regarding credit information along with the Data Privacy Act (Article 9 amended by Law No. 20,521), which contains provisions about personal data related to obligations of an economic, financial, banking or commercial character; to ensure that the information delivered through risk predictors is accurate, updated and truthful.
- Law No. 20,584, which regulates privacy on healthcare, encompasses provisions concerning the privacy of medical records together with the Data Privacy Act, which contains the confidentiality of the doctor’s prescriptions and laboratory analyses, and exams and services related to health services.
- Article 154bis of the Chilean Labour Code states that the employer shall maintain reserve of all private information and data of the employee to which it has access due to the labour relationship. Article 5 of the Labour Code expressly states that employers can exercise their rights within the limits imposed by the Constitution, especially regarding respect of privacy. Employers must abide by and comply with the privacy statements.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

There is no registration process for private entities. Though, regarding personal data processing by government entities, the Service of Civil Registration and Identification shall keep a record of personal data base processed by such agencies (no fee payable).

The Data Privacy Act states any individual can process personal data, if the following requirements are met:

1. The processing of personal data shall be authorized by one of the three following: (i) the Data Privacy Act; (ii) another legal provision; or (iii) the subject/holder of the personal data specifically consents thereto.

In addition, the authorization granted by the holder/subject of the personal data regarding to the processing of his/her data shall comply with the following requirements in order to be effective:

- it shall be accurately informed about the purpose of the storage of the personal data and if those data will be communicated or not to the public
 - the consent shall be specified; in writing; and
 - the personal data must be used only for the purposes for which it has been collected, unless it comes or has been collected from public sources. Even though, the data shall be accurate, updated and respond truthfully to the actual circumstances of the holder of the personal data.
2. The rights granted by the Data Privacy Act shall be respected and fulfilled;
 3. The purpose of the collecting and processing shall be allowing by the Chilean law;

3. How do these laws define personally identifiable information (PII) versus sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

According to the Data Privacy Act: personal data is referred to as any information concerning natural persons, identified or identifiable.

Sensitive Data: The Data Privacy Act enacts more severe rules regarding sensitive data; which refers to the physical or moral characteristics or circumstances of the private life or intimacy of the persons, such as personal habits, racial origin, ideologies and political opinions, beliefs or religious convictions, conditions of physical or mental health and sex life.

4. Are there any restrictions on, or principles related to, the general processing of PII - for example, must a covered entity establish a legal basis for processing PII in your jurisdiction or

must PII only be kept for a certain period? Please outline any such restrictions or “fair information practice principles” in detail?

Personal data shall be removed or cancelled when there are no legal grounds for its storage or when the data has expired.

Regarding financial data shall not be processed in the following cases:

- After 5 years since the corresponding obligation was enforceable;
- In case of debts incurred during a period of unemployment;
- Obligations that have been paid or extinguished by other legal means; and
- Debts related to electricity, water, telephone, gas and highways.

In the case of government entities which process personal data on rulings for felonies, administrative infringements or disciplinary failures, it should not be communicated after the statute of limitations applicable to the criminal or administrative action, or the sanction has elapsed, or once the penalty has been served. This is without prejudice to the fact that in Chile, the right to be forgotten has not been regulated by law.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of PII and, if so, are there are rules relating to the form, content and administration of such consent?

The Data Privacy Act states any individual can process personal data, if the following requirements are met:

(a) The processing of personal data shall be authorized by one of the three following:

- (i) the Data Privacy Act;
- (ii) another legal provision; or

(iii) the subject or holder of the personal data specifically consents thereto.

The consent/authorization granted by the holder/subject of the personal data regarding to the processing of his/her data shall comply with the following requirements in order to be effective:

- it shall be accurately informed about the purpose of the storage of the personal data and if those data will be communicated or not to the public
- the consent shall be specified; in writing; and
- the personal data must be used only for the purposes for which it has been collected, unless it comes or has been collected from public sources. Even though, the data shall be accurate, updated and respond truthfully to the actual circumstances of the holder of the personal data.

In addition:

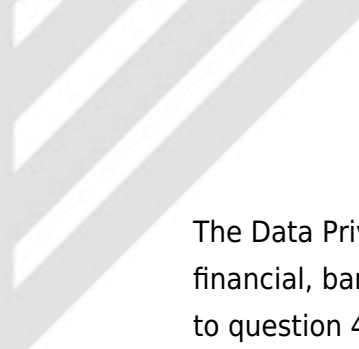
(b) The rights granted by the Data Privacy Act shall be respected and fulfilled;

(c) The purpose of the collecting and processing shall be allowing by law.

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of PII that are prohibited from collection?

The sensitive data may not be subject to processing, unless (i) the law so authorizes; (ii) there is express consent from the subject of the sensitive data; (iii) or it is necessary for granting health benefits.

In the case of physician or doctor prescriptions and laboratory analyses or exams and services related to healthcare; are confidential. Such content could be revealed or copied with the express consent of the patient, granted in writing. Nevertheless, pharmacies can publish for statistical purposes, the sales of pharmaceutical products of any nature, including the name and amount thereof.



The Data Privacy Act include special provisions regarding a person's economic, financial, banking or commercial information/data and its communication: see answer to question 4.

7. How do the laws in your jurisdiction address children's PII?


At present, there are no provisions concerning the processing of personal data of minors. Accordingly, general rules shall apply. It shall be necessary to comply with the provisions contained in the Data Privacy Act, especially, those regarding the consent/authorization of the individual/subject, the finality principle and report on the probable public communication of data. Since the subject of data is a minor shall require authorization of the parents or custodian.

8. Are owners or processors of PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

No, owners or processors of PII are not required to maintain any internal records of their data processing activities or to establish internal processes or written documentation. Unless, in case of data processing by public entities, in which case the Service of Civil Registration and Identification shall keep a record of personal data banks managed by such agencies.

9. Are consultations with regulators recommended or required in your jurisdiction and in what circumstances?

NO, because there is no Data Protection Officer in Chile, yet.

- 
10. **Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?**

No.

11. **Do the laws in your jurisdiction require appointment of a data protection officer, or other person to be in charge of privacy or data protection at the organization? What are the data protection officer's legal responsibilities?**

There is no Data Protection Officer in Chile yet. Not applicable.

12. **Do the laws in your jurisdiction require providing notice to individuals of the business' processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).**

No. The Data Privacy Act does not require providing notice to individuals of the business' processing activities; in some cases, it is required the consent/authorization of the data holder. The "consent" of the data holder according to answer to question 5 shall be accurately informed about the purpose of the storage of the personal data and if those data will be communicated or not to the public.

13. **Do the laws in your jurisdiction apply directly to service**

providers that process PII, or do they typically only apply through flow-down contractual requirements from the owners?

Yes, the Data Privacy Act apply directly to service providers that process PI because of all processing of PII is covered. In the Data Privacy Act, data processing is defined broadly as any action or set of technical operations or procedures, automated or not, that make it possible to collect, store, record, organize, prepare, select, extract, match, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use it in any form. Hence, there is no difference made between those who control or own PII and those who provide PII processing services to owners.

The Data Privacy Act only mentions to the person responsible for a *data registry or a bank*, which means any private legal entity or individual, or government agency, that has the authority to implement the decisions related to the processing of personal data. Therefore, there are no unlike duties for owners, controllers or processors. Still, government agencies can only process data regarding matters within their respective legal authority and subject to the rules set out in the Data Privacy Act.

14. Do the laws in your jurisdiction require minimum contract terms with service providers or are there any other restrictions relating to the appointment of service providers (e.g. due diligence or privacy and security assessments)?

Only in processing bank data, the Superintendency of Banks and Financial Institutions shall have authority to issue instructions and adopt all measures aimed at the correction of the irregularities he may observe and, generally, those he may deem necessary in order to protect the interests of the depositors or other creditors and of public interest.

According to the abovementioned, the Superintendency of Banks and Financial Institutions issued a ruling regarding incidents/breaches of security or cybersecurity, in which is mandatory for banks will report all the incidents related to Cybersecurity occurred in the current month, including updated information or complementary to

incidents reported in previous periods. It will be understood by Cybersecurity incident any event that threatens or adversely affect the information assets of the institution, as well as the infrastructure that supports it. It will consider alerts to those events registered but not materialized.

In addition, see answer to question 16 and 23.

15. Is the transfer of PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (for example, does cross-border transfer of PII require notification to or authorization from a regulator?)

Currently, the Data Privacy Act, does not encompass a specific provision in this respect. Though, any use of the data will require consent/authorization of the holder/subject of the personal data, if it is not subject to the exceptions mentioned in this document (transfer is a kind of personal data processing, therefore, all the data privacy rules shall apply, including the consent requirements).

16. What security obligations are imposed on PII owners and on service providers, if any, in your jurisdiction?

- In relation to security matters we can mention the implementation on the year of 1993, the Law No. 19,223 on cybercrimes with four provisions; nevertheless, this law is nowadays outdated. In April of 2017, Chile deposited the instrument of accession to the Budapest Convention on Cybercrime and in August of 2017, Chile became the 54th signatory country to the Treaty and the first country of South America. Law No. 19,223 on cybercrimes is a sub-category in the field of cybercrime related with the disturbance of the logical components of cyberspace (computer programs, information systems, databases) called computer-related crimes; it is describing the non-authorized access, theft and destruction of information systems and/or information.
- In addition, in October of 2018, the government introduced a bill in the Congress (Bill No. 12192-25) that establishes new rules on cybercrimes, revoking Law No. 19,223 and amending other legal bodies in order to bring them into line with the Budapest

Convention.

- According to Net Neutrality Law No. 20,453, states the principle by which the ISPs and those that own and administrate the backbone structure of the internet service, shall not make any discrimination and differentiation among the information that runs through their equipment or the network infrastructure. This law was complemented by a special regulation, published on 18 March 2011, which establishes the specific requirements that ISPs shall accomplish in connection with these network neutrality legal obligations. In addition, PTS concessionaires that provide internet access services (IAS), services providers (SP) and also ISPs: cannot arbitrarily block, interfere with, discriminate against, obstruct or restrict the right of any internet user to use, send, receive or offer any content, application or legitimate service through the internet, as well as any other activity or legitimate use performed through the network. They shall provide each user with an internet service access or connectivity with the provider of internet access, as appropriate, which cannot arbitrarily distinguish content, applications or services, based on the source or ownership thereof, taking into account the different configurations of the internet connection under the current contract with the users; cannot limit the right of a user to add or use any sort of tools or devices on the network, provided that they are legitimate and that they do not damage or harm the network or the service quality; shall provide, at the expense of users who request such services, parental control services for contents against the law, morality or good customs, provided that the user is clearly and precisely informed in advance about the scope of such services; and shall publish on its website all information connecting to the characteristics of internet access service offered, speed, link quality, distinguishing between national and international networks, as well as the nature of the service and service warranties. Nevertheless, providers of PTS and ISPs could take the measures or actions necessary for traffic and network management, in the exclusive scope of activity that has been licensed to them, if this is not designed to perform actions that affect or may affect free competition. Providers of PTS and ISPs shall seek to preserve user privacy, virus protection and network security.

17. Does your jurisdiction impose requirements of data protection by design or default?

In our jurisdiction there are no requirements imposed regarding “privacy by design” or “privacy by default; only the general requirements apply to data processing.

18. Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?

The responsible or in control of the data base is required to ensure that those involved in personal data processing are subject to and comply with confidentiality obligations because of security liability of the personal data storage in the data base. It shall be guaranteeing that the rights of the data subjects are safeguarded, and the communication is connected to the responsibilities and purposes of the participating organizations. In case of a request for personal data through an electronic network, the following information must be recorded: (i) the inquirer’s identity; (ii) the requested purpose, and (iii) the specific data being transferred. Regarding security requirements, the Data Privacy Act does not impose any type of security measures that data subjects and entities must take in relation to processing of personal data. Besides, the person responsible for the data base or banks in which personal data is stored (after its collection) should be manage them with due diligence, confidentiality and assuming responsibility for damages.

Furthermore, there are specific rules regarding banks and data of their clients and their wire transfers, in which encryption and notice of security breach is mandatory. This regulation is transitory and, it was dictated by the entity that supervises the banks. Currently, the bill that includes regulation in these matters is pending in Congress.

Additionally, there are some other regulations that contain cybersecurity provisions applicable only for certain areas; such as:

- Law No. 19,223 on cybercrimes, which regulates unauthorized access to databases or information, unauthorized disclosure of such information, among other criminal actions. This obsolete law is not enough to address the size and significance of today’s events on breach of security or cybercrimes.
- General Telecoms Law: (GTL) article 24 H: regarding the obligation of seeking to preserve network security for ISPs and telecommunications concessionaires;
- Decree No. 83 of 2005 issued by the Ministry General Secretariat of the Presidency, on the Confidentiality and Security of Electronic Documents for the Public Administration.
- On 2017, it was released the first National Cybersecurity Policy by the government. The objectives by 2022 include a risk management approach to preventing and reacting to incidents, including to protection of information infrastructure, combating cybercrime

while respecting fundamental rights, building cybersecurity culture through education and accountability, cross-stakeholder cooperation and active participation in national and international discussions, and promoting cybersecurity industry innovations. At the same time Chile has signed the Council of Europe Convention on Cybercrime, thereby becoming the 58th country that has signed or accessed it. As it indicated in the same policy, Chile has in place a set of legal and statutory regulations that relate directly or indirectly with the challenges of cybersecurity -which should be reviewed and updated in accordance with the guidelines set out in the abovementioned policy and with Chile's international commitments, such as, Law No. 19,223 about cybercrime or Law No. 19,628 about the protection of private life, among other rights.

- Supreme Decree No. 1,299/2004 setting out new regulations for the State's Connectivity Network managed by the Ministry of the Interior and describing the technological procedures, requirements and standards for the incorporation to such network by public entities (consolidates an intranet, named the State's Connectivity Network, where a number of ministries and public bodies should be interconnected).
- Supreme Decree No. 1/2015 approving the technical standards for the systems and websites of the State administration bodies: This Decree updates the technical standards for the websites of the State administration bodies regulating certain conditions about confidentiality, availability and accessibility of information contained in those websites, all of them being key elements of cybersecurity.
- On October 25th of 2018, Chilean President, Sebastián Piñera, signed a bill on computer crimes.
- In the same date, he issued a Presidential Instructive giving directive to public bodies related to cybersecurity, including urgent measures that should be implemented. Such as:

- Appointment of a high-level cybersecurity officer in each public-service, who must be independent of the institution's IT head.
- Application and updating of technical regulations on cybersecurity.
- Internal cybersecurity measures.
- Detailed revision of networks, systems and digital platforms of public operation.
- Surveillance and analysis of the operation of the technological infrastructure of State Administrative bodies. The Coordination Center of Government Entities ("CCEG") will verify compliance with current cybersecurity standards and will carry out cybersecurity exercises.
- Compulsory report of incidents to the CCEG, as soon as they become aware of them.
- Response to cybersecurity incidents. Regardless of the regulations issued in terms of cybersecurity by the head of each service, the Ministry of the Interior through the CCEG

will arrange the necessary actions to ensure the continuity and proper functioning of the networks.

- Transitional governance of Cybersecurity. While the implementation of the new model of national cybersecurity policy is pending, a temporary governance will be defined. This task will be the responsibility of the Ministry of the Interior, who will designate a responsible person who will implement the measures of the National Cybersecurity Policy in terms of transient governance.

19. **Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?**

The Data Privacy Act does not impose any obligations to notify the regulator or individuals of security breaches, because currently in Chile there is no Data Privacy Officer yet.

Nevertheless, there are specific rules regarding banks and data of their clients in which encryption is mandatory and notice of security breach. This regulation is transitory and, it was dictated by the entity that supervises the banks. Currently, the Bill that includes regulation in these matters is pending in Congress.

Furthermore, see answer to question 18 regarding cybersecurity directive to the public sector, issue by the President of Chile.

20. **Do the laws in your jurisdiction provide individual rights, such as the right to access and the right to deletion? If so, please provide a general description on what are the rights, how are**

they communicated, what exceptions exist and any other relevant details.

Yes, according to the Data Privacy Act:

Right to access or information: The subject or holder of personal data has the right to request information about him/herself, its origin data (how this data was collected); and addressee, the purpose of the storage and the identification of the persons or agencies to whom his/her data is regularly transmitted.

The information of personal data shall be free of charge. This right to access cannot be restricted by means of any act or agreement, except when it prevents proper compliance with the supervisory functions of the requested government entity or if it affects the confidentiality or secrecy established in legal or regulatory provisions, or the security of the nation or the national interest.

In order to exercise the right to access, the data subject must address to the person responsible for the data registry or data base claiming his/her right to access and if the person responsible for the personal data registry or bank fails to respond within two business days, or refuses a request on grounds other than the security of the nation or the national interest, the subject of the personal data shall have the right to sue before the civil court.

Right of modification: in case of erroneous, inexact, equivocal or incomplete data, and such situation has been evidenced;

Right of blocking: when the individual has freely provided his/her personal data or 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 subject may also request data be eliminated if its storage lacks legal grounds or if it has expired, when the subject has voluntarily provided his/her personal data, or it is used for commercial communications or does not want it to continue appearing in the

respective registry, either definitively or temporarily;


Right to free copy: the information, modification or elimination of personal data shall be free of charge, and a copy of the fragment of the registry that has been changed shall also be provided at the subject's request. If new modifications or eliminations of data are made, the subject may obtain a copy of the updated registry without cost, if at least six months have passed since the last time requested; and

Right of opposition/object: the subject may object the use of his/her personal data for purposes of advertising, market research or opinion polls.

21. **Are individual rights exercisable through the judicial system or enforced by a regulator or both? When exercisable through the judicial system, does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances? Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury of feelings sufficient?**

Yes. The rights included in the Data Privacy Act could be exercised through the judicial system, that is, through a summary procedure established in the Act itself. In the case that the person responsible for the data base, do not give an answer to the data holder within two business days following the respective request (for access, adjustment, deletion or blocking of personal data), or else the data controller rejects the request for reasons other than the national security or the national interest, the holder of the data has the right to initiate the judicial procedure.

Breaches of data protection caused by inappropriate processing of data could eventually lead to fines determined by the Data Privacy Act (fluctuating from US\$ 73 to US\$ 730 and US\$ 730 to US\$ 3,615 if the breach comes from financial-data). Fines-Penalties are viewed and determined in a summary judicial process.



The Data Privacy Act states a general rule under which damages (both non-monetary and monetary damages) that result from willful misconduct or negligence in the processing of personal data shall be compensated. The amount of compensation shall be established reasonably by the civil judge, considering the circumstances of the case and the relevance of the facts. There is no criminal liability for non-compliance with the Data Protection Act; Nevertheless, in relation to cybersecurity, the Law No. 19.223, states criminal liability for the actions described therein.

22. **How are the laws governing privacy and data protection enforced? What is the range of fines and penalties for violation of these laws? Can PII owners appeal to the courts against orders of the regulators?**

The Data Privacy Act is enforced through the judicial system through a summary jurisdictional process states by the Act, if the person responsible for the personal data registry or data base does not comply with the Act or fails to respond within two business days to a request of access, modification, elimination or blocking of personal data, or refuses a request on grounds other than the security of the nation or the national interest.

According to Chilean law, actual damage is required in order to be entitled to monetary damages or compensation. In fact, the Data Privacy Act states a general rule under which damages (both non-monetary and monetary damages) that result from willful misconduct or negligence in the processing of personal data shall be compensated. The amount of compensation shall be established reasonably by the civil judge, considering the circumstances of the case and the relevance of the facts. There is no criminal liability for non-compliance with the Data Protection Act; Nevertheless, in relation to cybersecurity, the Law No. 19.223, states criminal liability for the actions described therein.

A final ruling issued by the general courts of Chile regarding the procedure briefly described in the paragraphs could be appealed before to the respective Appeal Court.

23. **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

According to Net Neutrality Law No. 20,453, states the principle by which the ISPs and those that own and administrate the backbone structure of the internet service, shall not make any discrimination and differentiation among the information that runs through their equipment or the network infrastructure. This law was complemented by a special regulation, published on 18 March 2011, which establishes the specific requirements that ISPs shall accomplish in connection with these network neutrality legal obligations. In addition, PTS concessionaires that provide internet access services (IAS), services providers (SP) and also ISPs: cannot arbitrarily block, interfere with, discriminate against, obstruct or restrict the right of any internet user to use, send, receive or offer any content, application or legitimate service through the internet, as well as any other activity or legitimate use performed through the network. They shall provide each user with an internet service access or connectivity with the provider of internet access, as appropriate, which cannot arbitrarily distinguish content, applications or services, based on the source or ownership thereof, taking into account the different configurations of the internet connection under the current contract with the users; cannot limit the right of a user to add or use any sort of tools or devices on the network, provided that they are legitimate and that they do not damage or harm the network or the service quality; shall provide, at the expense of users who request such services, parental control services for contents against the law, morality or good customs, provided that the user is clearly and precisely informed in advance about the scope of such services; and shall publish on its website all information connecting to the characteristics of internet access service offered, speed, link quality, distinguishing between national and international networks, as well as the nature of the service and service warranties.

Nevertheless, providers of PTS and ISPs could take the measures or actions necessary for traffic and network management, in the exclusive scope of activity that has been licensed to them, if this is not designed to perform actions that affect or may affect free competition.

Providers of PTS and ISPs shall seek to preserve user privacy, virus protection and

network security.

Additionally, ISPs may block access to certain content, applications or services, only at the express request of the user and at such user's own expense. This blocking cannot arbitrarily affect other providers of services and applications that are provided through the internet. Finally, according to our legislation, a court instruction might order to block access to internet sites or services either by a ruling or an injunction.

Cybersecurity Policy: The country will have in place a robust and resilient information infrastructure, prepared to face and recover from cybersecurity incidents, under a risk management approach. In this regard:


- Concept. Risk identification and management: Cybersecurity is described as a condition presenting the least risk for cyberspace –understood as a set of physical and logical infrastructure, and the human interactions taking place in the same. Within this set, the main feature to be protected is information confidentiality, integrity and availability which, in turn, create a robust and resilient cyberspace.

This framework does not include the increased capability of state or private surveillance actions by using digital technologies, which relate with public order or national security objectives and are discussed in other instruments having a different focus. Surveillance actions proposed in this instrument will only be aimed at managing the risks of information in the cyberspace.

Prevention and management models for cyberspace will be created from the Policy, including physical risks that may affect the same, regularly updated by a continuous improvement model, which shall be the basis for technical measures to be adopted in order to prevent, manage and overcome actual risks, with an emphasis on service resilience and continuity within a set deadline and focus on maximizing the country's cybersecurity levels.

- Protection of the information infrastructure Information infrastructure is composed of people, processes, procedures, tools, installations and technologies supporting the creation, use, transport, storage and destruction of information.

There is an especially relevant group, within information structure, for a country to keep moving forward, called critical information infrastructure (CII), which includes the installation, networks, services and physical and information



technology equipment whose impairment, degradation, rejection, interruption or destruction may have an important impact on the security, health and wellbeing of people and on the effective operation of the State and the private sector.

Special emphasis will be placed on the impact that an information security incident may have on physical infrastructures controlled or monitored from the cyberspace, and on the security of industrial surveillance sensors and devices enabling such actions.

CII shall be designed with an architecture maximizing their robustness and resilience against events that may render them non-operational, and enabling them to adapt to natural phenomena, human interventions and information interferences such as non-voluntary incidents or cyber-attacks.

- Identification and prioritization of critical information infrastructure

Sectors included in the definition of CII are very similar and recurrent in various international classifications. In Chile, while consideration of a specific policy for critical infrastructure is under consideration, information infrastructure in the following sectors will be considered as critical: energy, telecommunications, water, health, financial services, public security, transport, the civil service, civil protection and defense. The policy contains a full set of areas, roles and responsible State entities used to identify and specify the critical level of each sector.

Technical bodies in charge of executing measures derived from this policy shall include special cybersecurity standards for CII depending on the different levels of development, especially about special processes.

The medium term will see the implementation of measures ensuring service continuity through the redundancy of the physical infrastructure of some CII, especially in the fields of telecommunications, civil service, civil protection and defense.

24. **Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies - how are these terms defined and what restrictions are imposed, if any?**

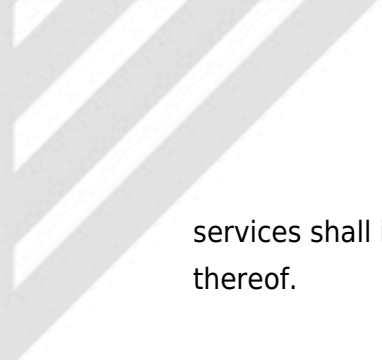
There are no laws governing online privacy on the use of tracking technologies such as cookies. In case, cookies gather personal data, they may be deemed as data processing, hence companies that place cookies, will require consent of the data subject. In addition, there is some risk in the use of cookies when is related to the Law No. 19,223 on computer crime that is not allowing unauthorized access to computers and information therein.

See also answer to question 23 regarding Net Neutrality Law No. 20,453.

25. **Please describe any laws addressing email communication or direct marketing?**

Currently, private entities can create and maintain data bases for purposes of sending marketing and promotional emails, provided that provided that are collected from publicly accessible sources, and it is required for direct response to commercial communications or marketing, or direct sale of goods or services. Though, any individual may require that his/her information be deleted in this case, either permanently or temporarily.

Therefore, under the law, electronic marketing is protected in the sense of establishing that no authorization is required for electronic marketing when the information comes from sources available to the public. In addition, Law No. 19,496 on the Protection of Consumer Rights contains a provision regarding marketing by email (also known as spam). In that case, every advertising or promotional communication sent by email shall specify the subject, the identification of the sender and a valid email address to which the recipient can request the suspension of the advertising communication, which will remain banned from then on (opt-out). Providers of direct promotional or marketing communications to consumers via mail, fax, telephone calls or messaging



services shall indicate an expedited way the addressees may request the suspension thereof.