Jurisdiction	Chile
Date	April 6, 2022
Law Firm	Urenda, Rencoret, Orrego & Dörr
Title, Name	Partner, Sergio Orrego; associate, Bernardita Schmidt
Contact Information	sorrego@urod.cl; bschmidt@urod.cl

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future?

Currently, Chile has a general law concerning the protection of personal information in the private and public sector.

The protection of personal data is regulated in the Constitution of Chile, which guarantees in its article 19 No. 4 the respect and protection of private life and honor of all persons and their families, and the protection of their personal data, setting forth that the processing and protection of said personal data shall be carried out in the manner established by law.

Besides constitutional protection, Law No. 19,628 enacted in 1999 on Protection of Private Life (the "DPL") is the main data protection law in Chile, which applies to private and public sector. In summary, this law regulates the processing of personal data in public or private registries or data banks in general, specifying the rights and obligations of the parties involved; the use of personal data relating to economic, financial, banking or commercial obligations; a procedure for the resolution of disputes; and the liability in case of infringements. It is important to note that, currently, the DPL does not consider a public agency in charge of monitoring data protection in Chile, so in the event of an infringement, any claim by affected data holders has to be filed before the ordinary courts of justice.

Congress is currently discussing a bill submitted on March, 2017 to amend the DPL (the "Bill"), which seeks to set higher standards for data protection, including the creation of a Personal Data Protection Agency, the creation of new rights for data holders (e.g. portability), the regulation that the consent can be evidenced not only in writing but also verbally or it can be expressed by electronic means, the establishment of specific fines for infringement of the DPL (the Bill seeks

to materially increase fines depending on the seriousness of the breach), the creation of a special category of personal data (of boys, girls and teenagers), the regulation of international transfer of personal data, etc.

There is no clear date for the approval and enactment of said Bill. If passed, the Bill would largely align Chilean law on data protection with the EU's General Data Protection Regulation.

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future?

As mentioned, the Constitution of Chile protects personal information in the private and public sector. Also, law No. 19,628 on the Protection of Private Life applies to public sector, specifically regulating the processing of data by public entities in Title IV.

iii. Does your country have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.)

Currently, other laws and regulations refer to or contain certain data privacy provisions, such as:

- Chilean Labor Code: states that the employer shall maintain confidentiality of all private information and data of the employee to which it has access due to the labor relationship (article 154 bis). Also, it expressly states that employers can exercise their rights within the limits imposed by the Constitution, especially regarding respect of privacy (article 5).
- Law No. 20,575: establishes the 'purpose principle' for the processing of certain personal data for commercial risk assessment and credit granting process.
- Law No. 20,584 (regulates the rights and duties of individuals in connection with healthcare actions): pursuant to this law, all information that arises from patient files, studies and other documents that register medical treatments or procedures will be considered as sensitive data. Also, this law establishes the obligation of healthcare professionals to maintain patient data confidential and to comply with the principle of purpose limitation.
- Law No. 19,496 (Consumer Protection Act): establishes the regulation regarding unsolicited commercial marketing on the protection of consumers' rights. Recently the

Servicio Nacional del Consumidor (National Consumer Service or "SERNAC") has some supervisory powers regarding personal data of consumers processed within a consumer relationship.

- Decree with Force of Law No. 3/1997 (General Law of Banks): article 154 establishes the confidentiality of individuals' transactions with and through banks.
- Law No. 20,285 on access to public information: article 33 m) establishes that one of the functions of the *Consejo para la Transparencia* (Council for Transparency) is to ensure compliance with the DPL by public entities.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I. (please add a reply column as necessary).

a) The title of the law：Constitution of the Republic of Chile

① The definition of "Personal Information"	Does not provide a definition.
② The scope in which the law applies	Fundamental law of Chile, which has a higher rank than the rest of the laws.
③ The territorial scope	Applies to the territory of Chile
④ URL	https://www.bcn.cl/leychile/navegar?idNorma=242302
⑤ Effective Date	August 11, 1980 (provision regarding protection of personal data was introduced in 2018).

b) The title of the law ：Law No. 19,628

① The definition of "Personal Information"	Personal data is defined as data related to any information regarding natural person, either identified or identifiable. Sensitive data is defined as personal data referred to individuals' physical or moral characteristics or facts, or circumstances of their private life or intimacy, such as personal habits, race, political views, religious beliefs, physical or mental health and their sexual life.
② The scope in which the	The DPL applies to the processing of personal data in

law applies	public and private registries or data banks in general. Processing is defined as any operation or set of operations or technical procedure, whether automated or not, that allows to collect, store, record, organize, elaborate, select, extract, confront, interconnect, dissociate, communicate, assign, transfer, transmit, or cancel personal data, or use them in any other way.
③ The territorial scope	Territory of Chile.
④ URL	https://www.bcn.cl/leychile/navegar?idNorma=141599
⑤ Effective Date	August 28, 1999.

c) The title of the law ：Chilean Labor Code

① The definition of “Personal Information”	Does not provide a definition. Nevertheless, this Code sets forth that the employer shall maintain confidentiality of all private information and data of the employee to which it has access due to the labor relationship (article 154 bis).
② The scope in which the law applies	Employment relationship.
③ The territorial scope	Territory of Chile.
④ URL	https://www.bcn.cl/leychile/navegar?idNorma=207436&idParte=0
⑤ Effective Date	July 6, 1987 (article 154 bis was introduced in 2001).

d) The title of the law ：Law No. 20,575

① The definition of “Personal Information”	Does not provide a definition.
② The scope in which the law applies	Data processing for commercial risk assessment and credit granting process
③ The territorial scope	Territory of Chile.
④ URL	https://www.bcn.cl/leychile/navegar?idNorma=1037366
⑤ Effective Date	February 17, 2012.

e) The title of the law ：Law No. 20,584

① The definition of “Personal Information”	Article 12 sets forth that all information that arises from patient files, studies and other documentations of medical treatments or procedures are sensitive data.
② The scope in which the	Rights and duties of individuals in relation with

	law applies	healthcare actions.
③	The territorial scope	Territory of Chile.
④	URL	https://www.bcn.cl/leychile/navegar?idNorma=1039348
⑤	Effective Date	April 24, 2012.

f) The title of the law ：Law No. 19,496

①	The definition of “Personal Information”	Does not provide a definition.
②	The scope in which the law applies	Consumer relationship.
③	The territorial scope	Territory of Chile.
④	URL	https://www.bcn.cl/leychile/navegar?idNorma=1160403
⑤	Effective Date	March 7, 1997 (SERNAC’s supervisory powers regarding personal data of consumers was introduced in 2021).

g) The title of the law ：Decree with Force of Law N° 3/1997

①	The definition of “Personal Information”	Does not provide a definition. Nevertheless, article 154 establishes that some transactions with banks are covered by secrecy and others by reserve.
②	The scope in which the law applies	General Law of Banks.
③	The territorial scope	Territory of Chile.
④	URL	https://www.bcn.cl/leychile/navegar?idNorma=83135
⑤	Effective Date	April 4, 1960 (provision regarding secrecy and reserve was introduced in 1987).

h) The title of the law ：Law No. 20,285

①	The definition of “Personal Information”	Does not provide a definition.
②	The scope in which the law applies	Access to public information.
③	The territorial scope	Territory of Chile.
④	URL	https://www.bcn.cl/leychile/navegar?idNorma=276363
⑤	Effective Date	August 20, 2008.

ii. If there are any special instructions about the laws, please describe them.

Please see above.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

Pursuant to article 4 of the DPL, processing of personal data can only be carried out when authorized by law or when the data holder expressly consents in writing thereto. However, the DPL considers exceptions (please see section ii.(a) below) which allows personal data to be processed without the data subject´s consent.

With respect to sensitive data, the DPL sets forth that it may only be transferred or used if authorization is granted by law or by the data holder, or if such data is necessary for determining or granting health benefits to the data holder.

(b) Data Quality Principle

Article 9 of the DPL establishes that personal data shall be used solely for the purpose for which it was collected, except if it comes or was collected from publicly available sources. The processed data shall be accurate, current and reflect the actual situation of the data holder.

The party responsible of a data bank where personal data is processed shall eliminate or cancel personal data when there is no legal basis for its storage, or when the personal data has expired. Likewise, when erroneous, inaccurate, misleading or incomplete, personal data shall be rectified. If the accuracy or validity of personal data may not be determined, it shall be blocked (if elimination is not required). Said actions shall be taken even in the absence of a request by the data holder. If cancelled or rectified personal data had previously been informed to a third party,

the party responsible of the data bank shall inform the cancellation or amendment to the third party, as soon as possible (article 12 DPL).

(c) Purpose Specification Principle

As mentioned above, according to the DPL, the processing of personal data can only be carried out when authorized by law or when the data holder expressly consents in writing thereto. When giving this consent, the data holder must be duly informed with respect to the purpose of the storage of his/her personal data and the possible communication of the same to the public. The referred to authorization can be revoked by the data holder, in writing.

Moreover, article 1 of law No. 20,575 establishes that the processing of personal data relating to economic, financial, banking or commercial obligations, may only be done in connection with commercial risk assessment and the credit granting process. Therefore, this type of data may only be communicated to established businesses, for said purpose. Also, the referred to data may not be requested in connection with recruitment or preschool, school or higher education admission processes, for urgency medical attentions, or in order to apply to a public office or governmental job.

(d) Use Limitation Principle

As mentioned above, the processing of personal data can only be carried out when authorized by law or when the data holder expressly consents in writing thereto (article 4 DPL). Also, personal data shall be used solely for the purpose for which it was collected, except if it comes or was collected from publicly available sources (article 9 DPL).

(e) Security Safeguards Principle

There are no legal requirements to take appropriate technical security measures to protect personal data. However, the party responsible of a data bank where personal data is stored shall take due care of said data, being liable for any damages (article 11 DPL).

Also, public entities must strictly implement the pertinent measures of the Cybersecurity National

Policy and the Presidential Instructions that impose specific measures on cybersecurity that must be observed by public entities.

(f) Openness Principle

There is no general policy of openness about developments, practices and policies with respect to personal data. Nevertheless, individuals are entitled to demand information about data concerning themselves, its origin and addressee, the purpose of the storage and the identification of the persons or agencies to whom his or her data is regularly transmitted.

(g) Individual Participation Principle

In general terms, according to article 12 of the DPL, data holders can request to the party responsible of the registry or data bank where their personal data is being processed to:

- provide them with information regarding their personal data, including the purpose of the storage and processing, the origin of the data, recipients of the same, etc.
- amend the personal data when the same is erroneous, inaccurate, misleading, or incomplete.
- where applicable, eliminate, cancel or block personal data, mainly when there is no legal basis for the storage of the same, or when the same is not current.

The above rights may not be restricted by an agreement between parties.

If the party responsible of a data bank does not duly and timely respond in 2 business days to a request made by a data holder to obtain information regarding the latter's personal data, or to amend, cancel or block said data, or denies such request based on reasons other than those established by law, then the data holder may file a claim before the relevant ordinary civil court of justice. If the claim is resolved in favor of the data holder, aside from any corrective measures, the court may also impose a fine against the party responsible of the data bank for an amount that ranges between 1 to 50 Monthly Tax Units[1], depending on the type of breach.

[1] 1 Monthly Tax Unit is equivalent to US$70 approx.

In addition, the data holder is entitled to pursue pecuniary and moral damages against the party responsible of the data bank that misused the former's personal data. The indemnification shall be prudentially set forth by the judge based on the circumstances of the case and the seriousness of the facts.

(h) Accountability Principle

The party responsible of a data bank where personal data is stored shall take due care of said data, being liable for any damages (article 11 DPL).

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

The application of the following principles is excluded as follows:

(a) Collection Limitation Principle

According to article 4 of the DPL, no consent is required for the processing of personal data that comes or is collected from public sources, that has an economic, financial, banking or commercial nature, is contained in lists relating to a category or group of persons that only make reference to information such as the belonging of individuals to said group, their profession or activity, educational degrees, addresses or dates of birth, or is required for commercial communications of direct response or direct sale of goods or services. Also, no authorization is required if private legal entities handle personal data for their exclusive use or the use of their associates and entities to which they are affiliated, provided it is used for statistic or rate-setting purposes or for any general benefit of those indicated above.

(b) Purpose Specification Principle

When the personal data has been collected from publicly available sources this principle does not apply.

(c) Use Limitation Principle

When the personal data has been collected from sources available to the public this principle does not apply.

(d) Individual Participation Principle

According to article 15 of the DPL, no information, modification, cancellation or blocking of personal data may be requested when it prevents or hinders proper compliance with the supervisory functions of the government agency to which the request is made or if it affects the confidentiality or secrecy established in legal or regulatory provisions, the security of the nation or the national interest.

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If yes, please describe them.

In Chile there is no regulation of a comprehensive government access to personal data. The processing of personal data by public entities may only be carried out regarding matters within their respective legal authority and subject to the rules set out in the DPL (article 20 DPL).

Regarding Data Localization (understood as the practice of keeping data within the country it originated from) there is no general rule that confine data within Chile's borders. Moreover, the transfer of personal data to other jurisdictions is not specifically regulated or restricted, so general rules of the DPL apply. The Bill seeks to regulate this matter, expressly allowing cross border transfer of personal data in certain cases (e.g., when the recipient is subject to a legal system that provides adequate level of protection to personal data; when the transfer of data is governed by contractual provisions; when the data holder expressly consents to a specific transfer, etc.).

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the

authority.

Currently, there is no data protection authority. However, in August 2021 the National Congress of Chile dispatched the pro-consumer Bill No 12.409-03 to Establish Measures to Encourage the Protection of Consumer Rights, which came into force in December 24, 2021 (Law No. 21,398). This law grants SERNAC some supervisory powers regarding personal data processed within a consumer relationship.

Additionally, article 33 of Law No 20,285 establishes that one of the functions of the Council for Transparency is to ensure compliance with the DPL by public entities.

Finally, as mentioned, the Bill seeks to set higher standards for data protection, including the creation of a Personal Data Protection Agency (*Agencia de Protección de Datos Personales*).