Bloomberg BNA | Bloomberg Law®: Privacy & Data Security

Reproduced with permission from Bloomberg Law: Privacy & Data Security, http://www.bna.com/bloomberg-law-privacy-data-security/.

Country Profile: CHILE

Rodrigo Velasco Alessandri of Alessandri Abogados, Santiago, provided expert review of the Chile Country Profile and wrote the Risk Environment section.

I. Applicable Laws and Regulations

Data processing and protection in Chile is governed primarily by Act No. 19-628, Law for the Protection of Private Life (PDPL) (in Spanish). Under Article 19 No. 4 of the Constitution of the Republic of Chile (in Spanish; in an unofficial English translation), an individual has the right to respect and protection of his/her private life and personal honor and those of his/her family, a fundamental privacy right further protected under the PDPL. Data processing refers to any operation or set of operations and technical procedures, automated or not, to collect, store, record, organize, develop, select, extract, compare, interconnect, dissociate, communicate, assign, transfer, transmit, or cancel personal data, or use it in any other form (PDPL art. 2(o)). Personal data is any information that refers to an identified or identifiable individual (PDPL art. 2(f)).

Personal data processing is generally only allowed when authorized by the PDPL, under another legal provision, or with the express consent of the data subject (PDPL art. 4). The data subject authorizing this processing must be duly informed of the purpose of the personal data storage and its possible communication to the public. Consent must be in writing and it may be revoked. Notwithstanding the above, consent is not required to process publicly accessible data from a legitimate source where (1) it is economic, financial, banking-related, or commercial in nature and meets other specific requirements under the PDPL (see art. 17); (2) it is background information about an individual to identify him/her as a member of a group and it is limited only to his/her profession, educational degrees, address, and date of birth; or (3) it is information necessary for direct marketing or advertising or sale of goods and services (art. 4). Another broad exception to the consent requirement is when the processing of personal data is done by a private legal entity or person for its exclusive use or for use by its associates and affiliates, for statistical purposes or tariff purposes, or for other purposes for their general benefit (art. 4, ¶5). Data controllers are required to designate a person or entity responsible for handling requests for information from its databases that contain personal data (art. 2(n) and 17). People that process personal data, whether as part of private or public entities, are required to keep information about the data secret when the data comes from sources that are not publicly accessible. This obligation does not cease after they end their employment in that field (art. 7). Personal data must only be used for the purposes for which it was collected, unless it comes from public sources (art. 9).

A data subject has the right to oppose the use of his/her personal data for purposes of advertising, market research, or opinion polls (PDPL art. 3, ¶2). Under Article 28B of the Consumer Protection Law, Law No. 19-496 (in Spanish), any promotional communication or e-mailed advertising must indicate the subject matter, the identity of the sender, and a valid address to which the recipient may send a request to opt out; and the communications must cease once an opt-out request is sent. Sellers or providers (manufacturers, service providers, etc.) that send promotions or advertising to consumers via mail, fax, or telephone must indicate one way recipients can expeditiously request suspension of those materials. After a consumer requests suspension, new communications are prohibited (art. 28B and 1(2)).

Government bodies and agencies are required to register databases containing personal data with the Civil Registry and Identification (in Spanish), which,

for each entry, contains the legal basis for the database, its purpose, data types stored, and all parties involved (PDPL art. 22). The agencies must inform the Civil Registry and Identification of any changes to that information within 15 days (PDPL art. 22).

Law No. 19-223 (in Spanish) provides for criminal penalties of imprisonment up to five years for maliciously altering, damaging, or destroying data contained in an information processing system as well as revealing or disseminating such data. Law No. 20-575 (in Spanish) regulates the processing of economic, financial, banking, or commercial personal data, which can only be communicated for commercial risk assessment and the credit process. Data controllers that process these types of data are subject to additional restrictions under Articles 17–19 of the PDPL.

II. Regulatory Authorities and Enforcement

Chile does not currently have an independent data protection authority. Personal data processing and data protection is overseen by the courts. An individual can bring a civil suit against persons or entities responsible for a database that caused property or moral damage to the individual by improperly processing his/her data under Article 23 of the PDPL, subject to appeals in the applicable Court of Appeals (PDPL art. 16(g)). For example, if an individual tries to exercise his/her right of access or to correct misleading personal data that an employer has about him/her (art. 12) and the data controller or the entity responsible for processing those data requests does not provide the information or make the modification in timely manner without cause, the individual can appeal to the civil court where the data controller is domiciled (PDPL art. 16). If the matter involves national security or the national interest, the claim must go before the Supreme Court (art. 16(h)). A judge can take measures deemed appropriate to protect the individual's rights under the PDPL, and determine an appropriate amount of compensation considering the circumstances and gravity of the facts of the case (art. 23). Violations involving economic, financial, banking-related, or commercial personal data can result in a fine of 10–50 UTM ("monthly tax unit"), an inflation-indexed measure of value, adjusted on a monthly basis (see PDPL art. 16; U.S. Department of State, 2013 Investment Climate Statement—Chile, Performance Requirements/Incentives, ¶6.) Untimely delivery of information or delay in making modifications to data as ordered by a court is punishable by a fine of 2 to 50 UTM if a public body is responsible for the database, and suspension of 5 to 15 days of the person responsible from his office.

The Transparency Council (in Spanish) ensures bodies of the State Administration comply with PDPL (art. 33(m)). Individuals can bring claims regarding relevant bodies directly to the Transparency Council (see Law of Transparency and Access to Public Information, Frequent Questions, 5, in Spanish). The Council's total 2015 Budget is 5,379,186 Chilean pesos. According to a 2013 Personnel Report, the Council employed around 346 people. The Council's August 2015 Monthly Statistics Report indicates that 345 agencies actively use the Council's Transparency Portal to process requests.

III. Risk Environment

Chile has no centralized Data Protection Authority; enforcement of the current data protection law is entrusted to the civil courts, and there are few cases interpreting the PDPL. The Courts are still not trained in this area of law, and the procedure is slow and expensive, which makes cases difficult to prove. Also, general legal remedies and torts are operating when there is damage as a consequence of a data security breach derived of a contract applying the general principles of the Civil Code.

Responding to the lack of enforcement, individuals have used other sources to enforce their rights, such as constitutional resources, administrative actions, and special protections arising from various legal instrumentalities in other areas of the Law. Practically speaking, multiple government ministries and entities are responsible for data protection in diverse sectors; the risk of enforcement depends on the industrial sector to which a business operator belongs and types of data that the business operator handles.

From the legislative perspective, the Chilean Congress is discussing substantial amendments to the law. These amendments are expected to be passed by the end of the current government. There are many groups contributing to the bill, and both the government and the general public consider this to be an important topic on the Government Agenda.

The Draft calls for the creation of a National Council for Data Protection, as an autonomous body to promote and control the protection of personal data, a National Data Protection Registry, the regulation of trans-border flows of personal data, and enhanced penalties for violations of the Law.

IV. EMERGING ISSUES AND OUTLOOK

A. New Draft Data Protection Law Announced

As Bloomberg BNA reported in May 2015, the Chilean government announced intentions to introduce new legislation on personal data protection which in part would create an independent data protection authority and bolster data protection enforcement. See "Long-Awaited Data Privacy Bill to Be Unveiled in June, President Says," *World Data Protection Report* (May 27, 2015). The report's title proved optimistic; at this writing, the new law has yet to be introduced and adopted. Processing milestones in proposed amendments to the PDPL are available at the Chamber of Deputies of Chile.