/Carey

June 8, 2016

LEGAL ALERT

Bill of Law Which Will Modify the Chilean Data Privacy Act

The government recently announced that a bill will be submitted to Congress to modify the Chilean Data Privacy Law N° 19,628 (“DPL”). In connection with the future bill (yet to be presented before Congress), the Ministry of Finance sent to several members of Congress a set of informal minutes outlining the structure and core aspects of the bill.

The following is a summary of the minutes, and an initial legal analysis prepared by Carey. Please note that the minutes are not official and have not been officially published by the government.

- The law will have **transversal applicability**, binding individuals and legal entities alike, whether public or private. The legal definitions will be updated and expanded in accordance with international standards.
- **Principles** of legality, purpose, proportionality, quality, security, responsibility and information will be expressly incorporated.
    - Only some of these principles are captured by the current DPL. These principles will result in new and specific obligations for data controllers.
    - We expect that the security and responsibility principles will involve new obligations related to security measures, and notification obligations related to data breaches, none of which are currently required.
    - The principles of purpose and information should provide clear provisions regarding the minimum content of personal data processing authorizations.
- Processing of personal data is allowed **as permitted by law or upon consent of the data subject**.
    - We expect that the definition of “law” in the clause above will allow for broad interpretation under this bill, so that companies will be exempted from the obligation to gather consent, provided they are subject to any

other law or sector-specific regulation that compels them to process data.

- **Consent** must be** first obtained, freely given, unequivocal and informed**.
  - Requirements of prior and informed consent are new; notwithstanding that the “prior” requirement was already generally accepted by doctrine and some administrative jurisprudence. The level of detail concerning the “free” requirement will be of great importance.
  - Written consent is replaced by the technologically neutral unequivocal consent; which will in practice allow a more liberal interpretation of manifestations of consent.
  - It will be interesting to see what exceptions arise under this bill. Currently, the LPD does not provide for reasonable exceptions to the obligation to obtain consent (e.g., domestic use, exigent circumstance).
- **Individual’s rights of access, rectification, cancellation and opposition** will be free of charge and non-waivable.
  - The right to challenge decisions when the decision is based on automated data processing is not included among these fundamental rights. It is likely that this matter will still be regulated in the law, but as a less fundamental, waivable right.

- The definition of **sensitive data** is extended to include gender, genetic and biomedical identity. New categories of sensitive data will be created such as health, children, biometric, genetic and proteomic related data.
  - It will be relevant to analyze the way in which the standards of data processing will be increased. The current LPD regulates sensitive and non sensitive data in a similar manner, only drawing a distinction on the fact that sensitive data allows for no exceptions to the obligation to gather the individual’s consent.
  - Innovation is made on the recognition of biometric, proteomic and genetic data. It will be interesting to analyze its definition; the practical application of its associated obligations; and how the law works out any contradictions arising between these limitations and the development of scientific activities.
- **Cross border data transfer** is regulated for the first time. These transfers shall only be allowed in countries with reasonable levels of protection, which would be countries with a similar standard of regulation

to Chile.

- No changes are made regarding **financial, banking and commercial personal data**.

  - This is being done in concert with the announcement of processing the bill of law on SOE (Economic Obligations System for its acronym in Spanish) in parallel.

- A **Data Privacy Authority** will be created: the National Direction of Data Privacy, which will oversee regulatory compliance with the LPD and enforcement.
- A **new set of infringements** will be created **with specific sanctions** of up to UTM 10,000 (USD 671,500 approximately) or in extreme cases the closure of the data processing operation.
- An obligation to **register databases** will be implemented, excluding databases for domestic use.

  - It will be important to review the extent of this obligation, particularly if the obligation requires registering modifications of the content of the registered databases (which are naturally dynamic and subject to constant change).

- A **complaint procedure** will be launched with three mandatory steps: first, a direct claim before the data processor; second, an administrative claim before the National Direction of Data Privacy; and finally a judicial claim disputing the decision of the National Direction of Data Privacy.
- New incentives for companies' compliance obligations are set up in the form of "infringement prevention models".

  - This space for self-regulation or construction of codes of conduct can be essential in the adjustment of the companies to this new legal structure. The specific tools granted to the private sector shall be relevant, and they will most likely be related to codes of conduct and self-regulatory statutes.
  - The adoption of "preventive models of infringements" shall consider clear and easily applicable incentives.

Authors: Guillermo Carey