/Carey

Analysis of the Bill which will Amend the Law Governing the Protection and Processing of Personal Data, and that Creates a Personal Data Protection Agency in Chile

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Carey contact.

Guillermo Carey
Partner
+56 2 2928 2612
gcarey@carey.cl

Paulina Silva
Counsel
+56 2 2928 2665
psilva@carey.cl

Carey y Cía. Ltda.
Isidora Goyenechea 2800, 43rd Floor
Las Condes, Santiago, Chile.
www.carey.cl

On Monday, March 13, 2017, the Chilean President sent a bill (the "**Bill**") to the Senate that significantly amends law No. 19,628 on Protection of Private Life.

The Bill seeks, among other things, to increase protection of privacy in order to fulfill international standards in matters of personal data processing, to meet the guidelines of the Organization for Economic Cooperation and Development (OECD), to adapt and modernize national legislation to meet the challenges that a digital economy entails, and to balance the safeguarding of people's privacy with free circulation of information.

The Bill will enter in force and effect 13 months after its publication, however, previously established databases will be allowed 4 years from the time the law enters into force to adapt their practices.

I. SCOPE OF THE BILL

The Bill regulates the processing of personal data as performed by individuals and organizations, both public and private, which are not governed by a special law.

The application of the law excludes the processing of data performed by the media in the exercise of freedom of press, and the processing performed by individuals in regard to their personal activity.

II. KEY AMENDMENTS

- It sets forth new principles that shall govern the use of personal data and new rights for data subjects.
- It defines and restricts the scope of the concept of personal data. Today, data is personal when it relates to information concerning an individual, whether identified or identifiable. The Bill qualifies this "identifiable nature" to means that require a reasonable effort.
- It regulates in greater detail the concept and requisites for consent, defining it as a free, specific, unequivocal, and informed manifestation that ought to be granted beforehand, and that must be specific regarding a purpose. The unequivocal manifestation must involve, "an act of assertion proving the clarity of the subject's will"; surpassing the "in writing" requisite of the current law.

/Carey

- It establishes a new statute of exceptions for consent.
- It establishes a conceptual difference between data communication or transmission (in which data is disclosed to a third party, without transferring the actual data source) on the one hand; and the assignment or transfer, which requires the fulfillment of additional requisites and makes the assignee responsible for the database.
- It further develops the concept of Sources of Public Access, specifying that they shall be those which may be accessed or consulted in a lawful manner by anyone, without restrictions, or legal obstacles, to access or use them. Additionally, it establishes sources of public access as an autonomous exception.
- It regulates sensitive data in greater detail (establishing new data, such as biometric data, and data regarding biological human profiles); and it establishes a new category of "special data", for the data of children; data used for historical, statistical, scientific purposes and others; and georeferentiation data.
- It restricts the automated processing of data, entitling data subjects to request that no decision affecting them significantly be adopted exclusively on the grounds of the automated processing of that data, with certain exceptions.
- It creates a Personal Data Protection Agency with the authority to monitor and punish violations of the law with of fines of up to 5,000 UTM[1] (approximately USD 350,600 at the date the Bill entered Congress).
- It creates a National Registry for Compliance and Penalties.
- It sets forth new procedures to prosecute liabilities.
- It regulates international data transfers.
- It regulates the duty to adopt safety measures, and reporting obligations in regard to security breaches.

[1] N. from the T.: UTM, acronym for the Spanish Unidad Ttributaria Mensual, or Monthly Tax Unit, a unit of account used in Chile for -as the name suggests- tax purposes, and calculated and published by the Chilean Central Bank.

- It establishes the possibility for the data controller to adopt and certify a model for breach prevention, associated with mitigating circumstances regarding liability.

III. PRINCIPLES

- **Principle of Lawfulness:** Processing of personal data may only be performed with the consent of the data subject or via the action of the law.

- **Principle of Purpose:** The processing of personal data must be limited to the fulfillment of the specific, explicit, and lawful purposes for which they were gathered.

- **Principle of Proportionality:** Personal data to be processed shall be limited to those that are necessary for the purposes of the processing. Plus, they must be kept only for the time necessary to meet the purposes of the processing, and after that they must be cancelled or made anonymous. A lengthier time span shall require a new legal authorization, or consent from the data subject.

- **Principle of Quality:** Personal data ought to be accurate and, if necessary, complete, and current, regarding the purposes of the processing.

- **Principle of Liability:** Those processing personal data shall be legally liable for the fulfillment of the principles, obligations, and duties set forth by law.

- **Principle of Safety:** Suitable levels of safety should be guaranteed, protecting data from unauthorized processing, loss, leaks, destruction, or accidental damage, and applying suitable technical or organizational measures.

- **Principle of Information:** The policies on data processing must be permanently accessible and available to anyone interested, in an accurate, clear, and unequivocal manner free of charge.

IV. DATA SUBJECT RIGHTS

- **Right to Access:** The right to obtain confirmation as to whether their data is being processed, to access their data and to obtain information regarding the origin of the data, the purpose for processing, addressees and timeframe during which their data is used.

- **Right to Rectification:** The right to request a correction whenever data is inaccurate, outdated, or incomplete.

- **Right to Cancellation:** The right to request a cancellation, among other scenarios, whenever data is unnecessary regarding the purposes of the processing, whenever consent has been withdrawn or when the data has expired. The Bill contains certain exceptions to this right.

- **Right to Opposition:** A subject's right to oppose the processing of their personal data, whenever such processing lacks lawfulness, whenever it refers to expired data, whenever it is used for advertising or marketing purposes, whenever it causes an arbitrary or unlawful damage to the subject, whenever it is an automated processing and decisions are adopted that imply an evaluation of the behaviors performed only on the grounds of that sort of processing, or whenever the subject of such data has passed away.

- **Right to Portability:** The right to obtain a copy of their personal data in a structured, generic, and regularly used electronic format, in order to communicate or transfer it to another party responsible for the database, when the data subject has delivered its data and the latter is processed in an automated manner, or when the data subject has given their consent, or the data is required for the execution of, or compliance with, an agreement.

- In order to protect the effective exercise of these rights, the Bill awards them with a personal, non-transferable, and inalienable nature. Additionally, such rights may be exercised by the heirs of the data subject after the latter has passed away.

- The timeframe for the data controller to reply to a data subject requirement is 10 business days following the filing date.

V. PROCESSING OF PERSONAL DATA

General Rule: Consent

Processing of personal data is legal – as a general rule – as long as the data subject grants their consent, or the processing of personal data is authorized by the law.

Consent must be a free, specific, unequivocal, and informed manifestation; it must be granted prior to the processing of personal data, and be specific as to its purpose. This unequivocal manifestation of consent must be granted through an oral or written statement, or granted through equivalent electronic means, or through an act of assertion that clearly evidences the data subject's will.

Consent is revocable without expression of cause, but such act of revocation does not have retroactive effects.

Exceptions to Consent

It shall not be necessary to obtain the data subject's consent for the following processing of personal data:

- If data has been gathered from a source of public access;
- If processing of personal data refers to data related to economic, financial, banking or commercial obligations, and is performed according to the provisions of title III of the law (which regulates use of such data);
- If processing of personal data is necessary for the execution or compliance of a legal obligation, or for an agreement of which the data subject is party to.

/Carey

ASSIGNMENT OR TRANSFER OF DATABASES. Assignment of all or part of a personal database is allowed when such assignment is necessary for the processing of personal data or the tasks of assignor or assignee. To make such assignment, prior consent from the data subject is required, informing him/her on the purpose of the data assignment and the type of activities that the assignee will perform. The assignment agreement must comply with certain requirements. The assignee acquires the role of data controller regarding the assigned databases; and assignor maintains such role regarding the operations it continues to perform.

PROCESSING OF PERSONAL DATA BY AN AGENT. The data controller may process personal data through an agent, who may only process data according to the tasks entrusted to them, and the instructions of the data controller. If the agent exceeds the limits of processing of personal data, they will be considered responsible for the database, and are jointly and severally liable for all legal purposes including infringements and damages.

VI. OBLIGATIONS OF THE DATA CONTROLLER

Among the obligations of the data controller we underscore:

- **Duty of Confidentiality** regarding personal data, except if it comes from a public source or if the data subject made the data manifestly public. This duty also requires dependents of the responsible entity to fulfill the same duty.

- **Duty of Information and Transparency** requires that personal data processing policies be made available to the public along with the identities of the individuals who are responsible for the database, the identification of the means through which the requirements are notified, the types of databases administered along with their characteristics, and the safety measures that are implemented to protect data.

- **Duty of Security** requires the establishment of the necessary safety measures taking into consideration certain variables such as the status of the technology, application costs and other specific variables concerning the data processing, such as the nature and purposes of the processing, the probability and severity of risks.

- **Duty to Report Security Breaches** to the Personal Data Protection Agency, and in some cases, to the data subject.

VII. SENSITIVE DATA AND SPECIAL CATEGORIES OF DATA

Sensitive data

The Bill maintains the structural definition of sensitive data, but extends its examples, in order to include gender, genetic and biomedical identity.

Sensitive data may only be processed if authorized by the law or if the free, informed, express, prior and specific consent of the data subject is granted through a written or verbal statement or an equivalent technological means.

Exceptions to the consent to processing of sensitive data:

- If sensitive data has been made manifestly public by the data subject;
- If the processing of personal data is made by a non-profit organization with a political, philosophical, religious, cultural, sports, union, or trade related organizational end, regarding its members or affiliates, in order to comply with its specific purposes; as long as the organization provides guarantees to avoid non-authorized use and the data is not communicated or assigned to third parties.
- If the processing of personal data is essential to safeguard the life, health or integrity of the data subject.

The Bill separately regulates the following types of sensitive data:

- **Sensitive personal data related to health**, may only be processed, as a general rule, when it is necessary for the diagnosis of a disease or for determining medical treatment.
- **Biometric sensitive data**, processing involves a special duty to deliver information to data subjects.
- **Data related to the human biological profile** (genetic, proteomic, or metabolic data), may only be processed for a specific purpose.

/Carey

Special Data

- **Personal data related to children** may only be processed if it is in the child's best interest and there are safeguards in place to protect the child's progressive autonomy. There must also be prior authorization granted by the child's legal guardian.

- **Data processed or gathered for historical, statistical, and scientific purposes, and for research studies or investigations** require the data subject's consent, which must be granted in an unequivocal, specific, prior and informed manner, and are subject to other special rules.

- **Geolocation data** may only be processed when the data subject has furnished previous, clear, and informed consent, determining the type of geolocation or mobility data that will be processed, its purpose and term of processing, and whether data will be shared with third parties for the provision of services with added value.

VIII. PROCESSING OF DATA BY PUBLIC ENTITIES

Apart from the general principles on processing of personal data, the Bill determines **coordination, efficiency, transparency, and advertising** as guiding principles for processing of data by public entities.

The rights of the data subjects and the rest of the guarantees granted to people by the Bill may also be exercised before public entities, and data subjects can submit an illegality claim in the event the entity violates the rules.

The National Congress, Judicial Branch and Comptroller General of Chile, the Public Ministry, the Constitutional Tribunal, the Electoral Service, the Electoral Commission, and other special courts created by law are excluded from the regulation, oversight or monitoring of the Personal Data Protection Agency.

IX. PERSONAL DATA PROTECTION AGENCY

A Personal Data Protection Agency (APDP for its acronym in Spanish) is created as a public, technical, decentralized entity, with a legal nature and its own capital, aimed at ensuring compliance with rules on personal data processing, and subject to the monitoring of the President of the Republic via the Department of the Treasury.

The Agency will be domiciled in the city of Santiago. Its management and senior administration will be overseen by a National Director who will be the main head of department and who will be appointed by the President of the Republic according to the Senior Management Public System.

The APDP will be an entity with ample powers, which include:

- Issuing general and mandatory instructions
- Overseeing compliance of the law on personal data and its regulations
- Settling claims filed by data subjects
- Working for disclosure and promotion of information to citizens
- Managing the National Registry of Compliance and Penalties

A public **National Registry of Compliance and Penalties** is created. It is administered by the APDP and will record the penalties imposed on those responsible for the database, models for prevention of infringements and duly certified compliance programs. This registry will be maintained and consulted electronically, and there will be no cost to access its information.

X. INTERNATIONAL TRANSFER OF PERSONAL DATA

The Bill regulates international transfers of personal data for the first time, instituting a duty to inform international transfers to the APDP. This transfer is allowed only to the extent it is made to persons or entities bound by a country's legal system presenting **adequate levels of protection** which follow similar or higher standards than those set forth by the law. The APDP will determine the countries with adequate levels of data protection, considering the elements established by the law.

The Bill allows for international transfers of data to countries that do not have an adequate level of protection in some specific scenarios, such as when the data subject has provided express consent; in relation to specific bank, financial or stock market international transfers, transfers carried out between corporations from the same corporate holding, related entities or subject to the same comptroller; or in cases where the transfer is aimed at providing or requesting international judicial aid, among others.

No international transfer of data is deemed to have occurred when an entity responsible for a database carries out data processing operations through a third party, agent of the data controller, subject to another country's laws. The power granted to the agent must be registered in a written agreement and operations must be reported to the APDP.

XI. INFRINGMENTS AND PENALTIES

The Bill classifies infringements as minor, serious and gross, and determines penalties of **fines ranging from 1 to 5,000 UTM (Monthly Tax Unit)** (between USD 70 to USD 351,000 by the date the project was filed).

Criteria are established to determine the amounts of fines, which include **liability mitigating circumstances**: unilateral actions, reparatory agreements entered between the data controller and the affected data subject, prior conduct, self-reporting and collaboration by the data controller on the administrative investigation carried out by the APDP.

In the event of repeated serious and gross infringements, the APDP may instruct the suspension of the data processing operations and their adaptation to the law.

In case of infringement recurrence, a fine may be imposed of up to three times the amount set forth by the law. Recurrence will take place when there are two or more penalties within a 24-month period.

Actions to impose penalties on infringements described in the Bill fall under the statute of limitations three years after the infringement.

XII. NEW PROCEEDINGS

The Bill includes the following proceedings to address infringements to the law on data protection:

- **Administrative proceeding for the safeguard of rights** to be filed before the APDP when the data controller has denied a request by the data subject to exercise any of the rights awarded by the law.

- **Infringement administrative proceeding:** instituted by the APDP as a consequence of a monitoring process or a claim filed by the data subject against the data controller due to legal infringement.

- **Judicial claim proceeding:** those affected by a resolution passed by the APDP may file an illegality claim before the Santiago Court of Appeals, or before the court of appeals of the claimant's domicile, at the claimant's choice.

XIII. MODEL FOR THE PREVENTION OF INFRINGEMENTS

The Bill allows the data controller to adopt a model for the prevention of infringements. The APDP must certify that those models comply with requirements established by the law and its regulations, and must oversee their compliance.

A special attenuation of liability is established for data controllers who prove that they have diligently fulfilled their duties of management and supervision for the protection of personal data under their responsibility.

The Bill instructs the enactment of a regulation that determines requirements, types, and procedures to implement, certify, register and oversee models for the prevention of infringements and compliance programs.