/Carey

April 2018

THE BILL AMENDING THE DATA PROTECTION ACT WAS APPROVED IN GENERAL TERMS: THIS IS ITS CONTENT

A bill that substantially amends the Data Protection Act No. 19,628 is currently being reviewed and processed in the Senate.

The Senate Constitution Committee **consolidated into one single text** two bills amending the data protection act: the Motion submitted by Senators Harboe, Araya, De Urresti, Espina and Larraín, along with the Message from the former President, the content of which we commented on at length a year ago.

On Tuesday, April 3rd, the Senate approved in general **the text of the consolidated bill by 42 votes in favor and one abstention** . In order for the bill to become a law, its discussion in the Senate, in particular, and its discussion in the Chamber of Representatives, is still pending.

The following is a summary of the main aspects of the Bill's current version.

THE BILL'S INNOVATIONS

• It expressly establishes **principles** that regulate and inform the use of personal data and **the new rights** of data subjects.
• **It changes the scope of personal data to** : "any information linked or referring to an identified or identifiable individual (natural person)," classifying that identifiability as such where the identity of the person can be determined using information combined with other data, in particular using an identifier, excluding those cases where the effort to determine the identity is disproportionate.
• It regulates in greater detail the **consent requirements** , defining these as a manifestation of free, specific, unequivocal and informed will; and eliminates the requirement of written consent.
• It establishes **new sources of lawfulness** for processing data, other than the binary processing "legal authorization or consent" of the current law. Namely, scenarios are established where data processing is authorized, even without requiring the data subject's

This news alert is provided by Carey y Cía. Ltda. for educational and informational purposes only and is not intended and should not be construed as legal advice.

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

consent.

• **It conceptually distinguishes between the transfer of personal data and the disclosure** (or transmission) of personal data. A transfer is the handing over of data from one controller to another and requires the fulfillment of special requirements. Disclosure (or communication), in turn, involves making the data known "without transferring them over".

• It establishes **special categories of personal data** subject to special regulations: that of children and adolescents, which are used for historical, statistical or scientific purposes, and geo-localization data.

• It establishes and regulates in a clear manner the rights of data subjects: access, rectification, cancellation, opposition and portability.

• It establishes a new right of **opposition to automated personal valuations** of the data subject, who may object to the controller adopting decisions that could negatively affect in a significant manner the data subject or produce adverse legal effects to the data subject's detriment, based solely on the automated processing of his or her personal data, including the creation of profiles.

• **It creates a Personal Data Protection Agency** that will have the ability to monitor and enforce compliance and penalize violations of the law by applying fines of up to 5,000 UTM (equal to CLP $236,500,000 as at April 2018).

• It creates a **National Registry of Compliance and Sanctions** .

• It establishes **new procedures** for pursuing accountability.

• For the first time, it regulates the **international transfer of personal data** .

• For the first time, it establishes **duties and obligations associated with data security** : the duty to adopt security measures and reporting obligations concerning security measure violations.

• It establishes the possibility of adopting **violation prevention models** , in association with factors that mitigate liability, which may be certified by the authority.

SCOPE

The Bill regulates personal data processing carried out by individuals and legal entities, whether public or private, that are not governed by a special law.

The law does not apply to data processing carried out by social

media when the freedom to issue opinions and inform is being exercised, or to the processing carried out by individuals in relation to their personal activities.

PRINCIPLES

• **Principle of lawfulness:** personal data may only be processed in compliance with the law.
• **Principle of purpose:** data must be gathered for specific, explicit and lawful purposes; and data processing must be limited to comply with such purposes. Certain exceptions allow processing data for purposes other than those informed herein, such as the existence of a contractual relationship that justifies the processing, or the data originates from a publicly accessed source.
• **Principle of proportionality:** data that are processed must be limited to those as needed in connection with the purpose of the processing and must be kept only for as long as necessary to meet that purpose. A longer period of time requires obtaining a new legal authorization or consent from the data subject.
• **Principle of quality:** personal data must be accurate, complete, and current in connection with the processing purpose.
• **Principle of liability:** those processing data shall be legally liable for complying with the legal principles and obligations.
• **Principle of security:** proper standards of security must be guaranteed, protecting data against unauthorized processing, loss, filtration, damage or destruction, applying appropriate technical or organizational measures.
• **Principle of transparency and information:** data processing policies must be made permanently accessible in a precise, clear, and unequivocal manner, and free of charge.
• **Principle of confidentiality:** the controller and those accessing data must keep the data confidential. The controller must establish proper controls to maintain confidentiality. This duty subsists even after the relationship with the data subject has ended.

DATA SUBJECT'S RIGHTS, THE "ARCOP RIGHTS"

Personal, non-transferable and non-waivable, yet transmittable rights, may be exercised by the data subject's heirs.

• **Right of access:** request and obtain confirmation as to whether your personal data are being processed, by accessing: (i) data processed and their origin; (ii) the purpose of the processing; (iii) the recipients

to whom the data have been disclosed or transferred or are to be disclosed or transferred; and (iv) the period of time during which the data will be processed. The Bill provides for certain exceptions to this right.

• **Right of rectification:** right to request rectification when the data are inaccurate, out-of-date or incomplete.

• **Right of cancellation:** right to request the destruction of the data, in scenarios such as (i) when they are unnecessary with respect to the purposes for which they were collected; (ii) when the consent has been revoked; (iii) when the data were illegally obtained or processed by the controller; among others.

• **Right of opposition:** right to request that no specific processing be carried out, if (i) it affects the data subject's fundamental rights and freedoms; (ii) the processing is done exclusively for direct marketing purposes, unless there is a contract between the data subject and the controller; (iii) the data subject has deceased; or (iv) the processing is done with respect to data obtained from a publicly accessible source.

• **Right of portability:** right to obtain a copy of the personal data in a structured manner, in a generic and commonly used format, that allows them to be operated by different systems and communicated to another controller when (i) the data subject has provided his or her data directly to the controller; (ii) it is a relevant volume of data, processed in an automated manner; and (iii) the data subject has given consent for processing the data or consent is required for performing or complying with a contract.

Term for acting or commenting: The controller must act or comment within fifteen business days as of the date the petition was entered.

CONSENT AND OTHER SOURCES OF LAWFULNESS

Consent is treated as the general rule: processing is lawful if the data subject provides his or her consent.

Consent must be **given freely, must be informed and specific** with respect to the purpose, as well as **unequivocal** . To that end, the anachronistic requirement of obtaining purely written consent is eliminated.

Consent is **revocable** without expressing cause, but does not have retroactive effects.

Consent may not be the source of lawfulness if there is an

observable imbalance between the data subject's position and the controller's position. In such cases, the controller must resort to another legal source to justify the data processing.

OTHER SOURCES OF LAWFULNESS. Personal data processing is lawful, even without consent:

• If the data have been collected from a **publicly accessible source** and the processing thereof is related to the purposes for which they were provided;
• When the data relate to **economic, financial, banking or commercial obligations** ;
• If the processing is necessary for the execution or compliance with a **legal obligation** ;
• If the processing is necessary in order to **enter into or execute a contract** between the data subject and the controller.
• If the processing is necessary to satisfy the controller's or a third party's **legitimate interests** , provided that in doing so the data subject's rights and freedoms are not affected.
• If it is necessary for the **defense of a right in trial**

DATA TRANSFER

The bill does not provide a definition of data transfer (or assignment) but it is our understanding that a transfer takes place when the data are being transferred from one controller to another.

Data transfer is permitted when (i) the data subject consents to it and in order to fulfill the purposes of the processing; (ii) it is necessary for performing a contract to which the data subject is a party; (iii) there is a legitimate interest by the transferor or transferee; and (iv) the law provides it as such.

The transfer must be recorded in writing or through any suitable electronic means, and must meet certain requirements and acknowledgements. The transferee acquires the role of controller with respect to the transferred data, and the treatment thereof must comply with the objectives of the transfer contract. The transferor retains the capacity as controller with respect to the transactions it continues to carry out.

If a transfer of data is ascertained without the data subject's consent, where consent is required, the transfer will be null.

PROCESSING BY A PROCESSOR

Processing can be carried out by a processor, who may only do so according to the instructions of the controller. If the processor exceeds the limits when processing, it will be considered as a controller for all effects and purposes, liable for breaches and jointly and severally responsible for the damages it causes, notwithstanding any contractual liabilities it has toward its principal.

Data processing carried out by the processor shall be governed by the agreement it enters into with the controller, which shall have special provisions. The Agency shall publish the standard model agreements and contracts on its website.

The processor must comply with the obligations of confidentiality, data security and notification of breaches in the same way as the controller.

DATA CONTROLLER'S OBLIGATIONS.

Among the obligations of the data controller, we highlight the following:

1. **Duty of confidentiality** with respect to personal data, unless these originate from publicly accessed means, or they have been clearly made public by the data subject. The controller must adopt any measures necessary so that the dependents and employees under its responsibility comply with this same duty.
2. **Duty of information and transparency** to keep information permanently available to the public that relates to:

1. Its data processing policy, the date and version thereof;
2. The identification of the controller, its legal representatives, and its head of prevention, if any;
3. The technological means by which data subjects may notify the controller of their requests;
4. The types of data its processes and the characteristics thereof, the recipients to whom they are intended to be disclosed or transferred, the purposes of the processing it carries out, and the processing operations that are based on satisfying legitimate interests;
5. The security policies and measures to protect the data it manages;
6. The data subject's entitlement to request its ARCOP rights.

3. **Duty to adopt necessary security measures** , taking into consideration the state of the art, costs of their application, the nature

and purposes of the processing, the likelihood of risks and the gravity of the effects thereof in connection with the type of data. The measures must ensure the confidentiality, integrity, availability and resilience of the data processing systems. The controller has the burden of demonstrating the existence and operation of the security measures.
4. **Duty to report breaches of security measures** to the Personal Data Protection Agency, "without undue delays", when:

1. the breach causes the destruction, filtration, loss, alteration, unauthorized disclosure of or access to the personal data in question; or
2. there is a reasonable risk that such incidents will result in harm to the data subjects.

If the data that are the object of the breach are sensitive, or relate to economic, financial, banking or commercial obligations, the controller must report the breach to the data subjects, along with informing the measures that will be adopted to manage them and prevent future incidents.

SENSITIVE DATA AND SPECIAL DATA CATEGORIES

SENSITIVE DATA

The Bill defines sensitive data as those that reveal ethnic or racial origin, political, union or trade association affiliations, ideological or philosophical beliefs, health information, human biological profiles, biometric data, and information relating to sex lives, sexual orientation, and gender identity.

Sensitive data may only be processed with express consent given in writing or verbally or by an equivalent technological means.

Other bases of lawfulness, other than consent, for processing sensitive data:

• If the sensitive data has been made manifestly public by the data subject and the processing thereof is related to the purposes for which they were published;
• The processing is based on a legitimate interest, carried out by a non-profit legal entity, under certain conditions;
• If the processing is indispensable to safeguard the life, health or

integrity of the data subject or of another person, or the data subject is physically or legally precluded from granting his or her consent.
• If the processing is necessary for establishing, exercising or defending a right before the courts of justices.
• If the processing is necessary for exercising rights and compliance with the data controller's or the data subject's obligations, in a labor or social security context.
• Express legal authorization.

Other sensitive data with special regulation:

• **Health-related sensitive data** may only be processed when necessary for a medical diagnosis or treatment; there is a medical emergency; the degree of dependence or disability of a person must be qualified; the processing is indispensable in order to comply with a contract that requires that these types of data must be processed; for historical, statistical or scientific purposes (in certain circumstances); in order to exercise or defend a right before the courts; or when the purpose of the processing is provided for in the law.
• **Data relating to the human biological profile** , such as genetic data, proteomic or metabolic data, which may only be processed in order to perform a medical diagnosis, provide assistance in emergencies, conducting scientific, medical or epidemiological studies or research that aid or benefit human health, archeological or medical forensics research, or to exercise a right before the courts.
• Whomever processes **personal biometric data** – such as fingerprints, the iris, hand or facial features, and the voice – must provide the data subject with information on the biometric system being used, the specific purpose for collecting the data, the period during which the data will be used, and must comply with a regulation that regulates the implementation of biometric systems.

SPECIAL DATA

• **Personal data relating to children and adolescents** . As a general rule, data on children (men and women under the age of 14 years old) may only be processed with a view to their best interests and respecting their progressive independence, with the prior consent of their parents or guardians. Data on adolescents (men and women over the age of 14 years old and under the age of 18 years old) will be processed in the same way as data on adults, with the exception of their sensitive data, which must be authorized by their parents or

guardians.

• **Data processed for historical, statistical and scientific purposes, and for public interest-related studies or research .** There is a legitimate interest – as a source of lawfulness for processing other than consented processing – for this type of data processing.

• Controllers must adopt and demonstrate that they have fulfilled all quality and security measures necessary to ensure that data are being used exclusively for such purposes, adopting quality and security measures necessary to ensure that the data are being used exclusively for those purposes, in which case the controller may process the data for an indefinite amount of time.

• **Geo-localization data.** These follow the general rules on the lawfulness of any data processing. The data subject must also be clearly informed of the type of geo-localization data that will be processed and the duration of the processing, among other matters.

PROCESSING BY PUBLIC BODIES

The processing of personal data by public bodies and agencies is lawful when it is carried out for the performance of their legal functions, within the scope of their competence and jurisdiction, in which case no consent is required.

In addition to the general principles of the processing of personal data, the Bill identifies **coordination, efficiency, transparency and disclosure** as the guiding principles for the processing of data by public bodies.

The data subject may exercise the rights of access, rectification, opposition and cancellation before the public bodies. These requests will not be accepted if such requests prevent or hinder the performance of the compliance monitoring, investigative or penalizing functions of the public body, or if they affect a legal duty of secrecy or confidentiality.

The data subject may complain before the Personal Data Protection Agency when the public body has expressly or tacitly denied him or her a request to exercise any of the rights that the law recognizes with respect thereto.

The National Congress, the Judiciary, the Comptrollership General of the Republic, the Public Prosecutor's Office, the Constitutional Court, the Central Bank, the Electoral Service, and the Electoral Court, and

other special courts created by law, are excluded from the regulation, compliance monitoring, or oversight of the Personal Data Protection Agency.

PERSONAL DATA PROTECTION AGENCY

A Personal Data Protection Agency is created; a public, autonomous, decentralized, and technical body with legal personality and its own assets, subject to the oversight of the President of the Republic through the Ministry of Finance, and which is responsible for ensuring compliance with the regulations on the processing of personal data and the protection thereof. The Agency will be subject to the Public Senior Management System.

Domiciled in Santiago, the Agency's management and senior administration will fall under the responsibility of a Director, who will be the senior chief of the Agency, appointed by the President of the Republic with the Senate's agreement adopted by the absolute majority of the votes of the Senate's members in office.

The Agency shall be a body with broad powers, including:

• Administratively applying and interpreting the legal provisions and regulations whose compliance it is responsible for monitoring.
• Providing general instructions.
• Monitoring and enforcing compliance with the principles, rights and obligations of the law.
• Resolving requests and complaints raised by data subjects.
• Investigating and determining breaches by data controllers and exercising the penalizing powers in accordance with the law.
• Adopting the preventive or corrective measures provided by the law.
• Proposing to the President legal regulations and rules to ensure the protection of personal data and perfecting the regulation thereof.
• Developing dissemination and educational programs in connection with respecting and protecting the right to privacy.
• Managing the National Registry of Compliance and Sanctions.

A **National Registry of Compliance and Sanctions** is created, a public entity managed by the Agency, which will record sanctions and penalties imposed on data controllers, the breach prevention models, and the duly certified compliance programs. This registry will be kept and may be consulted electronically, and access thereto is free of charge.

INTERNATIONAL TRANSFER OF DATA

The Bill regulates for the first time the international transfer of personal data, establishing those cases where such type of data transfer will be considered lawful:

• When the transfer is made to a person subject to the legal system of a country that provides **adequate levels of protection** , understood as meaning that such protection meets the standards similar or higher than those of the data protection law. The Agency will determine the countries that have adequate levels of data protection, considering the elements provided for by the data protection law.
• When the transfer is covered by **contractual clauses** or other legal instruments executed between the controller that makes the transfer and the recipient of the data, establishing in such clauses the rights and guarantees of the data subjects, the obligations of the controllers, and the means of control.
• When the controller carrying out the transfer and the recipient of the data adopt a **binding and certified compliance or self-regulation model** in accordance with the legislation of each one's country.
• When there is **express consent by the data subject** to conduct a specific and determined international transfer of data.
• When the transfer entails specific **banking, financial or stock market transfers** .
• When the transfer is made **between companies or entities that belong to the same corporate group** , related companies or companies subject to a same controlling or parent company in the terms provided for in the Securities Market Law, provided that all of them operate under the same standards and policies regarding the processing of personal data. In such cases, the controller conducting the transfer shall assume liability for any violation of the **binding corporate policies and standards** committed by any of the members of its corporate group.
• Where necessary in order to enter into or execute an agreement between a data subject and the controller, or for the execution of pre-contractual measures adopted at the data subject's request.

The Agency will monitor international transfer operations and transactions, and may make recommendations, adopt conservative measures and, in qualified cases, temporarily suspend the transmission of data.

BREACHES AND PENALITIES

The Bill classifies breaches by **controllers that are private legal entities** into minor, serious and gross, and sets forth penalties comprising **fines that range between 1 and 5,000 UTM** (approximately from CLP 47,300 to CLP 236,500,000, as at April 2018).

Criteria are established in order to determine the amount of the fine, which includes some of the following **mitigating circumstances of liability** :

• There are unilateral actions for redress and reparation or remedy agreements agreed between the controller and the affected data subject.
• The offender's cooperation in the administrative investigation.
• The absence of previous penalties.
• Self-reporting to the Agency, where the offender must notify the measures adopted to cease the breach.
• The diligent performance of their management and supervisions duties with respect to protecting the personal data subject to the processing, which will be verified by the Agency's certification for the prevention models and compliance programs that meet the legal requirements.

The Bill also establishes **aggravating circumstances of liability** :

• Recidivism: when the controller has been penalized on two or more occasions in that last thirty months.
• The continuing nature of the breach.
• Having placed the safety of data subjects at risk.

Sanction suspending data processing activities. If fines are imposed for gross breaches repeated over a 24-month period, the Agency may provide for the suspension of the data processing operations carried out by the controller for up to 30 days, extendable indefinitely for periods of 30 days if the controller fails to comply with the provisions of the suspension decision.

Statute of limitations for actions to penalize breaches: Three years as of the occurrence of the event.

Action for damages. As a general rule, the controller must indemnify the pecuniary and non-pecuniary damages the violation of the law causes to the data subject. This action is processed in accordance with summary proceedings, and is lodged only once the decision that favorably accepts the claim filed against the Agency is made final and enforceable. The statute of limitations of civil actions expires in three years as of the moment the administrative decision or judicial judgment, as the case may be, is made final and enforceable.

PROCEDURES

• **Administrative procedure for the protection of rights:** This action is exercised by the data subject before the Agency, and is admissible when the controller has denied the data subject a request to exercise any of the rights to which he or she is entitled as recognized by the law with respect thereto.
• **Administrative procedure for a violation of the law:** This action is ordered by the Agency as a result of a compliance monitoring process or as a result of a complaint filed by a data subject, in order to determine the offense for breaches of the principles, rights and obligations provided for by the law.
• **Judicial complaint procedure:** Persons aggrieved by a decision issued by the Agency may lodge a complaint for unlawfulness before the Appeals Court with jurisdiction, within 15 days as of the notification of the challenged decision.

BREACH PREVENTION MODEL

The Bill establishes the obligation providing that data controllers (public and private) must adopt mechanisms to prevent the commission of breaches; the possibility of adopting a breach prevention model, which must contain elements such as the appointment of a prevention officer; and also establishes the obligation of a compliance program that identifies certain elements such as the types of data being processed, operation protocols, and reporting mechanisms.

The Agency must certify that the breach prevention model and the compliance program meet the requirements provided in the law and in its regulations, and shall monitor compliance therewith.

Data controllers may extenuate their liability if they demonstrate that they have unequivocally fulfilled their duties of management and

supervision with respect to protecting the personal data under their responsibility. This will be considered to have occurred if the controller adopted and implemented a breach prevention model certified by the Personal Data Protection Agency. These certificates will be valid for three years, and under certain circumstances may be revoked and invalidated.

The Bill orders the issuance of regulations that establish the requirements, modalities and procedures for implementing, certifying, registering and supervising the breach prevention models and the compliance programs.

The bill will enter into force within **one year** as of its publication in the Official Gazette.

Databases created prior to the date on which the law enters into force must be adapted and modified within **two years** ; notwithstanding that data subjects may exercise their rights vis-à-vis the controller as of the law's entry into force.

Authors: Guillermo Carey