COLOMBIA’S NEW DATA PROTECTION LAW.

SUMMARY

The following is a brief summary of the new data protection law that will be soon enacted by the Colombian President. This summary does not constitute a legal opinion nor can be construed or interpreted as one.

Please note that according to the Colombian Constitution, a mandatory review of the Bill was performed by the Colombian Constitutional Court. As a consequence thereof, the Court upheld the Bill, except for articles 27, 29, 30 and 31. The ruling has not been published yet. Consequently, the content of this summary could be subject to updates or modifications.

I. Scope

The new Statutory Law (the “New Law” or the “New Regulation”) will be soon enacted as a comprehensive regulation on data protection and as complement to the regulation already provided by Statutory Law 1266/08.

The New Law applies to all matters related with the fundamental right to acknowledge, update and rectify personal information contained in databases as provided by Art. 15 of the Colombian Constitution.

Except for the matters previously regulated under Law 1266/08 (mainly financial, credit, banking and some commercial matters), the New Regulation will apply to all data collection and processing within the Colombian territory or whenever the controller or processor is obliged to apply Colombian law as provided under international treaties.

The new regulation does not apply to: (i) strictly personal databases; (ii) databases containing information regarding a) national security and defense, b) money laundering or financing of terrorism activities, and c) government intelligence and counterintelligence; (iii) databases and files containing journalistic and editorial information; and (iv) information regulated by Law 1266/08 and Law 79/93 (population census).

II. Definitions and Principles

- Definitions:

  a. Authorization: Previous, express and informed consent given by the data owner.
b. Database: organized set of personal data.

c. Personal data: Any information that can be linked or associated with one or various, natural and determined or determinable persons.

d. Data processor: Legal or natural person that processes personal data on behalf of the data controller.

e. Data controller: Legal or natural person that has the capacity of controlling databases and/or data processors.

f. Data Owner: Owner of the personal information or data.

g. Processing: Any operation related to the collection, storage, use, transfer or suppression of data.

- **Principles:** Must be applied whenever the law is interpreted and enforced.

  a. Legality: Data processing is a regulated activity that must be subject to the provisions established under the applicable legislation and administrative regulation.

  b. Finality: Data processing must always pursue a legal and legitimate purpose that must be previous and dully informed to the Data Owner.

  c. Liberty: Data treatment can only be carried out with the prior, express, and informed consent of the Data Owner.

  d. Accuracy or quality: Processing of personal data must be accurate, sufficiently complete, up to date, verifiable and understandable. It is expressly prohibited to process partial or incomplete data or information that may mislead users.

  e. Transparency: Data Controllers and Processors must guarantee Data Owners full access to their personal information contained in the data bases.

  f. Restricted access and circulation: The processing of data must be subject to the limits derived from the nature of personal data. Personal data, except for public information, cannot be available on internet or any mass media instrument, unless access can be technically controlled to provide information only to the Data Owner or authorized third parties.

  g. Security: Data Controllers and Processors must use adequate technical, human and administrative measures in order to prevent
deletion, modifications, breaches or unauthorized access of personal data.

h. Confidentiality: all persons involved in data processing must guarantee absolute confidentiality regarding information contained in databases.

III. Special data categories

The new regulation establishes two special data categories that demand special treatment upon processing and transfer of personal data:

a. Sensible data: The kind of data that affects the most private sphere of the Data Owner, such as, religion, political orientation, gender and sex orientation, trade-union memberships, human rights and/or social organizations, among others.

As a general rule it is prohibited the processing of sensible data, unless (i) the Data Owner has expressly given its consent, (ii) processing is absolutely necessary to protect vital interests of the Data Owner whenever he/she is not capable of providing its consent, (iii) when the processing is performed by foundations, NGO’s, or other similar organizations that have, amongst others, a political, philosophical, religious purpose (the processing of data in this event must be limited in all cases to members of the organization), (iv) whenever the information is of public knowledge and (v) for historical, statistical or scientific purposes for which the identity of the data owner must be suppressed.

b. Minors and teenagers data: processing of data that belongs to minors or teenagers is prohibited unless said data is deemed as public data.

IV. Data processing requirements

a. Data Owner rights: Data Owner are entitled inter alia to (i) acknowledge, update and rectify his/hers personal information; (ii) request copy of the authorization/consent given to the Data Processor; (iii) receive from the Data Controller or Processor information regarding the usage of the personal data, (iv) file complaints before the data protection authority (the Superintendency of Industry and Commerce); (v) revoke the authorization/consent and request the suppression of any personal data whenever data processing does not comply with the provisions of the Constitution and the law; and (vi) have free access to his/hers personal data.

b. Authorization: It is not necessary whenever the data is required (i) by administrative or judicial authorities for the performance of legal
duties; (ii) as public information; (iii) for sanitary or medical urgency; and (iv) for historical, statistical or scientific purposes.

c. **Data supply:** Data must be supplied by any physical or electronic means and must match the information stored in the database.

d. **Consent requirements:** In order to obtain the Data Owner’s authorization, the Data Controller must report to the Data Owner in a clear and express manner *inter alia* (i) the treatment that is going to be given to the Data Owner’s data; (ii) the Data Owner’s rights, and (iii) the identity of the controller and its contact details.

e. **Persons to whom information can be supplied:** the information that complies with the conditions provided by the new regulation may only be supplied to: (i) Data Owners, their successors in title or legal representative; (ii) public or administrative entities upon performance of their legal duties or through judicial order and; (iii) third parties expressly authorized by the Data Owner.

V. **Duties of Data Controllers and Data Processors**

- **Data controllers** must: (i) guarantee that the Data Owner is able to effectively to exercise his/hers right to Habeas Data; (ii) request and store a copy of the authorization granted by the Data Owner; (iii) inform the data owner about the finality or purpose for which the data is collected and processed; (iv) guarantee data security conditions; and (v) guarantee that the information supplied is accurate, truthful, complete, updated, verifiable and understandable.

- **Data processors** shall: (i) guarantee that the data owner is able to effectively to exercise his/hers right to Habeas Data; (ii) store data in a safe and secure environment; (iii) update data on a constant basis, in particular data updates provided by the Data Controller; and (iv) attend and reply to the consultations and complaints raised by Data Owners.

VI. **Fines and sanctions**

In case of breach of applicable regulation, the DPA can impose fines (up to 2000 Colombian Minimum Wages) to Data Controllers and Data Processors or order the cancellation of the activities performed by processors or controllers.
The new regulation provides for a public directory that contains a registry of all the operating databases in Colombia. This registry will be administered by the DPA.

VII. International data transfer

According to the New Regulation, cross-border transfer of data can only be performed to a country with a similar level of data protection as the one provided under Colombian law.

In principle the aforementioned shall not be deemed applicable if (i) data Owner grants express authorization; (ii) data transfer is related with medical information exchange whenever it is required for public sanitary measures or health matters related to the Data Owner; (iii) data transfer involves stock and banking transfers regulated by special legal provisions; (iv) data transfer is authorized by international treaties; (v) the transfer is necessary for the performance of a contract in which the Data Owner is a party to; (vi) the transfer of data pursues the protection of public interests.

VIII. Transitional Regime

The New Law grants a 6-month term for all persons and companies to perform the necessary personal or corporate actions and procedures in order to observe the new regulation.