Data. Protection. Adding Value.

Data Protection Laws - Colombia

Legislation

The Statutory Law 1581 of 2012, known as the Personal Data Protection Law, recognizes and protects the right of all individuals to know, update, and rectify the information collected about them in databases or files susceptible to processing by public or private entities. This right is supported by Sections 15 and 20 of the Colombian Constitution, which recognize privacy and data rectification as fundamental rights.

Scope: This law applies:

- To the processing of personal data carried out within Colombian territory.
- When the data controller not established in Colombia is subject to Colombian legislation under international rules or treaties.

Sectoral Law Carve-Outs/Exemptions: The Law 1581 of 2012 will not apply to the following databases:

- Databases maintained in an exclusively personal or domestic scope.
- Databases related to national security and defense, as well as the prevention of money laundering and the financing of terrorism.
- Databases regulated by Law 1266 of 2008 (financial information) and Law 79 of 1993 (population censuses).
- Databases of journalistic information and editorial content.

Risk Level: High

Enforcement

Enforcement (Fines, Criminal Penalties): The SIC may impose the following sanctions on Data Controllers and Data Processors:

- Fines: Fines of up to two thousand (2,000) minimum monthly wages.
- Suspension of activities: Suspension of activities related to data processing for up to six (6) months.
- Temporary closure: Temporary closure of operations related to data processing.
- Immediate and definitive closure: Immediate and definitive closure of operations involving the processing of sensitive data.

Remedies for Individuals: Submit a complaint to the data controller, and if the complaint is not resolved, go directly to the

Supervisory Authority

Supervisory Authority:
The Superintendence of Industry and Commerce (SIC), through its Delegation for the Protection of Personal Data, is responsible for supervising and guaranteeing respect for the rights established in Law 1581 of 2012 during the processing of data.

Registration/Approval Requirements: In processing, the prior and informed authorization of the Owner is required, which must be obtained by any means that may be subject to subsequent consultation. The authorization of the owner will not be necessary when they are: a) required by judicial order b) data of a public nature c) cases of medical emergency, among others.

Data Processing

Legal Basis for Processing: Previous and informed authorization from the data owner is required in order to process it.
Sensitive Personal Data: Processing sensitive personal data is prohibited, unless:

- there's authorization from the owner.
- it's necessary to safeguard the vital interest of the owner.
- it's being processed by foundations or ONGs in order to fulfil their legitimate activities.
- it's necessary for the legal defense of the owner in court.
- has a historical, scientific or statistical purpose..

Other Restrictions on Processing: Processing personal data of children and adolescents is prohibited, with exception of data of public nature.

General Data Privacy Principles

- **Principle of legality:** Data processing must comply with what is established in the law.
- **Principle of purpose:** Data processing must have a legitimate purpose, informed to the data subject.
- **Principle of freedom:** Data processing requires the prior, express, and informed consent of the data subject.
- **Principle of truthfulness or quality:** Data must be truthful, complete, accurate, and up-to-date.
- **Principle of transparency:** The data subject has the right to know the existence of data concerning them.
- **Principle of access and restricted circulation:** Processing must be limited to authorized persons.
- **Principle of security:** Measures must be implemented to protect data against unauthorized access.
- **Principle of confidentiality:** Individuals involved in the processing of personal data must guarantee the confidentiality of the information.

Transparency Requirements

In the processing, the data subject's right to obtain from the data controller or processor, at any time and without restrictions, information about the existence of data concerning them must be guaranteed.

pwc

Individual Rights

Under Section 8 of Law 1581 of 2012, the data subject has the following rights regarding their Personal Data:

- Know, update, and rectify their personal data with respect to the Data Controllers or Data Processors.
- Request proof of the authorization granted to the Data Controller, except when expressly exempted as a requirement for processing, in accordance with Section 10 of Law 1581 of 2012.
- Be informed by the Data Controller or Data Processor, upon request, regarding the use that has been made of their personal data.
- Lodge complaints with the SIC for violations of Law 1581 of 2012 and other regulations that modify, add to, or complement it.
- Revoke the authorization and/or request the deletion of data when the processing does not respect constitutional and legal principles, rights, and guarantees.
- Access their personal data that has been subject to processing free of charge.

Information Security

Regarding information security, the data controller has the duty to maintain the information under the necessary security conditions to prevent its loss or alteration.

- **Principle of security:** Measures must be implemented to protect data against unauthorized access.

In the event of any incident, the competent authority must be immediately notified, ensuring compliance with Section 17 of Law 1581 of 2012, duties of data controllers regarding personal data processing.

Duties of Data Controllers and/or Processors:

Within the framework of compliance, both data controllers and processors must primarily fulfill the following duties:

- Inform and ensure the exercise of the rights of data subjects.
- Process and provide timely responses to inquiries, requests, and complaints.
- Use the data collected for the purposes that have been disclosed.
- Only process data that is authorized or does not require authorization.
- Implement and respect the security and privacy conditions of the information.
- Comply with instructions and requirements issued by the administrative authority.

Authorization & RNBD

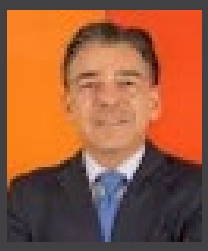
Authorization: Request authorization for the use of collecting personal data, which should include the identification of the data controller, as well as the company or companies (national and foreign) that will have access to such information, the purposes of its use, the rights of the data subjects, the channels to exercise them, and how to access the privacy policy.

National Database Registry (RNBD): The RNBD is the public directory of databases subject to processing that operate in the country. Companies or entities that meet the parameters established in Decree 90 of 2018 are obliged to register their databases with the RNBD managed by the SIC.

Other/To Watch

The data controller undertakes to have a personal data policy in physical and/or electronic format, which must be made known to data subjects. They must also have one or more internal procedure manuals regarding inquiries, complaints, and security incidents, written in clear and simple language.

Let's connect to discuss how we can help:



Wilson Herrera
Partner
TLS
PwC Legal Colombia
+57 317 6670668
wilson.herrera@pwc.com

Juan Manuel Duarte
Manager
TLS
PwC Legal Colombia
+57 300 7915264
duarte.juan@pwc.com