DATA PROTECTION LAWS OF THE WORLD

Colombia

COLOMBIA

Last modified 28 January 2024

LAW

Colombia recognizes two fundamental personal data rights under Articles 15 and 20 of its Constitution: (1) the right to privacy and (2) the right to data rectification. Personal data processing is further regulated by two statutory laws and several decrees that set out data protection obligations.

Statutory Law 1266 of 2008 (Law 1266) regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad. Law 1266 defines general terms on habeas data and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data.

Law 1266 defines the terms Data Subject, Data Source, User of Data and Data Operator, as follows:

- ‘Data Subject’ means the owner of the information;
- ‘Data Source’ means a person or entity who receives or collects the information in the context of a commercial relationship with the Data Subject and shares this information with the Data Operator;
- ‘User of Data’ means a person or entity who accesses databases and uses the information gathered by the Data Operator;
- ‘Data Operator’ means a person who manages a database with information provided by the Data Sources and shares it with Users of Data, under the rules provided by Law 1266. The most common example of a Data Operators is a Credit Bureau.

Law 1266 provides the applicable rules and conditions for Data Sources to share information with Data Operators and for such Data Operator to manage and share the information with Users of Data. Notwithstanding this, the Law privileges processing for purposes of managing financial, credit, commercial and services information, considering that this benefits the financial and credit activity as a public interest activity.

Law 1266 was amended by Law 2157 of 2021. The main modifications introduced by Law 2157 are the following:

- Data whose content refers to the time of default of an individual or a company, or data that refers to a lack of compliance with monetary obligations, shall be erased immediately or as promptly as possible. This erasure requirement applies mainly to small companies, small farmers, armed conflict victims, young people, women from rural areas, and other debtors who are in special situations, with the specificities foreseen in the Law.
- The obligation to update credit scores was created, provided that any negative data is erased.
- The Law established that the frequent consultation of a person’s credit history should not be a factor for lowering their credit rating.
- Claims and requests concerning the processing of financial data must be resolved within fifteen (15) working days from the date of receipt of the communication. If a prompt resolution is not given within this timeframe, the request is presumed accepted for all legal purposes.
- Financial data, credit records, and commercial information may not be used in making employment decisions.

- The Law introduced the principle of accountability for the processing of financial information. This update implies the Data Source and the Data Operator should adopt internal policies to guarantee the safety and confidentiality of the information.

Furthermore, Statutory Law 1581 of 2012 (Law 1581) regulates all personal data processing, as well as databases. Law 1581 defines special categories of personal data, including sensitive data and data collected from minors. Under the law a ‘Data Controller’ is a legal or natural person responsible for data treatment, or processing, and a ‘Data Processor’ is a legal or natural person in charge of personal data processing. The Data Controller creates databases on its own or in association with others, while the Data Processor processes personal data on behalf of the Data Controller. Nevertheless, an entity may be regarded as both Controller and Processor of personal data.

The law further regulates the obtention of authorization to treat personal data and the procedures for data processing. Moreover, the law creates the National Register of Data Bases (NRDB).

Law 1581 is applicable to all data collection and processing in Colombia, except data regulated under Law 1266 and certain other types of data or regulated industries. The law is further applicable in any case where a data processor or controller is required to apply Colombian law under international treaties.

Law 1581 does not regulate:

- Databases regulated under Law 1266;
- Personal or domestic databases;
- Databases aimed to protect and guarantee national security, prevent money laundering and terrorism financing;
- Intelligence and counter-intelligence agency databases;
- Databases with journalistic information and editorial content; and
- Databases regulated under Law 79 of 1993 (on population census).

Law 1581 further requires Data Controllers and Data Processors to guarantee that personal data: is maintained pursuant to strict security measures and confidentiality standards, will not be modified or disclosed without the data subject’s consent, and will only be used for purposes identified in a privacy policy or notice.

Decree 1377 of 2013 (Decree 1377), is a piece of secondary regulation related to Law 1581 which outlines requirements for personal and domestic databases regarding authorization of personal data usage and recollection, limitations to data processing, cross-border transfer of data bases and privacy warnings, among others. This Decree also requires controllers and processors to adopt a privacy policy and privacy notice.

Decree 886 of 2014 (Decree 886) and Decree 090 of 2018 (Decree 090) issued by the Ministry of Commerce, Industry and Tourism, regulate the National Register of Data Bases and sets deadlines for registration of existing data bases in Colombia.

Lastly, Title V of the Sole Circular issued by the Superintendence of Industry and Commerce provides additional guidelines regarding the following matters: (i) the processing of financial data, credit records and commercial information; (ii) the National Register of Data Bases and (iii) International Data Transfers.

DEFINITIONS

The Colombian data protection regime distinguishes between personal data and a sub-category of sensitive personal data, depending on the information and the harmful effects caused by its unlawful use. Law 1266 and Law 1581 contain particular rules related to sensitive personal data.

Definition of personal data

Under Law 1266, personal data is defined as any information related to or that may be associated with one or several determined or determinable natural or legal persons. Personal data may also be regarded as public, private or semi-private data. Public data is available to the public based on a legal or constitutional mandate. Private or semi-private data is data that does not have a public purpose, is intimate in nature and the disclosure of which concerns only the data subject.

Under Law 1581, personal data is defined as any information related to, or that may be related to, one or several determined or determinable individuals, meaning natural persons only.

Definition of sensitive personal data

Under Law 1266, sensitive personal data is defined as data that due to its sensitivity is only relevant to its owner.

Under Law 1581, sensitive personal data is any data that affects its owner’s intimacy or whose improper use might cause discrimination. Data that reveals any of the below information is considered sensitive data and its processing is prohibited by law:

- Ethnic or racial origin
- Political orientation
- Religious or philosophic convictions
- Membership in labor unions, human right groups or social organizations
- Membership in any group that promotes any political interest or that promotes the rights of opposition parties
- Information regarding health and sexual life, and
- Biometrics

Sensitive personal data shall only be processed:

- With the Data Subject's special and specific consent
- If necessary to preserve the data subject’s life, or a vital interest and the Data Subject is physically or legally unable to provide consent
- If used for a legitimate activity and with all necessary security measures, by an NGO, an association or any kind of nonprofit entity, in which case, the entity will need the Data Subject's consent to provide the sensitve personal data to third parties
- If such data is related to or fundamental to exercising a right in the context of a trial or any judicial procedure, or
- If such data has a historic, statistical or scientific purpose, in which case the Data Subject's identity may not be disclosed

NATIONAL DATA PROTECTION AUTHORITY

According to Law 1266, there are two different authorities on data protection and data privacy matters. The first of them, which acts as a general authority, is the Superintendent of Industry and Commerce (SIC). The second authority is the Superintendence of Finance (SOF), which acts as a supervisor of financial institutions, credit bureaus and other entities that manage financial data or credit records and verifies the enforcement of Law 1266.

Nevertheless, under Law 1581, the SIC is the highest authority regarding personal data protection and data privacy. It is empowered to investigate and impose penalties on companies for the inappropriate collection, storage, usage, transfer and elimination of personal data.

REGISTRATION

Law 1581 created the National Register of Data Bases (NRDB). Databases that store personal data and whose automated or manual processing is carried out by a natural or legal person, whether public or private in nature, in the Colombian territory or abroad, shall be registered in the NRDB. Database registration is also required if Colombian law applies to the data controller or data processor under an International Law or Treaty. Registration is mandatory for data controllers that are either of the following:

- Companies or nonprofit entities that have total assets valued above 100,000 Tax Value Units (TVU), meaning COP 3.800.400.000 million (USD 950.100)[1]
- Legal persons of public nature

Decree 866 states that each data controller shall register each one of its databases, independently and must distinguish between manual and automatized databases. In addition, in order to register each database, the data controller or data processor shall provide the following information:

- Identification information of the data controller, such as: business name, tax identification number, location and contact information
- Identification details of the data processor, such as: business name, tax identification number, location and contact information
- Contact channels to grant data subjects rights
- Name and purpose of the database
- Form of processing (manual / automatized)
- Security standards
- Privacy policy

All data bases were required to register by January 31, 2019. Any new data base(s) shall be registered within the 2 months following its creation.

Any substantial change to any of the abovementioned items, shall be updated in the National Registry of Data Bases. For this purpose, substantial changes are considered as any changes that are made in regards to the purposes of the databases, the data processors, the channels to process any claim or request from the data subject, the class or type of personal data, the security measures implemented, the data privacy policy and/or the international transfer or transmission of personal data.

Such updates shall be made:

i. Within the 10 first days of the month in which the substantial change was made,

and

ii. Yearly (between January 2 and March 31 of each year).

Moreover, through the National Register of Data Bases, data controllers shall inform of the following:

i. Any claim submitted by a data subject to the data controller and/or data processor, within each semester of the year. This information shall be registered within the first 15 business days of February and August of each year with the information of the previous semester.
ii. Any breaches of registered data bases. Such report shall be submitted within the 15 business days following the day on which the data controller had knowledge of the data breach.

Footnote 1: Based on the Tax Value Unit for 2022 (COP $38.004 (approximately USD 9.5)). The Tax Value Unit is updated yearly by the Colombian tax authority.

DATA PROTECTION OFFICERS

There is no requirement to appoint a formal data protection officer in Colombia. However, companies are required to appoint either a specific person, or a designated group within the company to be in charge of personal data matters, specifically the handeling of Data Subject rights and privacy request .

COLLECTION & PROCESSING

The processing of financial data, credit records and commercial information, collected in Colombia or abroad, does not require authorization from the Data Subject. However, this information may only be disclosed to:

- The Data Subject or authorized third parties, pursuant to the procedure established by law
- The Users of the Data
- Any judicial or jurisdictional authority upon request
- Any control or administrative authority, when an investigation is ongoing

- Data processors, with the Data Subject’s authorization, or when no authorization is needed , and the database aims for the same objective or involves an activity that may cover the purpose of the disclosing data processor

On the contrary, Law 1581, requires the authorization of the Data Subject for the data controller to process private and semi-private personal data. For the authorization to be valid it must be obtained prior to the data processing and must be "informed", meaning that the data subject must have been made aware of the exact purposes for which the data is being processed. Decree 1377 requires the following:

- Personal data shall only be collected and processed in accordance with the purposes authorized by the Data Subject.
- Such authorization may be obtained by any means, provided that it allows subsequent consultation.

Authorization is not required when:

- A public or administrative entity demands the information through a judicial order or exercising its legal duties.
- It is public data.
- A medical or sanitary urgency requires the processing of personal data.
- The data processing is authorized by law for historical, statistical or scientific purposes.
- The data is related to people’s birth certificates.

Regarding sensitive personal data, Section 6 of Decree 1377 states that the data controller shall do the following:

- Expressly inform the Data Subject that he or she is not compelled to provide sensitive personal data
- Expressly identify what data to be collected and processed is sensitive and
- Obtain the Data Subject's express consent prior to the processing of their sensitive personal data

In any case, silence is not considered a reasonable means of obtaining authorization for personal data or sensitive personal data processing.

Furthermore, when collecting personal data of children, both the data controller and the data processor shall ensure that personal data processed serves and respects the children’s superior interests and guarantees their fundamental rights. For these purposes, the child's legal representative (parent or guardian) must authorize the processing of their child’s personal data.

Privacy policy and privacy notice

Decree 1377 establishes the obligation for data controllers to develop a privacy policy that governs personal data processing and ensures regulatory compliance. For this reason, privacy policies are mandatory for all data controllers and shall be clearly written; Spanish is recommended. Finally, according to the Decree 1377, the minimum requirements for the privacy policy are:

- Name, address, email and phone number of the data controller
- Processes and handling of data and the purpose of such processing
- Rights of the Data Subject
- Individual or department within the data controller that is responsible for the attention to requests, consultations and claims to update, rectify or suppress data and to revoke authorization
- Procedure to exercise the abovementioned rights, and
- Date of creation and effective date

The privacy notice is a verbal or written communication by the data controller, addressed to the data subject, for processing her /his personal data. In this communication, the data subject is informed about the privacy policies of the data controller, the manner to access them and the purposes of the treatment.

TRANSFER

Per Law 1581, the transfer of personal data occurs when the data controller or the data processor located in Colombia sends the personal data to a recipient, in Colombia or abroad, who is responsible for the personal data, *ie*, a data controller.

Cross-border data transfers are prohibited unless the country where the data will be transferred to provides at least equivalent data privacy and protection standards and adequate safeguards to those provided by Colombian law. In this regard, adequate levels of data protection will be determined in accordance with the standards set by the SIC.

This restriction does not apply in the following cases:

- If the Data Subject expressly consented to the cross-border transfer of data
- Exchange of medical data
- Bank or stock transfers
- Transfers agreed to under international treaties to which the Colombia is a party
- Transfers necessary for the performance of a contract between the Data Subject and the controller, or for the implementation of pre-contractual measures, provided the data owner consented, and
- Transfers legally required in order to safeguard the public interest

Therefore, the data controller requires the authorization of the Data Subject for transferring the personal data abroad, unless such transfer is to one of the following countries which, according to the SIC, meet the standard of data protection and security levels.

Authorized countries for international transfer of personal data

- Albania
- Argentina
- Austria
- Belgium
- Bulgaria
- Canada
- Costa Rica
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungry
- Iceland
- Ireland
- Italy
- Japan
- Latvia
- Lithuania
- Luxembourg
- Malta
- Mexico
- Netherlands
- New Zealand
- Norway
- Perú
- Poland
- Portugal
- Republic of Korea

- Romania
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United States
- United Kingdom
- Uruguay

The SIC also considers that personal data can be transferred to any country regarding which the European Commission considers to meets its standard for levels of protection.

Transfer of personal data

The transfer of personal data takes place when the data controller provides personal data to a data processor, in Colombia or abroad, in order to allow the data processor to process the personal data on behalf of the data controller. The data subject’s consent is required for the transfer of data, unless an adequate data transfer agreement between the data processor and the data controller is in place.

In this regard, Decree 1377 requires that the aforementioned agreement include the following clauses:

1. The extent and limitations of the data treatment
2. The activities that the data processor will perform on behalf of the data controller, and
3. The obligations the data processor has to data subjects and the data controller

The data processor has three additional obligations when processing personal data:

- Process data according to the legal principles established in Colombian law
- Guarantee the safety and security of the databases
- Maintain strict confidentiality of the personal data

A data controller transferring data to a data processor must identify the data processor in the National Database Register for each database transferred. Finally, the data processor must process the personal data in accordance with the data controller’s privacy policy and the authorization given by the data subject.

SECURITY

Data controllers have the legal duty of guaranteeing that the information under their control is kept under strict security measures. For this reason, data controllers shall ensure that such information will not be manipulated or modified without the Data Subject's consent . For this purpose, the data controller shall develop an information security policy that prevents the unauthorized access, the damage or loss of information, including personal data.

BREACH NOTIFICATION

In accordance with Chapter 2, Title V of the Sole Circular issued by the SIC, a data breach refers to the violation of security codes or to the loss and unauthorized access of data subjects’ information held in a database managed by data controllers or data processors.

Under section 17. and section 18. of Law 1581, both the data controller and the data processor have a duty to notify the authority (SIC) in case of a breach of security, security risk, or a risk for data administration. Such notification shall be made no later than fifteen (15) business days from the date on which the data breach was detected.

Lastly, the Colombian data protection regime does not provide a threshold for data breach notifications. Hence, if there is a violation to the security codes or a risk in the management of data subjects’ information, data controllers and data processors must notify the breach.

ENFORCEMENT

Since privacy and proper maintenance of personal data are fundamental constitutional rights in Colombia, every citizen is entitled to pursue protection before any Colombian judge, via constitutional action. Any judge may order a private or public entity to modify, rectify, secure or delete personal data if it is kept under conditions that violate constitutional rights. Constitutional actions can take up to ten days to be resolved and an order issued and failure to comply may result in imprisonment of the legal representative of the violating entity.

The Criminal Code of Colombia sets out in section 269F that anyone who, without authorization, seeking personal or third party gain, obtains, compiles, subtracts, offers, sells, interchanges, sends, purchases, intercepts, divulges, modifies or employs personal codes or data contained in databases or similar platforms, will be punishable by 48 to 96 months of prison, and a fine of approximately USD 26,700 to USD 267,000.

Finally, since SIC is an administrative and jurisdictional authority, it is allowed to investigate (as mentioned above), request information, initiate actions against private entities, and impose fines up to approximately USD 534,000, and order or obtain temporary or permanent foreclosure of the company, entity or business.

ELECTRONIC MARKETING

Law 527 of 1999 (Law 527) regulates e-commerce and electronic marketing, but there is no specific regulation regarding data privacy on electronic marketing. In any case, the Data Subject's consent is required for marketing, whether electronic or not and the processing of any personal data for this purpose shall be in accordance with Law 1581.

ONLINE PRIVACY

There is no specific regulation regarding online processing of personal data. Thus, online privacy and data processing is governed by Law 1581.

Personal data must not be available online unless there are adequate security measures to ensure that access by any unauthorized user is restricted.

Collection and use of data collected through cookies or similar online tracking tools is prohibited unless the Data Subject has provided consent. Such consent may be obtained by a pop-up informing the user about the company's privacy policy and ways for the Data Subject's to review, manage or disable cookies.

KEY CONTACTS

Maria Claudia Martinez Beltrán
Partner
DLA Piper Martinez Beltrán
T +57 3174720
mcmartinez@dlapipermb.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.