大成 DENTONS CARDENAS & CARDENAS

Data Protection

Colombia

Luz Helena Adarve
Partner
D +57 3137800 ext. 232
luz.adarve@dentons.com

Juanita Acosta
Partner
D +57 3137800 ext. 266
juanita.acosta@dentons.com

Introduction

Following the experience gained by multiple countries in the area of privacy and personal data protection, in 2012 Colombia established a general data protection regulation that must be observed by all individuals and entities that process personal data in Colombia.

In particular, general provisions were established through Law 1581 of 2012, which contains a truly broad scope considering that it applies to all data processing carried out in Colombia, which are not within the exceptions established by the law. In addition, Colombian legislation is not limited to the data processing carried out in the private sector, but is equally applicable to the processing performed by entities of the public sector.

In Colombia, the data processing includes any operation carried out on personal data, including the collection, storage, use, deletion, update, transmission and transfer of the information. Therefore, the performance of any of the activities listed above that is not based on an exception established by the law automatically implies the application of Colombian privacy law.

The following is an overview of the obligations deriving from Colombian law, including a regulatory project on the subject that is currently under discussion.

Main definitions and actors

In order to properly understand the obligations established in Colombian privacy law, it is necessary to comprehend the scope and meaning of various terms that are transversal to the legislation, such as personal data, processing, authorization, data subject, data controller and data processor.

Personal data

Is any information linked or that may be associated directly or indirectly to one or more individuals.

Authorization

Is the prior, express and informed consent given by the data subjects in order to carry out the processing of their personal data. Under Colombian privacy law, the authorization constitutes a fundamental pillar as well as the general rule to legitimize the processing of personal data.

Data processing

As previously established, the data processing includes any operation carried out on personal data, such as the collection, storage, use, circulation, transmission, transfer and suppression of information, among others.

Data subject

Is the individual whose personal data are subject to processing. The data subjects, altogether with the data controllers and the data processors, are the main actors defined by Colombian privacy law.

Data controller

It is the natural or legal person, regardless of its nature, that by itself or in association with others, decides on the data processing. Generally speaking, companies are controllers over the personal data of their employees, suppliers and customers.

Data processor

It is the natural or legal person, regardless of its nature, that by itself or in association with others, performs the processing of personal data on behalf of a data controller. For example, external advisors are generally processors regarding the personal information that their clients send to them for advice purposes.

Main obligations on data controllers and data processors

The obligations established by Colombian privacy law depend on the quality of the individual or entity that processes the personal data, that is, if they are controllers or processors. While there are similar or identical obligations for both actors, data controllers must make greater commitments since they are the ones who decide on the databases and the purposes of the processing.

It is common that a same individual or entity simultaneously acts as both a processor and a controller. In such case, the obligations defined for each must be fulfilled.

The following are the main obligations for both data controller and data processors

TOPICS	OBLIGATIONS ON DATA CONTROLLERS	OBLIGATIONS ON DATA PROCESSORS
Data subjects' rights	Guarantee the data subjects, at all times, the full and effective exercise of the habeas data right (to know, update, rectify and suppress their personal data)	Guarantee the data subjects, at all times, the full and effective exercise of the habeas data right (to know, update, rectify and suppress their personal data)
Legitimacy of the data processing	Request and keep, under the conditions provided in the law, a copy of the relevant authorization granted by the data subjects.	Process the personal data in accordance with the instructions of the data controller and the purposes authorized by the data subjects.
Security of the personal data	Keep the information under the necessary security conditions to prevent the adulteration, loss, unauthorized or fraudulent consultation, use of or access to it.	Keep the information under the necessary security conditions to prevent the adulteration, loss, unauthorized or fraudulent consultation, use of or access to it.
Policies regarding the processing of personal data	Adopt a privacy policy as well as manuals and procedures to ensure proper compliance with the law, including the designation of a privacy officer or committee.	To adopt a privacy policy as well as manuals and procedures to ensure proper compliance with the law, including the designation of a privacy officer or committee.
Notification of security incidents	Notify the Data Protection Authority (Superintendence of Industry and Commerce) of violations of the security codes and risks in the data subjects' information management.	Notify the Data Protection Authority (Superintendence of Industry and Commerce) of violations of the security codes and risks in the data subjects' information management.
Registration of databases	Register their databases in the National Registry of Databases (in Spanish RNBD), which is a public directory administered by the Data Protection Authority	N/A

International data transfer and transmission

Colombian privacy law establishes specific obligations in order to protect personal data that is accessed or processed by third parties abroad. To this end, it distinguishes two categories.

International data transmission

Is the sending of personal information to a natural or legal person located abroad, who will process the data on behalf of a data controller. Examples of international data transmissions are

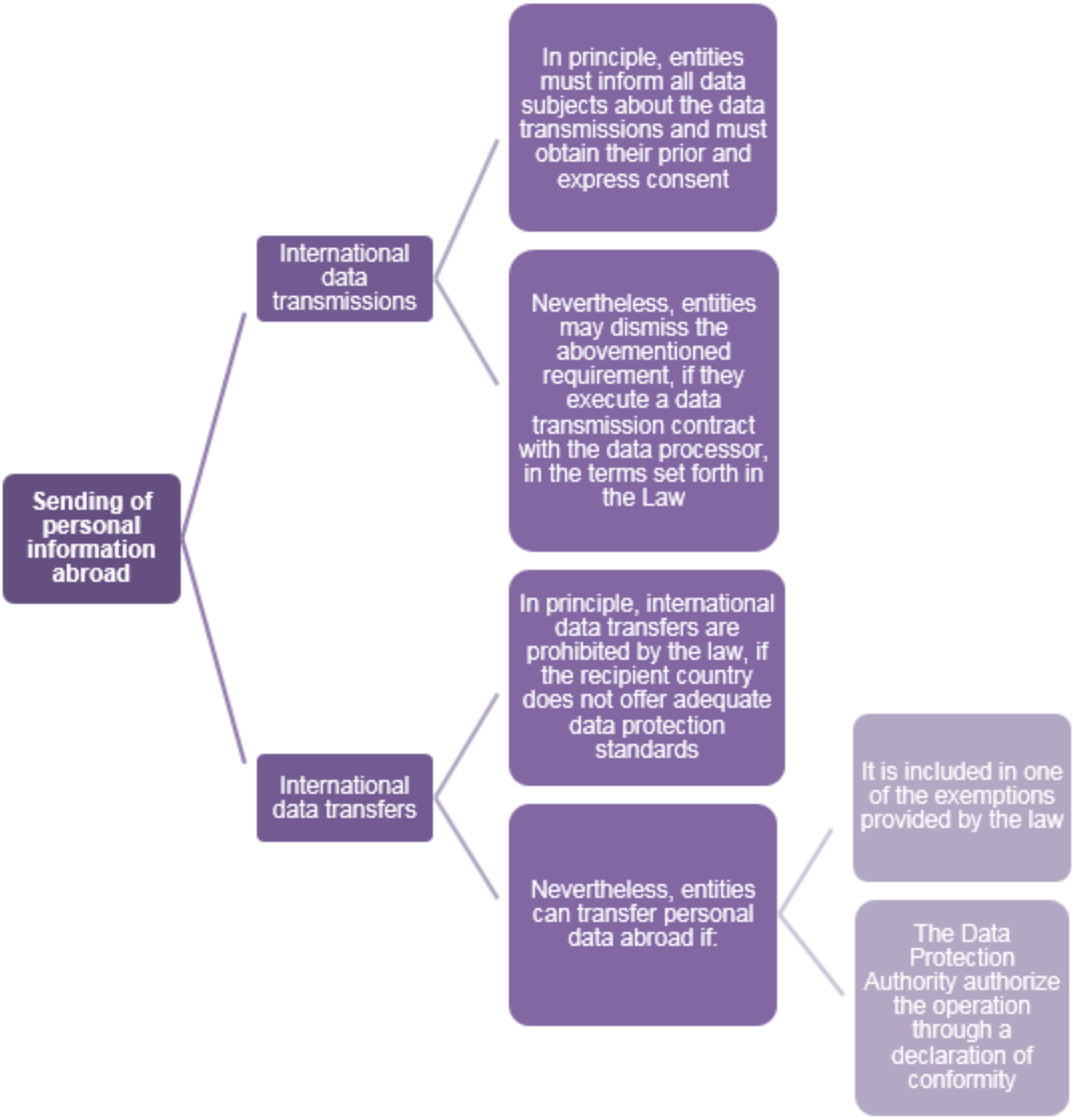
(i) the contracting of outsourcing services with entities located abroad, concerning the sending of databases or personal information (I.e.: Payroll management processes, health services overseas, etc.); Or

(ii) contracting cloud services, when the supplier stores information on a server located outside Colombia.

International data transfer

Is the sending of personal information to a natural or legal person located abroad, who will decide autonomously on the purposes and treatment of personal information. As an example of this figure, is the sending of information of a company Subsidiary to its parent company, when the latter uses the information according to its own parameters.

International data transfers and transmissions constitute different regimes with diverse obligations. Therefore, if an entity or individual transmit or transfer personal data abroad, the following requirements must be taken into account:


Sending of personal information abroad
International data transmissions
In principle, entities must inform all data subjects about the data transmissions and must obtain their prior and express consent
Nevertheless, entities may dismiss the abovementioned requirement, if they execute a data transmission contract with the data processor, in the terms set forth in the Law
International data transfers
In principle, international data transfers are prohibited by the law, if the recipient country does not offer adequate data protection standards
Nevertheless, entities can transfer personal data abroad if:
It is included in one of the exemptions provided by the law
The Data Protection Authority authorize the operation through a declaration of conformity

Notification of security incidents

Colombian privacy law establishes the obligation to notify the Data Protection Authority in the event of security incidents that generate risks in the administration of the personal data. This obligation is applicable to both data processors and controllers that process personal data in Colombia.

While there is not a single definition of a security incident, Colombian privacy law refers to them in the following terms:

a) Law 1581 of 2012 establishes that both data controllers and processors must inform the Data Protection Authority in the event of violations of security codes that generate risks in the administration of the personal data.

b) The Data Protection Authority defines security incidents as the violation of security codes or the loss, theft and / or unauthorized access of personal information from a database managed by a controller or a processor.

In addition, the Data Protection Authority established a definition through its Accountability Guidelines. Although this document is not binding, it establishes the parameters and definitions that the Data Protection Authority considers appropriate for the management of personal information. In relation to security incidents, the Guidelines state that they refer to any event against information systems, manual or systematized, which threatens the security of the personal data stored in them.

In other words, and considering the abovementioned definitions, it is possible to establish that a security incident is the violation of a physical or technological information infrastructure, which compromises the availability, integrity or confidentiality of the personal information contained in it.

On the other hand, the Data Protection Authority has delimited the information that must be provided at the time of reporting a security incident. Therefore, the report should contain at least the following information:

- Type of incident
- Date of occurrence
- Date in which the controller or processor had knowledge of the incident
- Causal
- Type of information compromised
- Number of data subjects affected by the incident

Currently, Colombian law has not defined a specific procedure for reporting security incidents. However, data controllers can make the notification through the National Registry of Databases within fifteen (15) working days following the moment the incident is detected.

Finally, it is important to keep in mind that data controllers and processors are not obliged to inform data subjects about the occurrence of security incidents. In spite of the above, the Data Protection Authority recommends to implement efficient mechanisms to inform data subjects of the occurrence of security incidents and their possible consequences, as well as to provide tools to minimize potential or caused damages. Therefore, even if the notification to data subjects is not mandatory, it can be assessed by the authority as an evidence of transparency.

Supervision and sanctions

The entity designated to supervise the compliance of Colombian privacy law is the Superintendence of Industry and Commerce, through its Data Protection Office. Please note that non-compliance with any of the provisions established by law may cause the following penalties:

- Fines, up to the equivalent of two thousand (2,000) minimum monthly legal wages (approximately COP $ 1,475,000,000 or USD $ 500,000)
- Temporary suspension or closure of activities related to the data processing.
- Immediate and definitive closing of the operation involving the processing of sensitive data

At present, most of the sanctions imposed by the Data Protection Authority refer to the violation of the Habeas Data regime for the financial sector (Law 1266 of 2008). However, regarding the general regime of data protection, the most frequent violations are derived from:

Law 1581 of 2012	
Data controllers	Not obtaining proper authorizations from the data subjects for the processing of their personal data. Failure to implement adequate security measures.
Data processors	Allow access to personal information to unauthorized persons / entities.

Legislative projects

At present, the issue that has generated the most discussion is the transfer of personal abroad. In consequence, on July 17, 2017, the Data Protection Authority presented a new draft circular in order to develop the existing regulation on international data transfers, which is currently being reviewed. Specifically, the draft circular explicitly sets forth the standards that must be considered when deciding if a country has an adequate data protection level, as well as a list of countries that met such criteria. Likewise, the draft circular defines specific parameters regarding the request of a declaration of conformity before the Data Protection Authority

In particular, the draft circular contains the following provisions:

Standards of an adequate level of data protection

In order to determine whether a country offers an adequate level of data protection, the following standards must be considered:

(i) the existence of binding regulations applicable to the processing of personal data;

(ii) the legal recognition of principles applicable to the data processing, the rights of the data subjects and the duties of both data controllers and processor;

(iii) the existence of judicial and administrative means and channels to ensure the effective enforcement of the law and the rights of the data subjects; and

(iv) the existence of competent authorities in charge of supervising the processing of personal data and enforcing the applicable

Countries offering adequate levels of data protection

According to the draft circular, the following countries offer an appropriate level of data protection: Austria, Belgium, Bulgaria, Cyprus, Costa Rica, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Iceland, Italy, South Korea, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Norway, Peru, Poland, Portugal, Spain, Slovakia, Slovenia, United Kingdom, United States, Romania, Serbia, Sweden, and countries that have been declared by the European Commission as countries with adequate levels of data protection. International transfers to the United States can only be executed to entities or individuals that joined the Privacy Shield Program established by the European Union in 2016.

Procedures related to the request of declarations of conformity

If data controllers fail to justify an international data transfer through the exceptions established in the law, the standards of an adequate level of protection or the listing of countries offering such level, they must request a declaration of conformity before the Data Protection Authority. To do so, data controllers must file a petition addressed to the Document Management and Physical Resources Group or send a request to the email contactenos@sic.gov.co, providing the information described in the "Guide to request the declaration of conformity" in Spanish. The procedure for requesting a declaration of conformity will be governed by the Contentious Administrative Code, specifically in relation to the general administrative procedure.

Tacit declaration of conformity

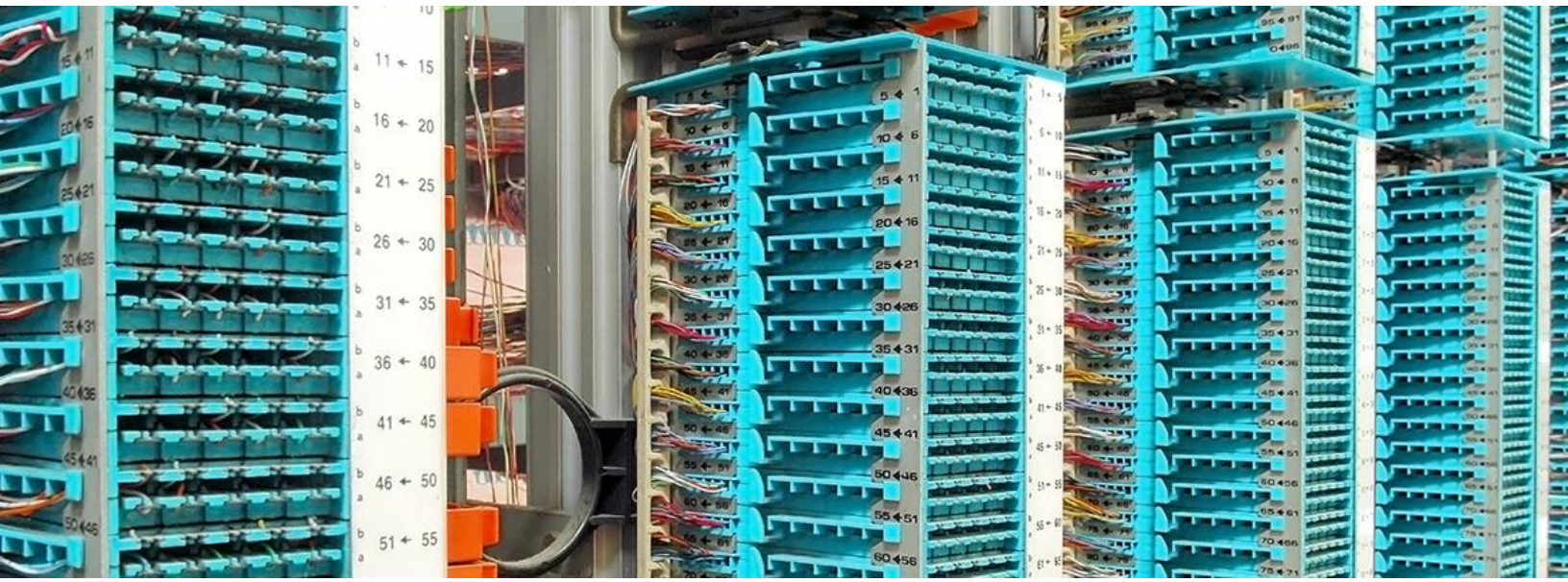
Data controllers may execute a data transfer agreement or any other legal instrument that guarantees the protection of the personal data, the compliance with the principles governing the data processing and that establishes the obligations for each party. If the legal instrument contains the above-mentioned elements and the data controller declares the existence of such document as well as the conditions of the international data transfer before the Data Protection Authority, it will be presumed that the operation is viable and that it has a declaration of conformity. Notwithstanding the foregoing, the Data Protection Authority may verify the conditions of the international data transfer, at any time, and may investigate and sanction non-compliance with Colombian privacy law.

In short, if the new draft circular is approved, the available options to legalize an international data transfer are:

1. Execute the data transfer in accordance to one of the exceptions established in Law 1581 of 2012; or
2. Verify that the recipient country is included in the list countries with adequate levels of data protection; or
3. Verify that the recipient country meets the standards of an adequate level of data protection; or
4. Request a declaration of conformity to the Data Protection Authority through a general administrative procedure; or
5. Execute a data transfer contract or other legal instrument according to the requirements established by the draft circular, and inform the Data Protection Authority about the operation to be made and the existence of the legal document.

According to the draft circular, data controllers should be able to demonstrate, at any time, that they have implemented adequate and effective measures to ensure the security and proper processing of the personal data that is being transferred abroad, even if such operation is carried out to countries that have an adequate level of data protection. In addition, the draft establishes that simple cross-border transits or redirection of data does not constitute international data transfers.

Currently, the draft circular is in the discussion, and consequently, all international data transfers that are carried out at the moment must comply with the conditions established by Law 1581 of 2012.



Conclusions

Although personal data protection is a relatively new topic in Colombia, it is increasingly relevant for companies operating in the country. On one hand, companies are more aware of their responsibility in the processing of personal information, due to the active role of the Data Protection Authority through investigations and the imposition of sanctions. On the other hand, citizens are more aware of the importance of protecting their personal information, as well as the mechanisms available to exercise their rights. The role of the Data Protection Authority has been of vital importance when enforcing the Colombian regulation in this area, as it is the motor that has driven companies to implement internal policies for the management of personal information.