Data Protection Matters: The Applicability of the Principle of Accountability to Companies in Colombia

This resource is sponsored by:

LLOREDA-CAMACHO 400

Overview

As data protection has developed in the later years, so have the principles associated with such an important topic. European nations and the United States are more familiar with the concept of accountability, and companies in such countries are already applying it, however as we pointed out in a previous occasion (Development of Data Protection Regulation in Colombia), Latin-American countries like Colombia has just started to regulate the use of data and the access to information. Now, when that regulation is in force, it becomes important for the companies, data controllers and data processors to be aware of the obligations that data handling implies. It is also important that those companies continue to implement internal processes to the applicability of data protection regulation and the protection of the data subjects’ rights. This Quick Counsel will focus on the way Colombian regulator has included the principle of accountability in the regulation on data protection and the way such principle should be apply. Also, this document will help you to determine the relevant aspects to be taken into account when applying Colombian data protection regulation and in assessing the action steps that must be undertaken inside your company in order to make it more suitable for processes of data handling.

Back to the top

CONCEPT OF ACCOUNTABILITY

The principle of accountability in relation with data protection was introduced to the Colombian regulation by Decree 1377 of 2013 (hereinafter the “Regulatory Decree”), which regulated Law 1581 of 2012 (hereinafter referred as the “Data Protection Regulation”), however the said decree did not establish a definition of accountability but mentioned that Data Controllers must be able to demonstrate, when the Superintendency of Industry and Trade - “SIC” after its Spanish acronym) requires it, that they have implemented the appropriate compliance programs to handle data.

Even though it is a new principle within the Colombian regulation for data privacy matters, the principle of accountability has been in the legal scope of data privacy for a while. This principle was first established by the Organization for Economic Co-operation and Development (OECD) in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, establishing that “a data controller should be accountable for complying with mechanisms which give effect to the principles stated above”.

Also European as well as the United States regulations, have adopted the principle of accountability as part of their data protection regimes. Regulations often include the principle either per se or directly (i.e. the Spanish data protection regulation - Organic Law 15/1999, of December 13th, establishes the obligation for data controllers to adopt organizational and technical programs and procedures that warrant the security of data).

In general, accountability means to comply with the applicable regulation, to apply compliance programs that assure that data is being handled correctly and securely, and most important to be able to demonstrate the authorities that your company is implementing such programs and procedures.

Back to the top

WHY IS ACCOUNTABILITY IMPORTANT FOR COMPANIES?

Nowadays, in the daily operation of companies a huge amount of data is handled. Data handling occurs in all of the activities that a company performs in order to operate (i.e. data from employees, subcontractors, clients, etc., handled by most of the companies, also a vast amount of data transfers is perform daily), even if the company is not in the business of data handling. Therefore, data protection regulation, in Colombia or in any other part of the world, is a matter all companies should take care of, especially those companies that handle data from third parties such as customers, patients, providers, etc.

Earlier in this document, when defining the principle of accountability we mentioned that it is the data controller’s obligation to assure that data is being handled correctly and that there are appropriate methods that warrant this obligation. As we have said, even companies in which data handling is not their core business must be able to show the compliance with the regulation, with mechanisms that warrant the application of the regulation and the protection of data. Companies need to be aware of the importance of handling data, but most important of the relevance of protecting the data in order to prevent any handling of data that does not complies with the applicable regulation, or any data leakage or violation to the privacy of data. Here is where accountability takes an important place, since it will help to prevent those events. Being able to determine the stages of data processing and the activities being performed with the data will help to avoid risk related with the data processing.

Companies should aim to prevent rather than solve, issues related with data privacy violation. Therefore, setting the appropriate internal policies will be helpful for the organization in order to warrant the secure and confidential handling of data. When the data handling is based on accountability and companies are aware of the way data should be handled and also the risks of handling, it will create and internal consciousness on data handling processes.

Also if a company has implemented appropriate procedures and is properly handling the data, in case there is any investigation by the authorities this will be the keystone on the company’s defense. Moreover, think about any exceptional case of data leakage caused by a human error, in such an event if your company has applied accountability and, therefore has established processes for handling data, this will help in obtaining a reduced penalty.

Back to the top

COLOMBIAN REGULATION AND THE PRINCIPLE OF ACCOUNTABILITY

The Regulatory Decree brought our attention to the accountability principle and included it in the Colombian regulation on data protection matters. The said decree establishes that the appropriate mechanisms used by a company should be proportional to the following:

1. The data controller’s legal form, the company’s size, in which it will be important to determine if it is a small, medium or big enterprise.
2. The kind of data that is being handled.
3. The type of technology used for handling data.
4. The potential risk that such handling may cause to data subjects.

Companies will also have to be able to provide, upon request of the SIC, a description of the data collection procedures, a description of the purposes to handle the data, and to explain the relevance for the company to handle such data.

Also the said decree establishes that the mechanisms or procedures to be implemented by a company must warrant, at least, the following aspects:

1. The existence of an administrative structure that is proportional to the size of the data controller.
2. The adoption of internal mechanisms that implement policies including training and education programs related with data privacy.
3. The adoption of processes for the attention of petitions, complaints and claims of data subjects, related with data handing.

The aspects mentioned above are some of the aspects that the Colombian authorities will take into account when imposing sanctions on the violation to the Data Protection Regulation.

Back to the top

MECHANISMS AND PROCESSES TO ADOPT

Having seen how important the application of accountability can be for a company, in this chapter you will find some aspects that we consider should be analyzed and taken care off, inside companies, in order to use accountability as a tool that will help on the appropriate handling of data. Please find bellow some useful recommendations:

1. Establish a privacy policy that complies with the applicable regulation.
2. Determine what kind of data your company process (i.e. sensitive data).
3. Determine the purposes of the data handling that your company is performing (i.e. if it is only for internal use, or if there are transfers/transmissions of data, etc.)
4. Establish what kind of actions are being taken inside the company in order to handle data (i.e. Are there any authorization required? Why are we collecting the data? Is it necessary to collect the data? Who may have access to the data? Will there be any restriction on the processing and storing data? Which are the procedures for data collecting and storage?)
5. Identify the employees that have access to personal data, and those that have access to personal sensitive data.
6. Implement education sessions on data privacy for all of your employees.
7. Design a privacy program that considers all the internal and external uses of data, and the purposes for which data is handled.
ADDITIONAL CONSIDERATIONS ON DATA PROTECTION IN COLOMBIA

We would also like to call your attention to the fact that the Colombian National Data Base Registry was recently regulated by Decree 886 of 2014, however the SIC has not put it in place. Once the registry operates the processes that companies have implemented thanks to the accountability principle will be important since they will help to identify all the requirements that will be needed to carry out such registration are the following:

1. Identification of the data controller.
2. Identification of the data processor.
3. Procedures for the data subjects to exercise their rights.
4. Name and purpose of the data base.
5. Method in which the data is being handled (manual or automatized).
6. Data privacy policy.

All of the aspects mentioned above will be easy to identify if a company has implemented a privacy program adapted to the company’s purpose.

CONCLUSION

The immense amounts of data handling, transfers and transmissions that occur in today’s business world, requires from the implied agents a bigger sense of protection of data. The importance of the regulation and of the applicability of procedures and compliance programs that warrant the compliance with regulation is mostly important because it applies to the data that is being handled by the companies, especially to that data that belongs to third parties and that is personal information. It is not enough with complying with the regulation but it is necessary to implement mechanisms and programs that assure the security, confidentiality and rightful handling of data. In doing so, accountability plays an important role, by giving companies the tools that are required to show their compromise and compliance with the regulation applicable to the handling of personal data. For example, Data Protection Regulation establishes the obligation of getting an authorization from the data subject to handle his/her data, however if the authorization is granted but data is not being handled correctly and its confidentiality is assured the authorization to handle data will not be of any use. What is important is to warrant that the company is using the data properly and that it has a structure that aims for the rightful handling, providing control mechanisms and adequate compliance programs for data protection.

Back to the top

ADDITIONAL RESOURCES

- http://www.privacybydesign.ca/
- http://www.informationpolicycentre.com/accountability-based_privacy_governance/
- http://www.sic.gov.co/drupal/node/9024