LLOREDA·CAMACHO &CO

Data protection regulation in Colombia

LLOREDA · CAMACHO & CO

Colombia has implemented general regulations on Personal Data protection since 2012. Before the issuing of Law 1581 of 2012 (the Data Protection Law), the Government had issued a specific regulation on Personal Data protection exclusively applicable to financial data; also, the National Constitution of 1991 includes habeas data as a fundamental right, however that was not enough to effectively protect and ensure the rights of privacy for all citizens.

Since the Data Protection Law was issued, its main goals have been to protect the rights of Data Subjects (individuals whose data is processed) and to ensure them that any company handling their data will comply with all the legal requirements. In this sense it is necessary that companies are aware of their operation regarding data handling in case they want to comply with the regulation.

1. Relevant Aspects

- Personal data protection is specifically regulated by the Data Protection Law along with its regulatory decrees, Circular 002 of 2015 from the Superintendence of Industry and Commerce ("SIC"), and Title V of the General Circular of the SIC. The regulation establishes a set of minimum requirements for the collection, storage, use and any type of operation to be performed with data ("Data Handling"). This regulation has been in force since 2012.

- Personal Data is any information that is linked or may be associated with an individual or individuals considered data subjects (the "Data Subject").

- Data Handling may be performed directly by an individual or entity (Data Controller), or by a third party designated by the data controller (Data Processor).

- The Data Protection Law will not be applicable to Personal Data stored in the following databases: a. Personal or domestic. b. Security and national defense, and the prevention, detection, monitoring, and control of money laundering and terrorism financing. c. intelligence and counterintelligence. d. Journalistic information. e. Financial and credit information (Law 1266 of 2008). f. Population censuses (Law 79 of 1993).

- The legal justification to handle personal data is based in consent given by the Data Subject. Therefore, any handling of personal data that is performed without explicit consent from the Data Subject would be considered unlawful, except in the cases in which consent is not required.

- Consent to handle Personal Data would not be required only in cases mentioned in article 10 of the Data Protection Law, which are the following:

    - Information required by a public or administrative entity in its normal operation, or by judicial order.
    - Public data.
    - Medical or sanitary emergencies.
    - Data handling specifically authorized by law for historic, scientific, or statistical purposes.
    - Information related with the civil registry.

- A relevant concept is the one of sensitive data. This includes data such as political or religious views, biometric information, health, or clinical information, among others. In order to handle sensitive data a more specific and previous consent must be obtained. For the handling of sensitive data, the data subject must be informed that he/she is not obliged to provide the sensitive data.

- Data Controllers must comply with different obligations, including the following, which are the most relevant:

o Implement a policy in which all the internal requirements for data processing by the company are established. The privacy policy must include at least the following:

- Name or company name, city of residence, address, email and telephone of the data controller.
- Purpose of the Data Handling.
- Data Subject´s rights.
- Person or responsible for the attention of requests, inquiries and complaints to which the Data Subject can direct his/her request in order to exercise his/her rights to know, update, rectify and delete the data and revoke their consent.
- Procedure to inform the Data Subjects about how to exercise their rights.
- Privacy policy's effective date and duration of the database.

o Always obtain in a prior and express manner consent to handle Personal Data. Consent must inform the purpose of the Data Handling and the type of data to be collected, among others. Consent may be obtained orally, by written means or by unequivocal conducts of the data subject; in any case consent must be available for review or access by the data subject at any time.

o The use of the information is limited to the purposes established in the consent given by the Data Subject.

o When obliged, data controllers must perform the registry of data bases within the National Data Base Registry (NDBR).

2. Accountability program

The Regulatory Decree 1377 of 2013 also dealt with accountability matters, establishing obligations for controllers to guarantee compliance with the Data Protection Regulation.

The regulation establishes that in the data handling, Data Controllers must be able to demonstrate that they have acted in a responsible manner and in compliance with the law. To implement an accountability program companies must consider the following:

- Have effective internal politics on data privacy.
- Implement compliance mechanisms
- Designate an individual or individuals that oversee the data protection matters, for example a Data Privacy Officer (DPO).
- Implement procedures to educate and make people aware of the need to warrant security and confidentiality of data.
- Evaluate risks and be able to mitigate them.
- Constantly review the implementations of matters related with data privacy.
- Implement security measures mentioned above as well as the mechanisms to exercise Data Subjects' rights.

3. Obligation to register the data bases that handle Personal Data within the NDBR

All the data controllers which total assets are of more than approximately USD$1,037,301.43 for year 2021 must register their data bases within the NDBR. Such registry requires that data controllers register general information of the company´s data bases which include, among others:

- Contact information of the Data Controllers and processors
- Purposes of data handling.
- Types of data registered within a specific data base.
- The number of data subjects.
- Mechanisms to exercise the rights of Data Subjects.
- Source of the Personal Data (identify how data was obtained)
- International or national data transfers or transmissions.
- The security measures applicable to each data base.

New data bases must be registered within the following two (2) months after its creation.

The registry must be updated at least in the following opportunities:

- In the first 3 months of every year, between January 2nd and March 31st. At this opportunity, a general update must be performed, and therefore aspects such as the number of registered data subjects must be updated.
- Complaints, queries, or requirements from data subjects must be registered on the first 15 business days of February and on and the first 15 business days of August every year. For 2021 no later than on February 19, 2021 and August 23, 2021. In such cases, the report made in August shall include the complaints, queries or requirements from subjects from the first semester of the year, and complaints, queries, or requirements from data subjects received during the second semester of the year shall be registered in February.
- Any substantial change in the data base (ej. A data transfer, the change of purposes, a new data processor) must be registered in the first 10 business days of the month following the change.
- Security breaches must be reported within 15 business days after the report is known.

The registry shall be performed though the SIC web page and it is relatively easy.

4. Criminal offenses related with the violation to Personal Data

The Colombian Criminal Code contains some criminal offenses related with "Information and Data Protection". In particular Article 269F states: "Violation of Personal Data: Anyone who, without being authorized to do so, to its own benefit or for a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies or uses personal codes, Personal Data contained in files, archives, databases or similar means, will be held liable for imprisonment for a term of 48 to 96 months and a fine from 100 to 1000 minimum monthly legal wages".

Therefore, in case that there is any breach or leakage of information anyone may file a criminal lawsuit under this article. The criminal offenses will be independent from any investigation that the SIC decides to start due to the breach or leakage.

5. Sanctions

The SIC is allowed to initiate administrative investigations against those who breach the provisions of the Data Protection Law and impose penalties of up to 2,000 Minimum Monthly Legal Wages (approx. USD$519,158 on 2021), and sanctions that include the temporary or permanent closure of the professional or commercial activities of the subject who breached the data protection regime. The penalties may apply individually to the company as well as to its directors and managers.

6. Recent developments

On December 2020, the SIC issued two new guides for controllers and processors handling personal data. The mentioned guides add up to the already published guides on accountability; marketing on internet; among others, and include recommendations and useful tools to prevent breaches to the Colombian personal data protection rules. The matters addressed were the following:

1. Handling of photos as personal data.
2. Management of security incidents when handling personal data.

In this regard, it is important to point out that the guides' purpose is to provide general recommendations to strengthen the self-regulation of those who, performing their activities, handle personal data.

Likewise, it should be noted that the guides do not cover all relevant aspects regarding the handling of photos as personal data or the management of security incidents, and therefore it is important that the applicable regulation is reviewed in order to identify the specific requirements for each specific case.

1. Guide on the handling of photos as personal data.

As per what the guide establishes, it is usual that when using photos, it is ignored that they may contain personal data. In general, it is usual that photos contain personal data, since if they are from a specific individual, they may contain biometric information that enables to identify one or more individuals included in the photography.

To that extent, the SIC compiled some of the most relevant duties regarding the handling of photos as personal data, as follows:

1. To obtain prior, express, and informed authorization to take and use photos.
2. To verify the legitimate origin of the photos provided by third parties.
3. To bear in mind the rules for handling photos of individuals under 18 years of age, especially since those may contain sensitive data or data of a special nature.
4. To inform the data subjects about the specific purposes for which the photos will be used.
5. To refrain from obtaining photos in a misleading manner and not assume that photos of public access can be freely used.
6. To request compliance regarding the data protection regulations from third parties hired to take photos.

Finally, it is important to clarify that despite the fact that the photos may contain personal data and therefore are protected by the said regulation, photos may be also protected from different legal perspectives, such as copyright, antitrust and image rights. The guide also establishes that the handling of photographs in the personal or domestic sphere, and for journalistic and editorial purposes is not forbidden as established in the regulation.

2. Guide for the management of security issues in the personal data handling.

The SIC also issued a set of practical recommendations to correctly deal with the occurrence and report of security incidents affecting data bases which contain personal data handled by data controllers and data processors.

As per Law 1581 of 2012, the handling of personal data, performed by controllers or processors must be done with the necessary technical, human, and administrative measures to guarantee the security and confidentiality of the information.

Therefore, it is necessary for organizations to be prepared to mitigate the effects or risks that may be generated when such security measures fail. Bearing in mind the above, the guide issued by the SIC provides orientation in relation to the implementation of the following measures:

1. To require data processors to report the occurrence of security incidents.
2. To maintain adequately documented all the security incidents.
3. To develop a personal data handling program that includes a response protocol in the management of security incidents.
4. To implement the necessary steps to deal with possible security incidents.

Also, the guide highlights the need to increase and maintain the confidence of the personal data subjects in the organizations, as a fundamental aspect for the consolidation of any activity that involves the personal data handling.

Finally, both guides reiterate the need to apply the accountability principle in the handling of personal data, and therefore it will be important that the specific guide issued by the SIC on the accountability principle is considered at all times when referring to the handling or personal data.

We look forward to commenting any query regarding the abovementioned matters.

Enrique Álvarez
SOCIO

María Alejandra De Los Ríos
ASOCIADA SENIOR

LLOREDA · CAMACHO &CO

www.lloredacamacho.com