Colombia

Marrugo Rivera & Asociados, Estudio Jurídico Ivan Dario Marrugo Jimenez

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

1581/2012 Act.

1.2 Is there any other general legislation that impacts data protection?

2377/2013 Decree.

1.3 Is there any sector specific legislation that impacts data protection?

1266/2008 Act, Financial (financial data) sector. 1712/2014 Act, Open Data and Transparency.

1.4 What is the relevant data protection regulatory authority(ies)?

Delegation for the protection of personal data from the Superintendency of Industry and Commerce.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

"Personal Data"

- Any information that can be associated with or linked to one or more identified or identifiable natural person.

"Sensitive Personal Data"

- Those affecting the privacy of the Legal Holder and the abuse of which may generate its discrimination.

"Processing"

- Any operation or set of operations on personal data, such as collection, storage, use, data movement or deletion.

"Data Controller"

- Natural person or legal, public or private person, which by itself or in association with others, decides on the basis of data and/or data handling.

"Data Processor"

- Natural person or legal, public or private person, which by itself or in association with others, performs the processing of personal data on behalf of the data controller.

"Data Owner"

- Natural person whose personal data are subject to treatment.

"Data Subject"

- This is not applicable.

"Pseudonymous Data"

- This is not applicable.

"Direct Personal Data"

- This is not applicable.

"Indirect Personal Data"

- This is not applicable.

"Authorisation"

- Prior, express and informed Holder consent is necessary in order to carry out the processing of personal data.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

Transparency

- The Holder must be guaranteed the right to obtain from the data controller or Data Processor at any time without restrictions, information about the existence of data concerning him.

Lawful basis for processing

- The treatment of data is a regulated activity that must be subject to the provisions in the law and the other provisions implemented.

Purpose limitation

- The treatment of data must have a lawful purpose in accordance with the Constitution and the law, which must be reported to the Holder.

Data minimisation

- Act 1581/2012 has not specified the Data minimisation as a principle. The unique express reference to data anonymisation is related with the Sensitive data processing. In this regard, Article 6 states that in the data processing of historical and statistic or scientific data, measures should be taken leading to supress the identity of holders.

Proportionality

- This is not applicable as a principle.

Retention

- Under 1266/2008 Act; Holder information may not be

provided to users or third parties as this is not the purpose of the database.

- **Security:** The information subject to treatment by the data controller or Data Processor which this Act relates to, should be handled with the technical, humane and administrative measures necessary to provide certainty for preventing adulteration of records, loss, query, use or unauthorised or fraudulent access.
- **Confidentiality:** All persons involved in the processing of personal data that is not public are obliged to ensure the confidentiality of information.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

Access to data

- To request and obtain information from the data controller of the personal data.

Correction and deletion

- The Holder has the right to know, update and correct their personal information where it is inaccurate, incomplete or fractionated, misleading or when it could be banned.
- **Objection to processing**

  Only in two cases: 1. Misuse of the information by the violation of the principles, rights and constitutional guarantees. 2. When the Superintendency of Industry and Trade certifies that the Responsible Manager has engaged in conduct contrary to the Constitution and the Law.
- **Objection to marketing**

  This is not applicable.
- **Complaint to relevant data protection authority(ies)**

  There are two procedures: 1. Consultation; and 2. Complaint.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There is a general notification requirement. To process sensitive personal data, authorisation is always needed prior to the treatment.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Registrations apply for each database.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

The principles and provisions contained in 1581/2012 Act shall apply to personal data on any database that makes them susceptible to treatment by public entities or private entities.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The pieces of information that must be registered are: Details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes, data underage.

5.5 What are the sanctions for failure to register/notify where required?

There are no specific penalties for non-registration. The SIC may impose economic sanctions, or temporary or permanent closure of establishments for breach of the regulations.

5.6 What is the fee per registration (if applicable)?

Registration is free.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

The national registry database is still under construction. According to a draft decree obligated parties will have six months after opening the registry to perform the initial procedure. Later, parties will have a period of 2 months for updates whenever necessary.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

For international transfer and transmission of personal data to countries that do not have an adequate level of protection of data.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

The obligated party must obtain declaration of conformity of the SIC for transfer to other countries. There is no legal timeframe for it.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a DPO is mandatory under articles 17 and 18 of 1581/2012 Act and Art. 23 of 1377/2013 Decree.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Office where required?

There's no specific penalty for the failing to appoint a DPO. General sanctions include: penalty of up to 2,000 minimum salaries (1,230 million pesos/USD570,000) approx.; suspension of activities and temporary or permanent closure of business establishments.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law?

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

General information regarding their responsibilities can be seen in Arts. 17 and 18 of 1581/2012 Act and specifics can be seen in the 1377/2013 Decree.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Obligated parties who process personal data must be registered on the National Register database.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, or SMS text message (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

There are no such restrictions in the Data Protection Act. There is a specific regulation on sending commercial communications by mobile operators but this is sectoral.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The delegate of data protection is working to strengthen the Colombian system, due to its recent expedition it still needs to mature.

7.3 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There´s no specific penalty for sending marketing communications. General sanctions include: A penalty of up to 2,000 minimum salaries (1,230 million pesos/USD570,000) approx., suspension of activities and temporary or permanent closure of business establishments.

7.4 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

This is not applicable. 1581/2012 Act did not regulate the use of cookies.

7.5 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

This is not applicable. 1581/2012 Act did not regulate the use of cookies.

7.6 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, it has not.

7.7 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable. 1581/2012 Act did not regulate the use of cookies.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

Art. 26 of 1581/2012 Act prohibits in general terms, the international transfer of data to countries that do not have an adequate level of protection. Only in specific cases can such transfer be done.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

The 1581/2012 Act mentioned the BCRs but they have not been developed into the regulation.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Yes, although this is still under construction. The SIC is working on a white list of countries with an adequate level of protection.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

In Colombia it is a criminal offence to violate personal data. Under the 1273/2009 act and the code of criminal procedure anyone who knows of a crime must report it. Facing the administrative procedure before the SIC, only the owner and his beneficiaries may present the complaint to initiate the procedure, according to the provisions of Section 15 of the Act.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

This is not applicable.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

There is a requirement to file the complaint about the personal data and submit it to the responsible organisation.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

There is no specific legislation relating to the use of CCTV so no prior approval is required by the delegate. In a recent development, SIC stipulated that surveillance activities should be subject to the 1581 Act.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

The Data Protection Act does not address this issue. Labor law permits the monitoring of employee activities however it also states that employers should respect the privacy rights of workers, a policy must exist where monitoring is disclosed to employees as well. The installation of video surveillance cameras in the workplace must preserve the privacy of the workers but the main reason for its use is to monitor the facility and offices, so it must be remembered that this right should not be violated.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

According to Article 5 of Law 1581, biometric data (in this case images), are categorised as sensitive data which affect the privacy of the owner. In this case, prior and informed consent of the Holder is necessary, which must be obtained by any means even if further consultation is required.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

This is not applicable. Data such as union membership are considered sensitive and their treatment is the most restrictive.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No. It is a good practice but not mandatory.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

It is permitted provided that the controller contractually transferred to the service provider the duties and obligations of the processor provided by law. Likewise the service provider must take the necessary security measures to prevent the tampering, loss, consultation, use, or unauthorised or fraudulent treatment of data.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

a) Ensure that the Holder has, at any time, the full and effective exercise of the right of habeas data.

b) Maintain information on security conditions necessary to prevent tampering, loss, consultation, use, or unauthorised or fraudulent access.

c) Perform timely updating, rectification or deletion of data in terms of this Act.

d) Update the information reported by the controllers within five (5) working days of your receipt.

e) To deal with inquiries and complaints made by the Holders under the terms stated in this law among others.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

When information is processed individually or in association with a particular person we are not in the scope of protection of personal data, and no consent is needed. The analysis and use of large volumes of data is then perfectly feasible, provided that the company takes precautions so that this information is not individualised and will not be associated with a particular person. Otherwise you must obtain the consent of the owner.

When large amounts of personal data are processed and these affect any right, in this case if the express and informed consent is required. In this case it is especially important downstream use to which this information will be subject.

13 Data Security and Data Breach.

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The 1581 Act states that the responsible care of custodians shall keep the information on security conditions necessary to prevent tampering, loss, consultation, use, or unauthorised or fraudulent access.

The Superintendency of Industry and Commerce has yet to provide

instructions regarding safety measures in the treatment of personal data. Currently the Act and Decree 1377 requires organisations to adopt effective measures and appropriate internal policies to ensure compliance with the obligations under the Act and Decree.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Yes. According to Article 17 and 18 lit n and k respectively of the 1581 Act, the data protection authority must be informed when violations of the security codes occur and there are risks in the management information headlines. So far it is still unclear how the report should be made, or the limited means or dates. However, with the new decree that is expected to be issued this year, the National Database registry will be enacted; in the inscription procedure entities will be able to inform if any breach or vulnerability has occurred in the personal data treatment.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Not to individuals, only to the authority.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/administrative Sanction	Criminal Sanction
Penalty	Administrative sanction	Prison sentence of 48 to 96 months
Suspension of activities	Administrative sanction	This is not applicable
Lockout	Administrative sanction	This is not applicable

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Operators of credit information Datacredito were recently sanctioned not running safety principles in the treatment of information. Telefonica movistar was financially penalised for breaking the rules regarding financial habeas data.

15 E-discovery / disclosure to foreign law enforcement agencies

15.1 How do companies within Colombia respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

This is not applicable to Colombian laws or regulatory procedures.

15.2 What guidance has the data protection authority(ies) issued?

This is not applicable to Colombian laws or regulatory procedures.

Colombia has signed treaties for international judicial cooperation and was recently invited to join the convention of Budapest on cybercrime. This is still in development.

Ivan Dario Marrugo Jimenez

Marrugo Rivera & Asociados, Estudio Jurídico
Cra. 45A #95-08 Of. 204.
Bogotá D.C.
Colombia

Tel: *+571 4674999*
Fax: *+571 4760798*
Email: *imarrugo@marrugorivera.com*
URL: *www.marrugorivera.com*

Ivan Dario Marrugo Jimenez: Lawyer at the University of San Buenaventura. Specialist in Telecommunications from at the University of Rosario. He also studied a Masters in Administrative Law at the same university. Certificate in Internal Auditor Security Information Management Systems ISO 27001. Computer Hacking Forensic Investigator - CHFI EC-Council v.8. Expert in Technology Law, specialises in Electronic Commerce, Computer Law, Information Security and Data Protection, Information Technology and Communications, Digital Evidence, Computer Forensics, Methods of electronic signatures and authentication, Intellectual Property, State Procurement and Legal Services.

MR MARRUGO RIVERA & ASOCIADOS Estudio Jurídico
¡Su Camino a la Seguridad Jurídica comienza Aquí!

Founded in 2008, Marrugo Rivera & Associates projected as a leading firm in providing services in Colombia and Latin America on emerging technology law. Our focus is given to provide comprehensive assistance in providing solutions in versatile Business Law, and a safe and reliable service to our customers. What makes us different is the commitment and passion that we give to each job. Innovation, agility, a serious ethical commitment and a sense of responsibility mark our legal practice. We are aware of the needs of businesses in a globalised world and we integrate our quality professional services and the training of our employees so as to ensure, by timely and effective care, the Legal Certainty that the companies need. Our main focus is the emerging technology law, information security, Data Protection and Privacy, e-commerce, software and computer law.