



NOKIA SOLUTIONS AND NETWORKS COLOMBIA LTDA.

MANUAL OF POLICIES AND PROCEDURES FOR THE PROTECTION OF PERSONAL DATA

BOGOTÁ D.C.

2018



PREAMBLE

Statutory Act 1581 of 2012 which provides general provisions for the protection of personal data, aims to develop the constitutional right of all persons to know, update and rectify the information that has been collected from them in databases or archives, as well as other constitutional rights, freedoms and guarantees, pursuant to article 15 of the Colombian Constitution and the right to information, in accordance with article 20 thereof.

The principles and provisions contained in Act 1581 of 2012, decree 1377 of 2013 and other rules that amend and/or complement them, are applicable to the personal data recorded in any database susceptible of processing by Nokia Solutions and Networks Colombia Ltda. (hereinafter "The Company"), a branch of a foreign company, identified by Nit. 900.134.430-4. Therefore, the processing of data made by The Company should be governed by the regime of protection of personal data set forth in the aforementioned regulations.

The Company accepts the general provisions contained in Act 1581 of 2012 and decree 1377 of 2013, and the other rules that amend the subject-matter, and therefore adopts this internal manual of policies¹ and procedures to comply with what is determined in the aforementioned regulations, and especially, with paragraph k of article 17 of Act 1581 of 2012.

¹ The Processing policies are understood to be incorporated in this manual, complying with the provisions of article 13 of decree 1377 of 2013.



GENERAL DATA OF THE COMPANY NOKIA SOLUTIONS AND NETWORKS COLOMBIA LTDA AS RESPONSIBLE OF PROCESSING

NIT: 900.134.430-4

Office: Bogotá D.C., Colombia

Address: 72nd Street # 8 – 56 Floor 2

Phone No.: +571 5875577



INTERNAL MANUAL OF POLICIES AND PROCEDURES FOR THE PROTECTION OF PERSONAL DATA

CHAPTER I

GENERAL PROVISIONS

Article 1. Identification

This internal manual of policies and procedures for the protection of personal data (hereinafter the "Manual") was prepared by The Company, a branch of a foreign company.

Article 2. Applicable law

This Manual was prepared pursuant to articles 15 and 20 of the Political Constitution of the Republic of Colombia, and the provisions referred to in Act 1581 of 2012, decree 1377 of 2013 and complementary Acts.

Article 3. Scope of Implementation

This Manual applies to the processing of personal data collected and managed by The Company.

Article 4. Purpose

This manual complies with the provisions of paragraph k) of article 17 of Act 1581 of 2012, which governs the duties which the persons responsible for the processing of personal data are subjected to, within which it is ordered to adopt an internal manual of policies and procedures to ensure proper compliance with the above mentioned Act, and especially to address queries and claims.

It also has the purpose of regulating the procedures for collecting, handling and processing the personal data managed by The Company, in order to guarantee and protect the fundamental right of habeas data within the framework determined in the same Act.

Article 5. Definitions

In order to facilitate the understanding of this manual, below there is a transcription of the definitions set out in Act 1581 of 2012 and those of decree 1377 of 2013:

a. Definitions of Article 3 of Act 1581 of 2012

i. Authorization: Prior, express and informed consent of the Holder to conduct the processing of personal data;



ii. Databases: Organized set of personal data that is subject to Treatment;

iii. Personal data: Any information linked to or which may be associated with one or more specific or determinable natural persons;

iv. Party in charge of the Treatment: Natural or legal, public or private person, who by himself/herself or in association with others, performs the processing of personal data on behalf of the party responsible for the Treatment;

v. Party responsible for the Treatment: Natural or legal, public or private person, who by himself/herself or in association with others, decides on the database and/or the Processing of the data;

vi. Holder: Natural person whose personal data are subject to Treatment;

vii. Treatment or Processing: Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.

b. Definitions included in article 3rd of decree 1377 of 2013

i. Notice of Privacy: Verbal or written communication issued by the Responsible party and addressed to the Holder for the Processing of his/her personal data, by which he/she is informed of the existence of the policies of Processing of information that will be applicable to him/her, the way to access it and the purposes of the Processing that is intended to be given to the personal data.

ii. Public data: These are data that are not semi-private, sensitive or sensitive. Public data are, inter alia, data relating to the marital status of people, their profession or occupation and their status as traders or public servants. By nature, public data may be contained, inter alia, in public records, public documents, official gazettes and bulletins, and in duly executed judicial dispositions that are not subject to reservation.

iii. Sensitive data: Sensitive data are those that affect the privacy of the Holder, or whose misuse may lead to discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical beliefs, memberships in trade unions, social and human rights organizations, or which promote the interests of any political party, or that guarantee the rights and guarantees of opposition political parties, as well as data related to health, sexual life, and biometric data.

iv. Transfer: The data transfer takes place when the Party responsible for and/or in charge of the Processing of the personal data, located in Colombia, submits the information or the personal data to a receiver, who in turn is responsible for the Processing and is in or out of the country.

v. Transmission: Processing of personal data that implies the communication thereof in or out of the territory of the Republic of Colombia, when the purpose is to conduct a Processing by the Party in charge on behalf of the Responsible party.

Article 6. Principles



The principles listed below are the guidelines that must be respected by The Company during the process of collection, storage, use and processing of the personal data, as well as in regard to the development, interpretation and application of this Manual:

a. Principle of legality with regard to Data Processing: The Processing referred to in this Manual is a regulated activity that must be subject to the provisions of Act 1581 of 2012, decree 1377 of 2013, and other provisions that comprise it together with this Manual;

b. Principle of purpose: The Processing must obey a legitimate purpose in accordance with the Constitution and the law, which must be informed to the Holder;

c. Principle of freedom: The Processing can only be exercised with the prior, express and informed consent of the Holder. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate releasing the consent;

d. Principle of truth or quality: The information subject to Processing must be truthful, complete, accurate, updated, verifiable and understandable. Handling partial, incomplete, fractional or error-inducing data is prohibited;

e. Principle of transparency: The Processing must guarantee the right of the Holder to obtain from the Party Responsible for the Processing or the Person in Charge of the Processing, at any time and without restrictions, information on the existence of data that concern him or her;

f. Principle of restricted access and circulation: The Processing is subject to the limits that arise from the nature of the personal data, the provisions of Act 1581 of 2012 and the Constitution. In this sense, the Processing can only be conducted by persons authorized by the Holder and/or by the persons provided for in Act 1581 of 2012, and the other rules that amend or add it;

Personal data, except public information, may not be available on the Internet or other means of mass communication or disclosure, unless the access is technically controllable in order to provide restricted knowledge only to the Holders or third parties authorized pursuant to Act 1581 of 2012 and other rules that amend or add it;

g. Security principle: Information subject to Processing by the Party Responsible for the Processing or the party in charge of the Processing in accordance with Act 1581 of 2012, must be handled with technical, human and administrative measures necessary to prevent the records from adulteration, loss, quest, unauthorized or fraudulent access or use;

h. Principle of confidentiality: All persons involved in the processing of non-public personal data, are required to guarantee the reservation of the information, even after the end of their relationship with any of the tasks involved in the Treatment, thus being able to provide or communicate personal data only when it has to do with the development of the activities authorized under Act 1581 of 2012, and in the terms thereof.

CHAPTER II

AUTHORIZATION

Article 7. Authorization

The processing of personal data by The Company requires the free, prior, express and informed consent of the Holder thereof. The Company, as the party responsible for the processing of personal data, has the necessary mechanisms to obtain the authorization of the holders, thus guaranteeing in every case that the grant of such authorization may be possible, which will be provided at the latest during the collection of the data.

Article 8. Form and Mechanism to grant the Authorization

a. Form

The authorization may consist of any mechanism that may ensure the subsequent quest, the authorization may be:

- i) In writing,
- ii) Orally,
- iii) Through unequivocal conduct of the holder that allows a reasonable conclusion that the authorization was granted; in no case can silence be assimilated as an unequivocal conduct.

The consensual authorization procedure ensures that the holder of the personal data has been informed of both the fact that his/her personal information will be collected and used for the purposes determined and known, and that he/she has been informed that has the option to know any alteration or modification to the information and the specific use that has been given to it. The foregoing in order for the Holder of the information to make informed decisions regarding his/her personal data, and control the use of his/her personal information.

b. The authorization shall contain the following:

- i) Who collects the data (party responsible or in charge)
- ii) What data is to be collected (data collected)
- iii) The reason why the data are collected (the purposes of the treatment)
- iv) How to exercise rights of access, correction, updating or suppression of the personal data provided
- v) If sensitive data are collected, and the possibility of not disclosing them.



Article 9. Proof of Authorization

The Company will adopt all the suitable and necessary mechanisms in order to maintain the record of when and how the authorization by the holders of the personal data for the Processing thereof was obtained.

Article 10. Notice of Privacy

The privacy notice is the physical or electronic document that will be made available to the Holder, in which he/she is informed of the existence of the Information processing policies that will be applicable to their personal data, the way to access them and the type of Processing that will be conducted. The privacy notice will contain the following information:

- a) Name or business name and contact details of the party responsible for the Treatment.
- b) The Processing which the data will be subject to, and the purpose thereof.
- c) The rights which the holder is entitled to.
- d) The mechanisms arranged by the responsible party, so that the Holder may know the information processing policy, as well as the substantial changes that occur in it or in the corresponding Notice of Privacy. In all cases, the Holder will be informed of how to access or consult the information processing policy.

Notwithstanding the foregoing, when sensitive personal data are collected, the privacy notice must expressly state the facultative nature of the response to the questions that deal with this type of data. In any case, the disclosure of the Notice of Privacy will not exempt the Responsible party from letting the holders know the information processing policy, in accordance with the provisions of decree 1377 of 2013.

CHAPTER III

RIGHTS AND DUTIES

Article 11. Rights of the Holders of the information.

In accordance with the provisions set forth in article 8 of Act 1581 of 2012, the Holder of the information is entitled to the following rights:

- a) Know, update and rectify their personal data with the parties responsible for the Processing or those in charge of the Processing. This right may be exercised, inter alia, against partial, inaccurate, incomplete, fractioned, misleading data, or those whose Processing is expressly prohibited or has not been authorized;
- b) Request proof of the authorization granted to the Person Responsible for the Treatment, except when expressly accepted as a requirement for the Treatment, in accordance with the provisions of article 10 of Act 1581 of 2012;



c) Be informed by the party responsible for the Processing or the one in charge of the Processing, upon request, of the use given to their personal data;

d) Submit complaints to the Superintendence of Industry and Commerce (SIC) for violations to the provisions of Act 1581 of 2012 and other rules that amend, add or complement it;

e) Revoke the authorization and/or request the suppression of the data when in the Processing the principles, rights and constitutional and legal guarantees are not respected. The revocation and/or suppression shall proceed when the Superintendence of Industry and Commerce has determined that during the Processing the responsible Person or in Charge has engaged in conducts contrary to Act 1581 of 2012 and to the Constitution;

f) Free access to their processed personal data.

Likewise, the Holders will be entitled to the rights enshrined in Act 1581 of 2012 and decree 1377 of 2013.

Article 12. Duties of The Company in Relation to the Processing of Personal Data.

The Company will strictly comply, in its capacity as responsible for the information, with the obligations contained in article 17 of Act 1581 of 2012; likewise, It is aware of the importance of observing the policies and protocols tending to protect the personal data of the holders, since it is aware that the data are the property of the holders, and only the latter can decide on them. Consequently, The Company undertakes to comply with the following duties in relation to the processing of personal data:

a) Guarantee to the Holder, at all times, the full and effective exercise of the right of habeas data;

b) Request and keep, pursuant to the conditions provided for in Act 1581 of 2012, a copy of the respective authorization granted by the Holder;

c) Duly inform the Holder of the purpose of the collection, as well as the rights which he is entitled to by virtue of the authorization granted;

d) Keep the information under the necessary security conditions in order to prevent its adulteration, loss, quest, use or unauthorized or fraudulent access;

e) Ensure that the information provided to the party in charge be truthful, complete, accurate, up-to-date, verifiable and comprehensible;

f) Update the information, by notifying the party in charge of the Processing in a timely manner of all new information regarding the data previously provided, and take other necessary measures so that the information provided can be kept up to date;

g) Rectify the information when it is incorrect, and inform the party in charge of the processing about pertinent issues;



- h) Provide the party in charge of the processing, as the case may be, with only data whose Processing has been previously authorized in accordance with the provisions of Act 1581 of 2012;
- i) Require from the party in charge of the Processing Compliance at all times with the security and privacy conditions of the information of the Holder;
- j) Process the submitted quests and claims pursuant to the terms set out in Act 1581 of 2012;
- k) Adopt an internal policy and procedure manual in order to ensure proper compliance with Act 1581 of 2012, and especially for the handling of queries and complaints;
- l) Inform the party in charge of the Processing when certain information is being discussed by the Holder, once the complaint has been filed and the respective procedure has not been completed;
- m) Report at the request of the Holder on the use given to his/her data;
- n) Inform the data protection authority when there are violations of security codes and risks in the management of the information of the Holders.
- o) Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

CHAPTER IV

PROCESSING THE DATA WILL BE SUBJECTED TO AND ITS PURPOSE

Article 13. Processing and Purposes

The Company will make the personal data processing of the following Holders, in accordance with the next purposes:

Article 13.1. Processing and Purpose of the Data.

The processing of personal data will be conducted for the fulfillment of The Company's corporate purpose, including but not limited to:

- a. Conducting selection, enrollment and departure processes of the Company.
- b. Celebrating the contract between the Holder and the Company.
- c. Complying with the Company's duties, such as: affiliation to the Social Security System and payment of contributions, affiliation to the Compensation Fund and payment of contributions, payment to the DIAN of the withheld amounts, release certificates of incomes and withholdings and work certificates requested by the Holder, and / or any information required by a national entity or authority that requires the Personal Data, according with the active regulations.



- d. Keeping the safety and health of employees in the workplace, according with the applicable regulations of the Occupational Health and Safety Management System (hereinafter, "OH-SMS") and keep the documents indicated in the article 2.2.4.6.13 of Decree 1072 of 2015.
- e. Filing personal data for historical, scientific or statistical purposes of The Company.
- f. Managing the personnel linked to The Company.
- g. Managing payroll.
- h. Notify the employees' family members in cases of emergencies during work hours or on its development.

Article 13.2. Purposes of the clients' personal data.

- a. Inform about our promotions, offers, novelties, products and services, alliances, contests, current and future contents related to events, contests, promotional activities and other commercial purposes directly or indirectly related to our activity.
- b. Report on new products or services that are related to those contracted or acquired, or changes thereof. Comply with the duties obtained with our clients.
- c. Evaluate the quality of the service.
- d. Conduct internal studies on consumption habits, as well as statistical studies that allow designing improvements in products and/or services to be provided.
- e. Facilitate the correct execution of purchases and provision of contracted services;

Article 13.3. Purposes of the suppliers' personal data.

- a. Identify the associated part as supplier.
- b. Contact by any means to the supplier representatives in order of discuss commercial relationships.
- c. Fulfill the duties agreed with the supplier.
- d. Evaluate quality of service.
- e. Perform studies, catalogs and internal files on suppliers.
- f. Facilitate the correct execution of the commercial relationship.
- g. Perform events and trainings.
- h. Perform banking and non-banking transactions associated with the provider's data in order to settle obligations.
- i. Verify data in order to control drug trafficking and money laundering.
- j. Verify if the Supplier's personnel meets the necessary physical requirements to safely perform the tasks for which the Supplier was contracted by the Company.

The database seeks to have the information updated so that the relationship with customers, suppliers, contractors, and/or other interested parties can be properly developed. The processing of personal data is not limited to the events described above, but the processing thereof will be carried out in a general way for the development of The Company's corporate purpose, and to fulfill the respective obligations.



Article 14. Sensitive data Processing

In the Processing of Sensitive Data, The Company will strictly observe the limitations and obligations established on Act 1581 of 2012, its regulatory decrees and other concordant norms. Therefore, in the case of performing Sensitive Data Processing, the Company must:

- a. Obtain the Holder's express consent;
- b. Inform the Holder that by means of sensitive data, is not obliged to authorize its Processing;
- c. Inform the Holder explicitly and previously, which of the data that will be subject to Processing are sensitive and the purpose of the Processing.

The Company performs Processing of sensitive data related to health, socioeconomic status and the academic level of the employees, for the compliance of the following purposes:

- a. Verify if the employee meets the necessary physical requirements to perform the position for which he/she was linked to The Company.
- b. Compliance with health and safety standards at work and implement the OH-SMS, and any other program, system and / or plan that seeks to protect the health of the employee in the workplace.
- c. Compliance of the legal duties derived from the employment relationship, such as: perform all necessary procedures for the registration of beneficiaries with the Social Security System, or any other activity derived from the applicable legislation.

Article 15. Children's and teenagers' personal data Processing

In the Processing of children's personal data, The Company will strictly observe the restrictions and duties established on Act 1581 of 2012, its regulatory decrees and other concordant norms. Therefore, in the case of Processing of children's personal data, The Company must:

- a. Perform Processing that answers and respects the best interests of the children and teenagers.
- b. Perform Processing that ensures the respect for the fundamental rights of children and teenagers.
- c. Evaluate the opinion of the child when he/she has the maturity, autonomy and capacity for understanding the matter related to the Processing of his/her personal data.

The Company will perform the Processing of the employees' children personal data of employees whose age are under 18 years. The Company must obtain authorization from the minor's representative, under the requirements set forth in Law 1581 of 2012 and its regulatory decrees. The purposes of the Processing performed by the Company on this kind of personal data are:

- a. Comply with the legal duties derived from the employment relationship, such as, perform all the necessary procedures for the beneficiaries' inscription on the Social Security System and other corresponding authorities;

CHAPTER V

PERSONAL DATA TRANSFER AND TRANSMISSION

Transfer and transmission of personal data that The Company makes to third parties located in or out the Colombian territory, must comply with the following:

Article 16. Personal Data Transfers to Responsible inside Colombian territory

When the personal data contained in The Company's Databases will be transferred to Responsible third parties located inside the Colombian territory, The Company must obtain authorization from the Holders to make the Transfer.

Article 17. Company's Personal Data Transfers to Officers located outside Colombian territory

Act 1581 of 2012 forbids international transfers of data to countries that does not provide the adequate levels of data protection, except when:

- a. Express and unequivocal authorization had been obtained by the Holder.
- b. If the case is related with an exchange of medical data, when it is required by the Holder's Processing for health reasons or public hygiene.
- c. If the case is related with banking or stock exchange transfers, according to the applicable legislation.
- d. If the case is related with Transfers in the context of international agreements in which Colombia participates, based on the principle of reciprocity.
- e. If the case is related with necessary Transfers for the execution of an agreement between the Holder and the Company, or for the execution of pre-contractual measures as long as it has the Holder's authorization;
- f. If the case is related with Transfers legally required for the safeguarding of the public interest, or for the recognition, exercise or defense of a right in a judicial process.

Through External Circular 005 of 2017, the SIC issued a list of with the countries that have adequate levels of protection of Personal Data. These countries are: Germany, Austria, Belgium, Bulgaria, Cyprus, Costa Rica, Croatia, Denmark, Slovakia, Slovenia, Estonia, Spain, United States, Finland, France, Greece, Hungary, Ireland, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, Mexico, Norway, the Netherlands, Peru, Poland, Portugal, the United Kingdom, the Czech Republic, the Republic of Korea, Romania, Serbia, Sweden, and Japan; and countries that have been declared with an adequate level of protection by the European Commission ("Countries with Appropriate Levels of Protection").

Transfers of Personal Data made to any of these countries, or those indicated by the SIC, are not forbidden. Otherwise, it must comply with was established on the External Circular 005 of 2017 issued by the SIC.



Article 18. Transmissions of The Company's Personal Data to parties in charge located inside or outside Colombian territory

The Company may perform the Transmission of Personal Data that has in its possession or even complete Databases to parties in charge located inside or outside of Colombia, as long as:

- a. Has obtained authorization from the Holders; or
- b. Has a Contract of Personal Data Transmission, in the terms established on article 25 of Decree 1377 of 2013.

CHAPTER VI

CONFIDENTIALITY IN THE PROCESSING OF PERSONAL DATA

Article 19. Confidentiality

All employees of The Company must keep the confidentiality of the Personal Data that is subject of Processing. All contracts that the Company performs with its employees or with third parties that will have access to the Personal Data contained in the Company's Databases, must contain a confidentiality clause regarding to Personal Data. The Personal Data may only be object of Processing for the purposes described in this Manual.

Any infraction to the confidentiality duties from the employees, will be considered as a violation of the Internal Work Regulation, and will be subject to the sanctions contained therein.

CHAPTER VII

PERSON OR AREA RESPONSIBLE FOR THE HANDLING OF REQUESTS, INQUIRIES AND COMPLAINTS

Article 20. Person or area responsible for the handling of requests, inquiries and complaints

The Company has appointed Security organization, or the person appointed by it as the responsible for looking after the fulfillment of this policy.

This person in charge will stay tuned to resolve requests, queries and complaints by the holders, and to perform any updating, rectification and deletion of personal data, through the electronic mail personaldataprivacy.colombia@nokia.com.

Article 21. Data of contact of the person in charge of the Processing of the Information

Name: Nokia Solutions and Networks Colombia Ltda.

Corresponding address: 72nd Street # 8 – 56 Floor 2

Email: personaldataprivacy.colombia@nokia.com

CHAPTER VIII

PROCEDURE FOR HANDLING QUERIES, CLAIMS AND REQUESTS

Article 22. Queries

In accordance with the provisions of article 14 of Act 1581 of 2012, the Holders or their assignees may consult the personal information of the Holder filed in databases managed by The Company.

The Holder of the information may request the query of his/her information in writing or by electronic means to the mail personaldataprivacy.colombia@nokia.com; in these cases, in order to protect the personal data, a copy of identity documents must be attached.

When the assignee (s) wish to consult the information, they must submit their request in writing or by electronic means, enclosing a document proving the relationship, together with the identity document.

If, after reviewing the documents submitted and the name of the Holder, it is found that there is agreement in them, a response will be given within a maximum term of ten (10) business days from the date of receipt of the query. In the event that The Company considers that it requires a longer time to respond to the query, it will inform the Holder of such a situation by stating the reasons for the delay and indicating the date on which the query will be handled, and the response will be given in a term that will not exceed five (5) business days following the expiration of the first term.

Article 23. Claims

In accordance with the provisions of article 15 of Act 1581 of 2012, the Holder or the assignees who consider that the information contained in a database should be corrected, updated or deleted, or when they notice an alleged non-fulfillment of any duty contained in the Act, they may file a claim with The Company, which will be processed pursuant to the following procedure:

1. The claim will be made to The Company or to the party in charge of the Processing, including the identification of the Holder, the description of the facts that give rise to the claim, the address, and the documents in question.
2. If the claim is incomplete, the concerned party will be required to remedy the deficiencies within five (5) days from the receipt of the claim.
3. After two (2) months from the date of the request, if the applicant does not submit the requested information, it will be understood that he/she has desisted from the claim.
4. If the person receiving the claim is not competent to solve it, then he/she will transfer it to the respective party in a maximum term of two (2) business days, and will inform the concerned party of the situation.



5. Once the complete claim has been received, a legend saying "claim in process" will be entered in the database along with the reason for it in a term no more than two (2) business days. This legend must be maintained until the claim has been settled.

6. The maximum term to handle the claim will be fifteen (15) business days from the day following the date of receipt. When it is not possible to deal with the claim within that term, the concerned party will be informed of the reasons for the delay and the date on which his/her claim will be handled, which in no case may exceed eight (8) business days following the expiration of the first term.

Article 24. Request for Updating, Rectification and Deletion of Data

The Company will rectify and update, at the request of the holder, the information that is incomplete or inaccurate, in accordance with the aforementioned procedure and terms, for which the holder may make his/her request in writing or by electronic means to the mail personaldataprivacy.colombia@nokia.com, indicating the update, rectification of the data and attaching the documentation that supports the request.

Article 25. Revocation of the Authorization and/or Deletion of the Data

The Holders of the personal data can revoke the consent to the processing of their personal data at any time, as long as it is not prevented by a legal or contractual provision, for which the holder may submit the revocation in writing or by electronic means to the mail personaldataprivacy.colombia@nokia.com.

If on the expiration of the respective legal term, The Company, as the case may be, has not deleted the personal data, the Holder will be entitled to request the Superintendence of Industry and Commerce to order the revocation of authorization and/or deletion of personal data. For these purposes, the procedure set forth in article 22 of Act 1581 of 2012 will be applied.

Article 26. Personal Data Preservation

The Company will collect the data that are strictly necessary to carry out the pursued purposes and will keep them to meet the needs that data have been registered for. Moreover, the Company will respect the freedom that the Holder has for authorizing or not the use of his/her personal data, and consequently, the mechanisms used to obtain the consent will allow the Holder to state clearly that he/she grants such authorization.

CHAPTER IX

INFORMATION SECURITY

Article 27. Security Measures

The Company will take the necessary technical, human and administrative measures in order to ensure the security of the personal data being processed, thus avoiding their unauthorized access or quest, adulteration or fraudulent use.



CHAPTER X

APPLICABLE REGULATIONS

Article 28. Referral and implementation of additional regulations

This Manual includes the provisions enshrined in Act 1581 of 2012, decree 1377 of 2013 and other rules that complement and/or add it. Likewise, Judgment C - 748 - 11 by the Constitutional Court will be part of this Manual and will serve for its interpretation.

CHAPTER XI

DATE OF ENTRY INTO FORCE OF THE MANUAL

Article 29. Entry into force

Our work team was informed of the substantial aspects of this Manual, as well as of the mandatory compliance of each and every one of the aspects that make up the same, and in accordance with the above, this Manual will begin to govern on September 1st, 2018. The databases subject to Processing shall remain in force as long as it may be necessary for the purposes determined in this Manual.