



**PERSONAL DATA PROTECTION POLICY
FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA -
CAFECERT**

REVIEW DATE:
2021/03/24

APPROVAL DATE:
2021/03/24

VERSION: 01

CODE: OPGD-D-014

I. GENERALITIES:

This document establishes the Personal Data Treatment Policy of THE FOUNDATION FOR THE CERTIFICATION OF CAFÉ DE COLOMBIA - CAFECERT (hereinafter, "CAFECERT "). This Policy describes the mechanisms by means of which CAFECERT guarantees an adequate handling of the Personal Data collected and processed in its Databases, for the Purposes described here, in order to allow the Owners of these the exercise of Habeas Data right.

II. RESPONSIBLE:

CAFECERT is a non-profit entity domiciled in Bogotá DC identified with NIT 900.799.907-9, its contact details are the following:

COMPANY NAME: FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA (*FUNDACION PARA LA CERTIFICACIÓN DEL CAFÉ DE COLOMBIA*) - CAFECERT

NIT: 900.799.907-9

ADDRESS: Calle 73 No. 8-13 Torre A, Piso 4, Bogotá DC, Colombia

PHONE: (+57) - 1 - 3136600 ext. 1345-1421 - (+57) - 1 - 3257421

WEBSITE: www.fundacioncafecert.org


III. CONTENT OF THE DATABASES:

General information such as full name, number and type of identification, gender, contact information (email, physical address, landline and / or mobile phone), and data associated with the profession or trade is stored in the CAFECERT databases. In addition to these, and depending on the nature of the Database and the labour or commercial relationship that CAFECERT has with the Data Owner, images, work and / or academic history can also be stored; Sensitive data such as union membership, health data, and biometric data (fingerprints) and information on minors.

The Processing of Personal Data mentioned above, that are not of a Public nature, will be conducted with the prior and express Authorization of the holders, in accordance with the Authorization criteria established in Law 1581 of 2012, Decree 1377 of 2013, and any other regulation that modifies or adds them.

IV. TREATMENT:

The Personal Data found in the CAFECERT Databases are subjected to different forms of Treatment, such as, collection, exchange, updating, processing, reproduction, compilation, storage, use, systematization, organization and elimination; all of them partially or totally in compliance with the applicable regulations and the Purposes established herein.

	PERSONAL DATA PROTECTION POLICY FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA - CAFECERT		
REVIEW DATE: 2021/03/24	APPROVAL DATE: 2021/03/24	VERSION: 01	CODE: OPGD-D-014

The Personal Data for which CAFECERT is the Responsible Party may be delivered, transmitted or transferred to public or private entities, including business partners and allies, contractors, parent companies, affiliates or subsidiaries, solely for the purpose of fulfilling the purposes established in this Policy. Likewise, Personal Data, including Sensitive Data, may be transferred or transmitted to third countries, observing the list of countries that offer an adequate level of data protection, published by the Superintendence of Industry and Commerce; making the declaration of conformity established by the Law, as well as the signing of Agreements or Contracts of transfer or transmission that promote the protection of the Personal Data object of transfer.

In any case, the delivery, transmission or transfer, will be made after signing the commitments that are necessary to safeguard the confidentiality of the information.

In compliance with legal duties, CAFECERT may provide personal information to judicial or administrative entities.

CAFECERT will ensure the correct use of Personal Data of minors, guaranteeing that the applicable legal requirements are met and that all treatment is previously authorized and justified in the best interests of minors.

V. PURPOSES:

A. CUSTOMER MANAGEMENT:

- Know their financial, commercial and credit behaviour and compliance with their legal obligations.
- Conduct all the necessary steps to confirm and update the client's information.
- Establish, maintain or terminate a commercial and / or contractual relationship.
- Offer and provide products or services through any means or channel of communication (including telephone, text message or instant messaging, email, among others).
- Receive information from CAFECERT regarding current and future commercial campaigns, promotion of products and services, both its own and those of third parties, and other communications necessary to keep the customer informed and informed through any means or channel of communication (including telephone, text message or instant messaging, email, among others).
- Receive messages related to collection management and portfolio recovery, either directly or through a third party hired for this function.
- Conduct an adequate provision and administration of the services of CAFECERT's corporate purpose.
- Conduct commercial, statistical, risk, market analysis and research, including contacting the client for these purposes.
- Prevent money laundering, terrorist financing, as well as detect fraud, corruption, and other illegal activities.
- Conduct satisfaction surveys concerning to the services provided by CAFECERT.
- Consult fines and sanctions before the different administrative and judicial authorities or public databases whose function is the administration of data of this nature.

B. SUPPLIER MANAGEMENT:

- Manage the supplier engagement process in accordance with CAFECERT's internal accounting, financial and commercial procedures.



**PERSONAL DATA PROTECTION POLICY
FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA -
CAFECERT**

REVIEW DATE: 2021/03/24	APPROVAL DATE: 2021/03/24	VERSION: 01	CODE: OPGD-D-014
-----------------------------------	-------------------------------------	--------------------	-------------------------

- Verify commercial and reputational records and the risks of money laundering, terrorist financing and illegal activities.
- Manage and strengthen commercial or contractual relationships with the supplier.
- Review and evaluate the supplier's results.
- Offer and provide products or services from CAFECERT or third parties, through any means or channel of communication (including telephone, text message or instant messaging, email, among others).
- Conduct commercial, statistical, risk and / or market analysis and research based on the supplier's results.

C. PERSONNEL MANAGEMENT:


- Conduct the entrance evaluation and the process of linking applicants.
- Management of existing labour relations with workers, or of the service provision relations of contractors and interns, as well as the development of the different activities established by CAFECERT. Among which we highlight the following:
 - To comply with the obligations and rights derived from their activity as an employer and with the activities of its main and related corporate purpose, which can be conducted directly or with the support of third parties with whom their information will be shared for related purposes with the object of the contract.
 - Share their personal data with national or foreign authorities (judicial or administrative) when the request is based on legal, procedural, and / or tax reasons.
 - Access and authorization of the benefits established by the employer, according to the requirements defined in each case.
 - Consult their data in the lists related to the Risk Management System for Money Laundering and Terrorism Financing - SARLAFT.
 - Deliver their information to employee funds and mutual investment funds to which they have authorized to know it.
- Comply with the obligations that may arise by virtue of the employment relationship that existed in accordance with Colombian law, or by virtue of the services that may be provided by virtue of the employment or commercial relationship with CAFECERT, as well as providing the required labour certifications that are requested by the former collaborator or by third parties against whom they conduct a selection process.

D. CORPORATE GOVERNANCE:

- To comply with the obligations and rights as associates, founders, members of the Board of Directors and / or of any CAFECERT Committee in accordance with Colombian legislation.
- Give access to the information of associates, founders, members of the Board of Directors and / or of any CAFECERT Committee to the judicial or administrative authorities that request said data in the exercise of their functions.
- Manage the risk of money laundering and financing of terrorism and commission of illegal activities.

E. VIDEO SURVEILLANCE SECURITY AND BUILDING ACCESS CONTROL:

- Having information on each worker, contractor and outsourced staff providing services to CAFECERT and on each visitor entering the premises of CAFECERT in the country.
- Control and identify access to CAFECERT facilities in the national territory.

	PERSONAL DATA PROTECTION POLICY FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA - CAFECERT		
	REVIEW DATE: 2021/03/24	APPROVAL DATE: 2021/03/24	VERSION: 01

- Maintain security and access control to CAFECERT facilities in the national territory.

VI. DURATION OF THE PROCESSING OF PERSONAL DATA:

The personal data will be processed by CAFECERT during the contractual or commercial term in which the holder of these has the service, contract or relationship, plus the term established by law, or until the authorization is revoked provided that said revocation complies with the established in this Policy.

VII. RIGHTS OF THE HOLDERS:

The natural persons whose Personal Data are processed by CAFECERT have the following rights, which they can exercise at any time:

- Know the Personal Data on which CAFECERT is conducting the Treatment.
- Request at any time that their data be updated or rectified, for example, if they find that their data is partial, inaccurate, incomplete, fractioned, misleading, or those on which said Treatment is expressly prohibited or has not been authorized.
- Request proof of the Authorization granted to CAFECERT for the Processing of their Personal Data.
- Be informed by CAFECERT, upon request, regarding the use that it has given to their Personal Data.
- Present before the Superintendence of Industry and Commerce complaints for infractions of the provisions of the Law.
- Request CAFECERT to delete their Personal Data and / or revoke the Authorization granted for the Treatment of these, by submitting a claim, in accordance with the procedures established in this Policy. Notwithstanding the foregoing, the request for the deletion of the information and the revocation of the Authorization will not proceed when the Holder of the information has a legal or contractual duty to remain in the Database and / or files, or while the relationship between the Holder and CAFECERT, by virtue of which their data was collected.
- Free access to their Personal Data that have been subject to Treatment.

The rights of the Holders may be exercised by the following persons:

- By the Holder;
- By their successors in title, who must prove such relation; or
- By the representative and / or attorney-in-fact of the Holder, prior accreditation of the representation or power of attorney.

VIII. CAFECERT OBLIGATIONS:

CAFECERT will use the Personal Data collected only for the Purposes for which it is duly empowered and for which the Holder has given his / her authorization, respecting, in any case, the Law, which establishes that he must:

- Guarantee the Holder, at all times, the full and effective exercise of the right to Habeas Data;
- Request and keep a copy of the respective authorization granted by the Holder, under the conditions set forth in the Law;
- Inform accurately and promptly the Holder about the Purpose of collecting their data and the rights that assist them by virtue of the Authorization granted;



**PERSONAL DATA PROTECTION POLICY
FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA -
CAFECERT**

REVIEW DATE: 2021/03/24	APPROVAL DATE: 2021/03/24	VERSION: 01	CODE: OPGD-D-014
-----------------------------------	-------------------------------------	--------------------	-------------------------

- Keep Personal Data under the security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access;
- Guarantee that the information provided to the Person in Charge is true, complete, exact, updated, verifiable and understandable;
- Update the information, communicating in a timely manner to the Person in Charge of Treatment, all the news regarding the data previously supplied to him, and adopt the other necessary measures so that the information supplied to him is kept up to date;
- Rectify the information when it is incorrect and communicate the pertinent to the Manager;
- Provide the Person in Charge, as the case may be, only data which Treatment is previously authorized in accordance with the provisions of the Law;
- Demand from the Person in Charge, at all times, to respect the security and privacy conditions of the Owner's information;
- Process the queries and claims formulated in the terms indicated in this Law;
- Adopt an internal manual of policies and procedures to guarantee adequate compliance with this Law and especially, for the attention of queries and complaints;
- Inform the Person in Charge when certain information is under discussion by the Holder, once the claim has been submitted and the respective procedure has not been completed;
- Inform at the request of the Owner about the use given to their data;
- Inform the data protection authority should any violations of the security codes or should any risks in the administration of the information of the Holders occur;
- Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

IX. PROCEDURES FOR PRESENTATION AND RESPONSE TO INQUIRIES, COMPLAINTS AND CLAIMS


Holders of Personal Data may conduct inquiries, complaints or claims (hereunder and altogether the "Applications") when required, through the mechanisms provided for this purpose in this Policy. The Requests made by the Holders must contain, at least, the following information:

- Identification of the Holder or of whoever is making the request, indicating name and identification number
- Clearly describe the reasons for the request, specifying the facts that have been presented.
- Prove the legitimate interest by which the person filing the claim acts and attach, if necessary, the corresponding supports
- Indicate the physical or electronic address and telephone number of the Holder or whoever is making the request to which the response must be notified and sent.
- Documentation that they would like to provide as evidence

A. INQUIRIES:

The Holders, their successors in title or any other person who has a legitimate interest, may request information regarding the Personal Data subject to Treatment, proof of the Authorization of Personal Data Treatment, or about the Use that is being given to Personal Data contained in any of the CAFECERT Databases.

Queries will be answered within a term of ten (10) business days from the date of receipt of the respective Request. When it is not possible to attend the query within said term, the interested party

	PERSONAL DATA PROTECTION POLICY FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA - CAFECERT		
	REVIEW DATE: 2021/03/24	APPROVAL DATE: 2021/03/24	VERSION: 01

will be informed, stating the reasons for the delay and indicating the date on which the query will be attended, which in no case may exceed five (5) business days following the expiration of the first term.

B. CLAIMS:

The Holders, their successors in title or any other person who has a legitimate interest, who requires or considers that the Personal Data should be updated, corrected or deleted or are subject to inappropriate Treatment or in contravention of the duties established in the applicable legislation, or Those who wish to revoke the Authorization for their Treatment, may file a claim following the requirements of article 15 of Law 1581 of 2012 and described in this document.

If the Claim is incomplete, the interested party will be required within five (5) days after receiving it to correct the faults. If after two (2) months from the date of the request, the applicant does not present the required information, it will be understood that he has withdrawn from the Claim.

Upon receipt of the full Claim, and within a term not exceeding two (2) business days, a caption stating "pending claim" will be included in the Database and the reason for this. Said caption must be kept until the claim is decided.

The maximum term to attend the claim will be fifteen (15) business days from the day following the date of receipt. When it is not possible to attend the Claim within said term, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case may exceed eight (8) business days following expiration. of the first term.

- a. **Deletion of Personal Data:** In case of requiring or requesting the partial or total deletion of personal data, CAFECERT will analyse the request to determine if the owner has any legal or contractual duty for which it is necessary for it to remain in the database and then proceed or not with the suppression of the data.
- b. **Revocation of the Authorization for the Processing of Personal Data:** The revocation of personal data will proceed in all cases, except in the event that the owner has a legal or contractual duty to remain in the database managed by CAFECERT.

X. SERVICE CHANNELS:

Any request, complaint or claim related to the Processing of Personal Data, in application of the provisions of the Law, may be sent via the following means, and will be processed by the Quality Management area of CAFECERT.

- A. **WEBSITE:** On the CAFECERT website, in the "CONTACT" section, selecting the service of interest "PERSONAL DATA" [https:// www. fundacioncafecert.org](https://www.fundacioncafecert.org)
- B. **EMAIL:** The holders of personal data can submit their requests for personal data to the electronic mail datos.personales@fundacioncafecert.org within the terms established by law.

	PERSONAL DATA PROTECTION POLICY FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA - CAFECERT		
	REVIEW DATE: 2021/03/24	APPROVAL DATE: 2021/03/24	VERSION: 01

XI. DEFINITIONS:

- **Authorization:** Prior, express and informed consent of the Holder to conduct the Processing of personal data.
- **Privacy Notice:** Verbal or written communication generated by the Treatment Manager, addressed to the Owner for the Treatment of their Personal Data, by means of which they are informed about the existence of the Information Treatment Policies that will be applicable, the way of accessing them and the purposes of the Treatment that is intended to give the Personal Data.
- **Database:** Organized set of Personal Data that is subject to Treatment.
- **Personal Data:** Any information linked or that may be associated with one or more specific or determinable natural persons.
- **Private or Intimate Personal Data:** Are those Personal Data that due to their intimate or reserved nature only interest the Holder of the information. For its Treatment, express authorization of the Holder is required. Examples of Private or Intimate Personal Data are: the stratum, level of education, location and contact data not associated with the profession or that are not found in public directories (telephone and home address), a photocopy of the identity card, consumer preferences, among others.
- **Public Personal Data:** Are those Personal Data that the regulations and the Constitution have expressly determined as public, and for whose collection and Treatment the Owner's Authorization is not necessary. They are generally contained in public records and documents. Examples of Public Personal Data, the marital status of people, their profession or trade, the data contained in duly executed judicial decisions that are not subject to reservation, business address and telephone, business email, among others.
- **Semi-private Personal Data:** These are Personal Data that are not intimate, reserved, but not public, whose knowledge or disclosure may interest not only the owner, but also a group of people or society in general. For its Treatment, the Express Authorization of the Holder is required. Examples of Semi-Private Personal Data are financial and credit information.
- **Sensitive Personal Data:** Are those Personal Data that affect the privacy of the Holder or whose improper use may generate discrimination. For its Treatment, express authorization from the Holder is required, where the treatment of Sensitive Data is specifically accepted and the option not to provide said Data is given. Examples of Sensitive Personal Data are those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of unions, social organizations, human rights or that promote the interests of any political party or that guarantee rights. and guarantees from opposition political parties, as well as data related to health, sexual life, and biometric data (fingerprints, iris, facial recognition), among others.
- **Person in charge:** Natural or legal person, public or private, who by himself or in association with others, carries out the Processing of personal data on behalf of the Person Responsible for Processing.
- **Law:** Statutory Law 1581 of 2012 "by which general provisions are issued for the protection of personal data"; Regulatory Decree 1377 of 2013 "that partially regulates Law 1581 of 2012" (Compiled in Decree 1074 of 2015); and any rule that replaces or modifies them.
- **Responsible:** Natural or legal person, public or private, who by itself or in association with others, decides on the database and / or the Processing of the data.
- **Owner:** Natural person whose Personal Data are subject to Treatment.
- **Transfer:** It is the Treatment of Personal Data that implies the communication of the same within or outside the territory of the Republic of Colombia when it is intended to conduct a Treatment by the Person in Charge on behalf of the Responsible.
- **Transmission:** It is the Personal Data Processing activity through which they are communicated, internally or with third parties, within or outside the territory of the Republic of Colombia, when said communication is intended to conduct any Processing activity by the recipient of the Personal Data.

	PERSONAL DATA PROTECTION POLICY FOUNDATION FOR THE CERTIFICATION OF COFFEE OF COLOMBIA - CAFECERT		
REVIEW DATE: 2021/03/24	APPROVAL DATE: 2021/03/24	VERSION: 01	CODE: OPGD-D-014

- **Treatment:** Any operation or set of operations on Personal Data, such as: the collection, storage, use, circulation or deletion.

XII. PRINCIPLES

- **Principle of legality:** The Processing of Personal Data is a regulated activity that must be subject to the provisions of the Law and the other provisions that develop it.
- **Principle of purpose:** The Treatment must obey a legitimate purpose in accordance with the Constitution and the Law, which must be informed to the Holder.
- **Principle of freedom:** Treatment 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 that relieves consent.
- **Principle of truthfulness or quality:** The information subject to Treatment must be truthful, complete, exact, updated, verifiable and understandable. Processing of partial, incomplete, fractional or misleading data is prohibited.
- **Principle of transparency:** In the Treatment, the right of the Holder to obtain from the Treatment Manager or the Treatment Manager, at any time and without restrictions, information about the existence of data that concerns him or her must be guaranteed.
- **Principle of access and restricted circulation:** Treatment is subject to the limits derived from the nature of the Personal Data, the provisions of the Law and the Constitution. In this sense, the Treatment may only be done by persons authorized by the Holder and / or by the persons provided for in the Law. Personal Data, except for public information, may not be available on the Internet or other means of dissemination or mass communication, unless the access is technically controllable to provide restricted knowledge only to the Holders or authorized third parties in accordance with the Law.
- **Principle of security:** The information subject to Treatment by the Person in Charge of Treatment or Person in Charge of Treatment must be handled with the technical, human and administrative measures that are necessary to provide security to the records avoiding their adulteration, loss, consultation, use or access unauthorized or fraudulent.
- **Principle of confidentiality:** All persons who intervene in the Processing of Personal Data that are not public are obliged to guarantee the reservation of the information, even after the end of their relationship with any of the tasks that the Treatment comprises, being able to only perform supply or communication of Personal Data when this corresponds to the development of the activities authorized by the Law and in the terms of this.

XIII. VALIDITY

CAFECERT's Personal Data Processing Policy has been in force since March 2021. CAFECERT reserves the right to modify them under the terms and within the limitations provided by Law.