



FUNDACIÓN CLIMÁTICA IRIS, UNIDOS POR EL CLIMA

POLICY ON PERSONAL DATA PRIVACY

## Content

Context.....	3
Objectives.....	4
Scope.....	5
Responsibility.....	5
Principles and definitions.....	6
Consent and sensitive personal data.....	8
Sensitive data.....	8
On the personal data retention regime.....	9
Personal data processing .....	9
Obligations in personal data processing .....	10
Processing of personal data from images and voice obtained through the use of security cameras or any other device .....	10
Non-compliance with the provisions relating to the protection of personal data.....	11
National and international transfer of personal data.....	11
Security and protection of personal data in electronic format.....	12
Use of personal data.....	14
Purpose and use of personal data.....	15
Availability and modifications to the privacy policy.....	15

## CONTEXT

Technological advances, and especially the digital environment, impact people's economic, political, and social lives, particularly their enjoyment of their rights, which is reflected in our society.

A new horizon in business models, personalized services and products, and engagement models are converging in the physical and digital worlds, shaping an ecosystem whose dynamics and economic and social impacts are constantly evolving through the large-scale use of technologies. Therefore, these ecosystems are not immune to unexpected attacks in terms of surveillance and privacy.

Constitutional precepts establish that human dignity is the supreme value that underpins the recognition and exercise of the rights and duties enshrined therein, and that all persons have the right to respect for their personal and family privacy, their own image and voice, their honor and personal identity.

It is also recognized that every person has the right to access their personal data in records, files, or other databases and information of a public nature, as well as to request its non-disclosure and obtain its proper correction, rectification, modification, updating, or cancellation, and to ensure that the use and processing of this data is carried out in accordance with the law.

The existence of records, files, databases, or other means of a public or private, physical or digital nature, through which personal information is stored, processed, provided, and used, as well as free access to this data, may violate the rights of the data owner and other related rights if not properly regulated.

Considering the above, in Cuba, the regulatory provision guaranteeing the right of individuals to the protection of their personal data was approved, regulating the use and processing of such

data by public and private individuals or entities, as well as of public information, and contributing to promote, foster, and disseminate a culture of data protection in society at large. This regulatory provision is **LAW No. 149 ON THE PROTECTION OF PERSONAL DATA**, dated **May 14, 2022**, and **RESOLUTION 58/2022, REGULATIONS FOR THE SECURITY AND PROTECTION OF PERSONAL DATA IN ELECTRONIC MEDIA**.

We, the Fundación Climática IRIS, Unidos por el Clima (hereinafter, the Foundation), are strongly committed to achieving a safer Internet against both illegitimate invasions of privacy and legitimate ones without guarantees. Within this framework, we have decided to move forward with the development of a privacy policy that generates complete consistency between our external actions and our internal practices.

This policy aims to incorporate standards and good practices to provide a framework for the use of personal data of all persons linked to the Foundation.

It seeks to protect, preserve and objectively manage the Foundation's information, against internal or external threats, whether deliberate or accidental, to ensure compliance with the confidentiality, integrity, availability, legality, and non-repudiation characteristics of information.

## OBJECTIVES

Consequently, in accordance with the legal provisions, the Foundation:

1. Establishes the fundamental principles, procedures and definitions to guarantee every natural person linked to it the right to the protection of their personal data contained in records, files, archives, databases or other technical means of data processing, whether physical or digital, public or private, installed in its premises;
2. ensures due respect for personal and family privacy, the image and voice, honor and personal identity of every natural person linked to it;

3. regulates the use and effective processing of personal data and public information, holding those responsible for managing this information accountable;
4. strives to contribute to promoting, fostering and disseminating a culture of protection in society;
5. establishes that the owners of application of this procedure are natural persons and legal entities linked to the Foundation, regarding their data;
6. states that personal data is considered to be information concerning a natural person, identified or identifiable, that can lead to their identity (a person is identifiable when their identity can be determined directly or indirectly through any information).

## SCOPE

The Foundation will protect the personal data of people linked to it, related to sex, age, image, voice, gender, identity, gender identity, sexual orientation, skin color; ethnic, national and territorial origin; migratory status and classification; disability status, religious beliefs, political affiliation, marital status, address, medical or health data; economic-financial, academic and training, professional and employment, judicial and administrative data, and any information related to this data, which can lead to the identification of a specific person, collected from records, files, archives, and databases, as established by law.

## RESPONSIBILITY

The responsibility for this activity falls on the administrative body, as records, files, archives and/or databases will be created, whether electronic or not, to maintain the organized set of personal data that are subject to processing (regardless of the method of their formation, storage, organization and access).

The processing of personal data consists of systematic operations and procedures, whether electronic or not, that allow for the collection, preservation, organization, storage, modification, correlation, evaluation, blocking, destruction, and, in general, the processing of personal data, as well as its transfer to third parties through communications, consultations, interconnections, and transfers.

## PRINCIPLES and DEFINITIONS

In accordance with the aforementioned Law 149/2022, the Foundation's Personal Data Privacy Policy is governed by the following principles:

- a) **Limitation of collection:** the collection and storage of information that may lead to the identification of a specific person must be limited to what is relevant and strictly necessary for the required purpose, adjusted to a specific, lawful and explicit objective, and kept only for the time required in accordance with that purpose;
- b) **data quality:** the personal data obtained, stored and processed must be truthful, exact, complete, correct and up-to-date, provided by the owner, without using unfair or fraudulent means to obtain them. They will remain in that form until the owner states and proves the need for its rectification, modification, updating or cancellation;
- c) **specification of purposes:** the specific purposes for obtaining, storing and technically processing any type of personal data must be made known to the data owner in advance, accurately, in a comprehensible and relevant manner;
- d) **limitation of use:** the personal data obtained, stored and processed may only be used for the specific and lawful purpose that was informed to the owner, and by natural or legal persons, or other entities authorized by the latter;

e) **legitimacy**: only bodies, agencies, entities and natural or legal persons are entitled to obtain, store and process personal data when they have authorization to create archives, in accordance with their functions or the activities they carry out, as regulated by the legislation in force for such purposes;

f) **safeguarding security**: natural or legal persons responsible for archives containing personal data are obliged to safeguard their security and guarantee, with the corresponding technological, administrative, material or physical measures, that only they or authorized personnel, where applicable, access or process such data using the established procedures;

g) **transparency of information**: the person responsible for and in charge of personal data archives guarantees the data owner the right to access the files for the purpose of verifying, rectifying, updating, erasing, or objecting to them. Archives must also be suitable for inspection or review by the competent authority;

h) **individual participation**: personal data may only be obtained with the individual participation of its owner, as an expression of respect for their right to identity, privacy, honor, image and voice;

i) **responsibility**: natural or legal persons responsible for obtaining, storing and processing personal data in records, files, archives and databases are accountable for their lawful use for the purposes informed to their owner, guaranteeing their security;

j) **legality**: the possession and processing of personal data is for lawful purposes only; those responsible for records, files, archives, and databases must comply with the provisions of the relevant regulations in their actions;

k) **degrees of confidentiality of information:** personal data provided to records, files, archives and databases are confidential and may only be accessed by the owner or a person with a proven legitimate interest; and

l) **consent:** the data owner must freely, unequivocally, specifically and in an informed manner express their wishes regarding the processing of personal data, specifying the purpose for which consent is granted.

## DEVELOPMENT

### 1.1 Consent and sensitive personal data

1.1.1. The person processing personal data must have the consent of the data owner, except in the exceptional cases provided for by law.

1.1.2. Consent may be expressed when stated verbally, in writing, or by any comparable means; or tacit when, once the data owner has been informed of the purposes for processing their data, they do not express their will to the contrary.

1.1.3. Persons with disabilities themselves provide their consent for the collection, storage, and processing of their personal data, assisted by the support required, where appropriate, to exercise their legal capacity, and use the suitable personal and technical means.

### 1.2 Sensitive data

1.2.1. Personal information whose misuse may lead to discrimination, imply a distinction harmful to human dignity, or pose a serious risk to its owner.

1.2.2. Sensitive data includes, among others, data that may reveal **sex, gender, identity, gender identity, sexual orientation, ethnic origin and skin color**, current or future health status, **disability status, religious beliefs, political affiliation, police and criminal records**.



1.2.3. A person cannot be forced to provide sensitive personal data, nor is it lawful to process it without the express, unequivocal, free, and informed consent of its owner.

### 1.3. On the personal data retention regime

1.3.1. The personal data retention regime complies with the applicable provisions in the relevant area and takes into account legal, administrative, historical, and other aspects.

1.3.2. The conservation regime may not exceed the deadlines for the fulfillment of the purposes that justify data treatment.

1.3.3. Personal data that have fulfilled the purposes for which they were processed in accordance with applicable provisions are deleted, ex officio or at the request of the owner of the physical or digital records, files, archives, and databases, or other technical means of data processing in which they are stored, once the retention period has concluded.

1.3.4. The retention period is up to five years, as long as a different term is not provided for by law or the owner consents to another period.

### 1.4. Personal data processing

1.4.1. Personal data control through records, files, archives and/or databases collects the following information:

1. Name and surname, ID number, and legal address of the natural person responsible for collecting the data and other information agreed upon by both parties.
2. In the case of a legal entity, the data that identifies it and other information agreed on by both parties.
3. Identification of the individuals with access to information processing; data retention period; and the manner and conditions under which individuals with a legitimate

interest may access the collected data for rectification, correction, modification, updating, deletion, or objection to it.

**1.4.2.** The Foundation, in accordance with the provisions of the Law, declares the existence of its personal data record, file, archive, or database to its Council of Government, and notifies to said Council of any changes to the information recorded, thereby ensuring the transparency and legal security of these databases against third parties.

### **1.5. Obligations in personal data processing**

**1.5.1.** The Foundation's governing body, responsible and in charge of personal data processing, guarantees the material, technical, and organizational conditions, adopts data security measures, and prevents unauthorized alteration, loss, processing, or access. It also promotes communication and legal education activities on personal data protection and, under no circumstances, processes personal data of any nature other than for the purposes stated by the Foundation.

### **1.6. Processing of personal data from images and voice obtained through the use of security cameras or any other device**

**1.6.1.** The Foundation assumes that personal data such as images and voices, when captured by video cameras or any other device that allows recording, may in no case cause any violation of the rights and guarantees recognized in the Constitution and the Law.

**1.6.2.** The installation of the devices described in the previous section is justified only if the purpose is legitimate, the presence of these devices is reported, and/or identifiers are placed in the areas where they are located, provided that no other means can be used; furthermore, they cannot be used for purposes other than those for which they were intended.

## 1.7. Non-compliance with the provisions relating to the protection of personal data

1.7.1. Failure to comply with the provisions of this policy and the legislation for these purposes will be dealt with in accordance with Cuban law.

## 1.8. National and international transfer of personal data

1.8.1. The transfer of personal data within the national territory is authorized, at the request of those responsible for or in charge of data processing, in the following cases:

1. Exchange of investigative data when required for processing by the owner or for collective interest;
2. when data transfer is for the general welfare;
3. bank transfers regarding the respective transactions;
4. to facilitate the exercise of the right to vote in the Foundation's own elections; and for other reasons that significantly warrant and are approved by its Board of Directors.

1.8.2. The governing body is responsible for authorizing the transfer within the scope of its powers, complying with the principles established in this policy.

1.8.3. International data transfer, at the request of the responsible authority of the receiving country, is permitted in the following cases:

1. International collaboration;
2. exchange of medical data when required for the treatment of the data owner, and an epidemiological investigation, provided that this is carried out after adopting a procedure for dissociating the information, so that the data owner is unidentifiable;
3. bank or stock exchange transfers in relation to the respective transactions and in accordance with applicable legislation;

4. when the transfer has been agreed within the framework of current international legal instruments to which the Foundation is a party; and
5. when the transfer of data is for the purpose of lawful international cooperation.

**1.8.4.** In order to authorize the international transfer of data, the Board of Directors will take into account the nature of the data requested, the purposes for which they are used, the consent or information given to the data owners when required, the duration of the processing to which they are subjected or planned, the country of origin and final destination of the information, applicable general or special legal regulations, applicable specific professional regulations, and technical and organizational security measures in force in the destination countries.

## **1.9 Security and protection of personal data in electronic format**

**1.9.1.** The processing of personal data in electronic format is considered to be the systematic operations and procedures that allow the collection, conservation, organization, storage, modification, correlation, evaluation, blocking, destruction and, in general, the processing of personal data, as well as its transfer to third parties through communications, consultations, interconnections and transfers, when they are carried out.

**1.9.2.** The governing body, together with the IT security officer, must be responsible for and in charge of the registry, file, archive, and/or database, and as such they must:

- a) guarantee the security and protection of personal data in electronic format;
- b) establish the necessary technical and administrative measures to ensure the processing of personal data in electronic format, in accordance with the provisions of the Law and other current regulations; and
- c) notify the competent authorities of the occurrence of cybersecurity incidents concerning personal data in electronic format under their custody.

**1.9.3.** The administrative body, as the entity responsible for and in charge of the registry, file, archive, and/or database, is the only entity authorized to manage computer programs or applications related to databases containing personal data in electronic format.

**1.9.4.** The administrative body, as the entity responsible for and in charge of the registry, file, archive and/or database, has the following obligations:

a) create the means for the owner of personal data in electronic format, their support or legal representative to access, modify and cancel the data at the time they deem appropriate, with the greatest possible brevity and transparency;

b) establish the cancellation of personal data in electronic format at the request of its owner, their support or legal representative, or when the purpose for which it was collected has been fulfilled, provided that this does not violate the provisions of a specific law or that it requires its conservation for legal, administrative, historical or other reasons, and adopt the necessary technical measures for the elimination of any link to this data and copy;

c) define the terms and conditions regarding the use of personal data in electronic format, which must be understandable to any user, and establish the ways for them to confirm their approval in accordance with the characteristics of the database and the service;

d) maintain the confidentiality and integrity of personal data in electronic format and prevent unauthorized access, modification or transfer; and

e) ensure the backup of personal data in electronic format.

**1.9.5.** The persons responsible for and in charge of the security and protection of personal data in electronic format may only host or replicate electronic records, files, archives, and databases containing personal data on national servers located within the country, except in cases provided for by law.

#### 1.10. Use of personal data:

1.10.1. Personal data in electronic format may be used for academic, research, or social purposes, and includes the minimum data necessary to fulfill its purpose, without commercial interest.

1.10.2. The exchange of information to achieve these objectives must be carried out contractually and comply with current legislation.

1.10.3. Data owners linked to the Foundation have the following rights:

- a) know the purpose for which their data is requested and the use that is given to it;
- b) access, update and cancel, at any time they deem appropriate, the personal data provided for the use of the service;
- c) that their data be deleted when they deem it appropriate, once the purpose for which they were collected has been fulfilled, or when they consider that they are being processed in a way that violates their interests and rights; and
- d) be informed about the privacy settings available that allow them to determine how their information is processed, shared and stored.

##### 1.10.3.1. Purpose and Use of Personal Data

Data obtained by the Foundation are treated as strictly confidential, except in the case of judicial questioning, and with the necessary security measures to guarantee their protection. Therefore, we will request the consent of the individuals in order to also use them to:

- identify them as allies, investors, etc.
- contact them and send them relevant information about our activities,
- respond to requests for information, attention and activities,

- contact them and send them newsletters about achievements and events organized by the Foundation, or third parties that are allies or investment partners,
- other purposes identified that benefit both parties in a lawful manner.

## 2. AVAILABILITY AND CHANGES TO THE PRIVACY POLICY

2.1. Upon implementation of this policy, an email will be sent to the founding partners informing them of this Privacy Policy and requesting their consent.

2.2. If data owners do not agree that their personal data be used for the purposes mentioned above, they will send an email stating their preferences.

2.3. The Foundation reserves the right to amend or modify the Data Privacy Policy as it deems appropriate, to comply with legislative changes regarding personal data protection or with internal provisions.

2.4. The Foundation will make this policy available to natural or legal persons, national or foreign, whenever necessary.

2.5. This Policy will be available on our website <http://www.fundacioniris.cu/> in the Privacy Policies section.

*This document will be reviewed and updated in accordance with the legal framework and the context in which the Foundation's activities are carried out.*

***Ms. Odalys Aldana Mazorra***  
***President***