Inter-American Institute for
Cooperation on Agriculture

Personal Data Protection Policy

November, 2020

Table of Contents

1. Foreword

This Policy responds to current needs, best practices and international standards on the processing of personal data. Its purpose is to strengthen institutional control mechanisms as well as foster a transparent and adequate use of the personal data of individuals tied to the Institute, in fulfillment of the Institute's mission. To this end, a series of guidelines have been developed.

2. Regulatory framework

This Policy is based on international frameworks as well as other institutional policies, namely:

a. IICA Information Disclosure Policy dated February 2020, whose Article V. Standard of Disclosure and Exceptions, point 5, establishes the information that is exempt from disclosure.

b. Policy on the Protection of Whistleblowers and Witnesses, dated July 2019, whose Article VII. Anonymity and Confidentiality for Whistleblowers and Witnesses, establishes the confidentiality of personal data provided by whistleblowers as far as possible, based on the legitimate needs of the investigation.

3. Applicability and scope

This Policy applies to all individuals who are directly tied to IICA, including staff members, consultants, interns, suppliers, associate personnel, counterparts and strategic partners, among others, in all Member States and at Headquarters, with whom the Institute cooperates to fulfill its mission.

4. Objective

Establish mechanisms for the processing and protection of personal data, with a view to guaranteeing and protecting the rights of individuals who are tied to the Institute, under the principles of transparency, security and respect.

5. Definitions

a. Personal Data: Any information related to an individual who can be identified from that data and other information; or by any means that could reasonably be used in connection with such data. Personal data includes biographical data (biodata), such as name, sex, marital status, date and place of birth, country of origin, country of asylum, individual registration number, occupation, religion and ethnicity; biometric data such as a photograph, fingerprint, facial or iris image; as well as any written expression of opinion about the individual, such as assessments of his or her specific status and/or needs.

b. Private personal data: Data that is only relevant to the data subject because of its private or personal nature.

c. Sensitive personal data: Data that affect the privacy of the data subject or whose misuse may lead to discrimination, including aspects related to racial or ethnic origin, political and sexual orientation, religious beliefs and any other data deemed sensitive.

d. **Public data:** Data that is not private, semi-private or sensitive. Data related to the marital status of individuals, their profession or trade are considered public data.

e. **Data subject:** An individual whose data is subject to processing (internal personnel, clients, suppliers).

f. **Authorization to use personal data:** Informed, written statement by the data subject in which he or she agrees to the use of personal data relating to him or her, in order to legitimize the data processing. This statement allows for ensuring that the data subject is aware of all of the ways in which the information that he or she provides will be utilized.

g. **Consent:** A written and express statement in which the data subject agrees to the processing of his or her personal data. Consent may also be provided orally, by means of an affirmative action that has been duly recorded.

h. **Privacy notice:** Written or verbal communication verified by the person responsible for data processing, to inform the data subject about the application of the Information Processing Policy established by the organization.

i. **Data file:** Structured set of personal data. The provisions on data protection and data processing shall not apply in the case of data files for internal use.

j. **Data processor:** An individual or public or private legal entity that has been designated by the corresponding individual to process data, either individually or through others.

k. **Processing of personal data:** Any operation or series of operations, automated or not, that is performed on personal data, including but not limited to the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, transfer (whether in computerized, oral or written form), dissemination or otherwise making available, correction or destruction.

l. **Personal data breach:** A breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed.

m. **Third party:** Any natural or legal person other than the data subject or IICA. Some examples of third parties are national governments, international governmental or non-governmental organizations, private sector entities or individuals.

6. Processing of personal data by IICA

Personal data is, by definition, classified as confidential. The Institute and its staff must respect the confidentiality of personal data at all times when processing personal data. To ensure that this confidentiality is respected, personal data must be archived and stored in such a way that it is

accessible only to authorized personnel and transferred only through the use of protected means of communication. The Institute will therefore guarantee data protection by:

a. Maintaining the physical security of its facilities, portable equipment, individual case files and records.

b. Maintaining the security of equipment and information technologies, access control (e.g., passwords, tiered access), user control, storage control, entry control, communication and transportation control (e.g., encryption).

c. Ensuring that, under deteriorating security conditions that generate a serious risk of personal data breaches, all necessary and possible measures are undertaken to prevent personal data breaches, by relocating or, as a last resort, destroying individual files containing personal data, whether on paper or in digital format, to prevent any damage to data subjects.

6.1. Principles of personal data processing

IICA shall carry out data processing based on the following principles:

a. Legitimate and fair processing: Processing of personal data must be carried out in accordance with legitimate purposes and not further processed in a manner that is incompatible with those purposes.

b. Purpose specification: Personal data will be collected for one or more specific purpose(s).

c. Necessity and proportionality: Data that is processed should be adequate and relevant to the identified purpose, and not exceed that purpose.

d. Precision: Personal data should be recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed.

e. Respect for the data subject's rights: Individuals shall be informed of the purpose for which the data will be processed, how the data will be utilized, whether such data will be transferred, and the importance of the data subject providing accurate and complete information.

f. Confidentiality: The confidentiality of the personal data of persons of concern shall be maintained at all times, even after a data subject is no longer tied to the Institute.

g. Security: The Institute shall implement security measures in its procedures and through technological means to guarantee the security of personal data.

h. Relevance: Personal data must be kept up to date. The person in charge of the data file will delete data that is no longer relevant or necessary, based on the purpose for which such data was received and recorded. Under no circumstances shall personal data that could affect the data subject in any way be kept more than ten years since the occurrence of the recorded events, unless otherwise provided for by special regulations. Should it be necessary to store such data beyond this period, the data must be disassociated from the data subject.

i. **Truthfulness**: Personal data must be truthful. The person responsible must modify or delete any data that is not truthful. Likewise, he or she shall ensure that the data is processed in a fair and lawful manner.

6.2. Rights of the data subject

a. **The right to be informed:** Data subjects whose personal data are requested must be previously, explicitly, precisely and unambiguously informed of the following:

- the existence of a personal data file;
- the purpose thereof;
- the recipients of the information, as well as those who may consult this information;
- the obligatory or optional nature of their response to the questions asked during the data collection process;
- the manner in which the requested data will be utilized;
- the consequences of refusing to provide the data; and
- the possibility of exercising his or her rights.
- Where questionnaires or other means of collecting personal data are utilized, these warnings shall appear in a clearly legible form.

b. **The right to provide consent:** The person collecting personal data must obtain explicit consent from the data subject or his or her representative. This consent must be provided in writing, either by means of a physical or electronic document, which may be revoked at any time with no retroactive effect. Consent may also be provided by means of an oral statement expressing an affirmative action, which must be duly recorded.

Express consent is not required in the case of the following exceptions:

- There is a reasoned order issued by a competent judicial authority, or an agreement adopted by a special research committee of the legislative body in the performance of its duties.
- Access to the personal data is unrestricted and can be consulted on sources that are available to the general public (i.e., public data).
- Data must be provided as a result of a constitutional or legal provision.

- The collection of data without the informed consent of the data subject, or the collection of data by means of fraudulent, unfair or illegal means is prohibited.

6.3. Notification of a personal data breach:

Institute staff must immediately notify the Representative and Administrator at the corresponding IICA Delegation and the Director of Corporate Services **when the risk of a personal data breach has been identified**. If the personal data breach could be detrimental to a data subject, the person responsible at the corresponding Delegation and at Headquarters must inform the data subject so that he or she may take any necessary precautions; if the data breach occurs at an IICA Delegation, the Director of Corporate Services must also be informed.

This notification must describe the nature of the personal data breach, potential and actual consequences, and the measures taken or proposed to mitigate its possible adverse effects.

6.4. Transfer of personal data to a third party:

The Institute may transfer personal data to a third party, provided that it ensures an adequate level of data protection (equal to or similar to the level provided by this Policy).

Taking into account possible data protection risks involved in transfers to third parties, the third party must bear in mind the principles indicated in section 6.1. of this Policy.

Prior to transferring personal data to a third party, IICA, through the Administrators in the Delegations, and the Director of Corporate Services or whomever he designates, and with support from the Legal, International Affairs and Protocol Unit, must ensure that such data is protected by means of an agreement, a confidentiality clause or other measures to guarantee data protection.

6.5. General information:

a. To ensure that the institutions, organizations, consultants and suppliers, among others, that engage in cooperation activities with the Institute or that provide services to the Institute, comply with the contents of this Policy, all legal instruments that establish any relationship with IICA must include the following clause to guarantee compliance:

   "All IICA counterparts that engage in cooperation activities with the Institute or that provide services to the Institute are aware of and agree to comply with the Institute's Personal Data Protection Policy".

b. Furthermore, to contribute to the fulfillment of this Policy, the attached Declaration must form part of the supporting documents for the procurement of goods and services or the contracting of personnel.

c. No provision included in this Policy or related to it shall be considered an express or tacit renunciation of the immunities, privileges, exonerations and benefits enjoyed by the Institute

and/or its personnel, in accordance with international law, international treaties and conventions or the national legislation of its member countries.

7. Responsibilities

Implementation of and compliance with this Policy is the responsibility of all members and employees of the Institute. Directors and managers of IICA have the responsibility of ensuring that all persons related to the activities of the Institute are aware of the content of the Policy and agree to adhere to it.

The Administrators at the Delegations and Director of Corporate Services shall be responsible for ensuring compliance with this Policy. The Internal Audit Unit will conduct annual assessments of the implementation of this Policy and issue recommendations to the Director General and the Director of Corporate Services.

8. Complaints

Staff members, consultants, interns, suppliers, associate personnel, counterparts or strategic partners, among others, who identify a personal data breach may inform the Institute through the channels it has established for the receipt and processing of complaints. Individuals may confidentially submit their complaints regarding the issues covered by this Policy:

a. via IICA's Intranet site at www.iica.int, under the REPORTS/COMPLAINTS section and

b. via email at ec.ce@iica.int

All complaints, claims, investigations, reports and information in this regard shall be objectively examined and analyzed by the Institute's Ethics Committee, which will define how to address the topic, disciplinary measures and corresponding actions.

9. Publication

This Policy will be available in the institutional repository, on the Institute's website, as well as on the Institute's Intranet.

10. Review and adjustments

The Director of Corporate Services, or whomever he designates, shall be responsible for keeping the contents of this Policy up to date, in accordance with the highest international standards on this topic, as it relates to the Institute's work.

11. Validity:

This Policy will enter into force on the date that is announced by the Director General.

Annex: Declaration

In keeping with the provisions of the Personal Data Protection Policy of the Inter-American Institute for Cooperation on Agriculture, namely point 6.5. General Information, paragraph b, the following declaration must be signed:

- I have been explicitly informed that the data provided to IICA will be processed and managed internally, as well as stored for follow-up in an IICA database.

- I understand that this information will be used solely for the abovementioned purposes and that I will be duly informed of any changes in this regard via the agreed-upon communication channels. Likewise, I undertake a direct commitment to inform IICA of any changes to these conditions and accept that failure to do so will release IICA from any responsibility regarding the accuracy of these conditions.

IICA confirms that its database is managed in a decentralized manner and that, upon request, the Institute can provide further details regarding the personal data that is stored in the database. Such requests must be made via a signed note, which must be emailed to xxxx@iica.int[1].

In agreement with the foregoing, I sign in XXXXXXXX on XXXXXXXXXXXXX.

Name:

ID:

Signature:

Authorized email address for correspondence:

[1] Each IICA Delegation in a member country must indicate its official email address. In the case of Headquarters, the address is XXXX.