Inter-American Institute for Cooperation on Agriculture

Personal Data Protection Policy

January 2023

Index

PERSONAL DATA PROTECTION POLICY

I. Foreword

This Policy was developed in accordance with the current global context, international best practices and standards on personal data processing, with a view to strengthening institutional control mechanisms and fostering transparent and proper use of the personal data of individuals collaborating with the Institute to fulfill its mission.

II. Regulatory framework

The Inter-American Institute for Cooperation on Agriculture (IICA) is committed to ensuring compliance with personal data protection, and thus this Policy adheres to international standards and complements other institutional regulatory guidelines. From an operational perspective, the Policy will be implemented by way of IICA's Procedural Manual on Personal Data Protection (hereinafter referred to as the PMPDP).

III. Applicability and scope

This Policy applies to all individuals who have a direct involvement with IICA, including employees, consultants, interns, suppliers, associate personnel, counterparts and strategic partners, among others, in all Member States and at Headquarters, with whom the Institute is collaborating to fulfill its mission. Application of this Policy is the responsibility of all staff Members at the Institute and compliance is mandatory.

IV. Objective

To establish mechanisms for personal data processing and protection, so as to guarantee and protect the rights of legal entities or individuals that are collaborating with the Institute, in keeping with the principles established in international standards on this issue and with institutional values.

V. Definitions

1. **Authorization to use personal data:** informed, written statement in which the data subject agrees to the use and by extension the processing of his/her personal data. This statement serves as confirmation that the data subject is aware of all of the ways in which the information provided will be utilized.

2. **Privacy notice**: a statement issued by the data controller to inform the data subject about the application of the information processing policy established within the organization.

3. **Database**: organized system that stores and systematizes personal data.

4. **Lawful basis**: list of specific situations or circumstances in which personal data may be processed. In other words, this establishes a rule that stipulates that the data controller cannot simply process data at will, but only when empowered to do so. Therefore, personal data may only be processed when there is a lawful basis (that is, when one of the legally established situations arises).

5. **Consent**: a written and express statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, by means of an affirmative action that has been duly recorded.

6. **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 genetic and biographical data (biodata), such as name, gender, 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/her specific status and/or needs.

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

8. **Sensitive personal data**: personal data that indicates ethnic origin or race, political opinions, religious or philosophical convictions, trade union affiliations, as well as the processing of genetic personal data, biometric data aimed at unequivocally identifying an individual, health-related data or data related to the sex life or sexual orientation of an individual.

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

10. **Personal Data Protection Management Team or Data Protection Officer**: members of staff who are responsible for coordinating, developing the necessary actions and providing guidance on the implementation of the Personal Data Protection Policy and on IICA's Procedural Manual on Personal Data Protection, as well as ensuring the sustainability of this institutional process.

11. **Legitimate Interest**: Interest of the data controller or of third parties that justifies the processing of the personal data, without the consent of the data subject, provided that the necessary consideration has been given to the subject's rights and interests, fundamentally, the right to a private life and to personal data protection.

12. **Public interests**: Series of aspirations arising out of the collective needs of the members of a community, which differ from and therefore outweigh individual interests.

13. **Vital interest**: an interest that affects survival, which if the need arises, one is willing to protect and to defend against any risk or threat that endangers survival.

14. **Legal obligation**: an obligation that immediately enters into effect and becomes enforceable once the parties, of their own will, or due to any other source of obligations, agree to it by way of a legal instrument.

15. **Contractual relationship**: relationship between two or more people by way of a legal instrument, which establishes the obligations of all signatories to the instrument.

16. **Data controller**: an individual or public or private legal entity that processes data or designates that responsibility to others to do so on his/ her/ its behalf.

17. **Third party**: Any individual or legal person other than the data subject or IICA. Some examples: the national or local governments, counterparts, as well as partners or allies, whether public or private, and employees.

18. **Data subject:** An individual whose data will be subject to processing.

19. **Processing of personal data:** Any operation or series of operations, automated or not, that are 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 disclosure by any other means, correction or destruction.

VI. Institutional provisions for personal data protection

Through this Policy and its implementation by way of the PMPDP, the Institute is establishing the provisions for the proper and correct processing of personal data, which it may have access to in order to fulfil its mission and to execute externally funded projects.

The rights of all individuals or their contact information as a legal entity shall prevail, in terms of personal data protection, confidentiality, processing in accordance with the principles established in international standards, the implementation of security measures for the

protection and safeguarding of data and guidelines regarding access to and/or transfer of the data.

By definition, personal data is classified as confidential. This confidentiality defines how the private information of an individual or legal entity shall be processed, administered and disseminated. At all times, in processing this data, the confidentiality of personal information shall be respected by the Institute and its staff.

1. Personal data processing principles

The Institute's processing of personal data shall be in accordance with the principles established in international standards and in this Policy.

These principles shall apply to:

(i) the design and implementation of all procedures that call for processing of personal data,
(ii) all contracts or obligations formalized by the Institute with individuals or legal entities,
(iii) the implementation of any systems and platforms that enable IICA staff and/ or third parties to access—whether in digital or analog form—and process personal data, while, respecting, in all cases, the principles established herein.

a. Principle 1: Lawful, fair and transparent processing:

Processing of personal data shall be lawful, fair and transparent and processed only for specific, explicit and legitimate purposes. These purposes shall be defined at the time that the data is collected.

In cases in which it is mandatory or convenient, the data subject shall be asked to provide expressed, explicit and written consent to collect his/her data. Other than consent, the following lawful bases for processing data shall be considered valid:

(i) a contractual relationship,
(ii) a legal obligation,
(iii) a vital interest,
(iv) a public interest,
(v) a legitimate interest.

Specifically, IICA will not collect or process sensitive personal data regarding ethnic or racial origin, political ideology, beliefs, religious or philosophical convictions, sexual

lifestyle or orientation, trade union affiliation, health, genetic or biometric information aimed at unequivocally identifying the person, except when the collection of said information is necessary, lawful or required by internal processes that contribute to the safety of the individual or to provide Technical Cooperation services to the Member States of the Institute. In such cases, the data shall be collected and processed in accordance with the personal data protection provisions established in this Policy.

Processing of personal data shall be made transparent to data subjects, providing easily accessible and easy to understand information regarding the processing of the data, expressed in clear and simple language. Individuals should be explicitly informed that their personal data is being processed, and told the purpose for and justification of each instance of personal data processing.

The lawful basis shall be determined, based on the reason for processing the personal data.

Detailed information shall be provided to the data subject regarding the processing of the personal data, both with respect to how it is being processed, as well as to the data subject's rights, and shall comply with the guidelines established in this Policy.

b. Principle 2: Personal data shall be collected for specific, explicit and legitimate purposes:

Personal data shall be collected for specific purposes or ends that have been previously communicated to the data subject and that comply with the principles in this Policy. It shall not be processed in a manner that is incompatible with the reasons given to the data subject nor further processed in a manner that is incompatible with these ends. Further processing for archival purposes in the public interest, for scientific or historic research, or for statistical purposes is not considered as incompatible with the initial purposes.

c. Principle 3. Adequate, pertinent and limited:

The personal data that is processed shall be adequate, pertinent and limited to the purposes for which it is being processed. Personal data shall only be processed if the purpose cannot be reasonably achieved through other means. As such, only personal data suitable for the stated purpose or purposes shall be processed and data not needed to fulfil these purposes shall not be processed.

d. Principle 4. Accuracy:

Personal data should be accurate and, where necessary, should be updated. All reasonable measures shall be taken to immediately delete or rectify any personal data that is inaccurate, with respect to the purposes for which it is being processed.

e. Principle 5: Integrity and Confidentiality:

Personal data shall be processed in a manner that ensures its security. This shall be guaranteed through the use and application of technical and organizational measures. The Institute shall establish operational guidelines in the PMPDP to promote adequate data security measures to prevent unauthorized or illicit processing and to safeguard against loss, destruction or accidental damages.

Measures regarding the personal data that is collected and processed by IICA shall ensure confidentiality, integrity, availability and the permanent resilience of systems used to store and process the data, ensuring that it cannot be used for purposes other than those that were used to justify and enable its collection or transferred to or shared with third parties, except in cases that are permitted by way of agreements and that comply with the data protection principles established in this Policy.

The Institute shall establish regular verification, assessment and evaluation procedures to ensure that technical and organizational measures are effective, thereby guaranteeing personal data processing security. These processes shall be established by way of the PMPDP.

f. Principle 6: Limitations on the storage period:

Personal data must be kept in a form that makes it possible to identify data subjects for no longer than is necessary for the processing purposes.

Data shall not be stored for longer than is necessary to achieve the purpose for which it is being processed, except in legally prescribed situations. Guidelines on data storage periods shall be established in the PMPDP.

Storing personal data for longer periods is allowed when the processing of the data is for purposes in the public interest or for scientific, historical research or statistical purposes, without prejudice to the application of the appropriate technical and organizational measures established under this Policy, in order to protect the rights of the data subject.

g. Principle 7: Proactive responsibility (accountability):

The Institute shall be responsible for complying with the principles stipulated in this Policy and shall be able to demonstrate its compliance, if required.

IICA, in accordance and compliance with its Policies and Procedures shall conduct a risk evaluation of the data processing that it is undertaking, to determine the measures to apply to guarantee that personal data is processed in accordance with this Policy. Any risk identified regarding personal data shall be addressed in accordance with provisions established in the PMPDP and institutional guidelines for risk management.

2. Rights of the data subject

a. To be informed:

Data subjects whose personal data is requested must be explicitly, accurately and unambiguously informed of the following, prior to its collection:

i. The existence of a personal data file and the individual responsible for processing at the Institute.
ii. How the personal data was obtained, whether from official or public sources, in the event that the data subject was not the source of the information.
iii. The specific purpose(s), as well as the lawful basis for each use of the personal data.
iv. The recipients of the information, as well as those who may consult this information.
v. Whether their response to the questions asked during the data collection process is mandatory.
vi. The manner in which the requested data will be processed.
vii. Whether or not there will be automated decision-making.
viii. How long the processed personal data will be kept.
ix. The possibility of exercising their right to submit a request to the Institute to erase or rectify their personal data, or in justified cases, a claim at the institutional level, as indicated in section **VIII Requests and Complaints regarding Personal Data Protection.**
x. All the information above shall appear in a clearly legible and accessible form.

b. Exercise of rights:

All data subjects whose personal data is being processed by IICA shall have the following rights with respect to protection of their personal data:

i. Access: to know if personal data is being processed, and if so, to know the conditions of processing.
ii. Rectification: the right to correct incorrect personal data and to complete incomplete data.

iii. Objection to being subject to individualized decisions: the right to object to personal data being processed in certain circumstances, for reasons related to a specific situation.
iv. Erasure ("the right to be forgotten"): the right to be allowed to have their personal data erased in certain circumstances.
v. Restriction of processing: the right to restrict processing of personal data in certain circumstances.
vi. Portability: the data subject's right to receive the personal data he/she has provided in a structured, commonly used and machine-readable format and to send it to another person for processing.

Additionally, IICA recognizes that all data subjects shall have the right to the confidentiality of electronic communications.

3. Security and security breaches that affect personal data

IICA shall establish mechanisms and procedures to ensure the protection of personal data; internal protocols and breach notification channels, risks and security violations affecting personal data.

a. Destruction, loss or accidental or unlawful alteration of personal data:

In the event of destruction, loss or accidental or illicit alteration of personal data, or the transfer of or unauthorized access to said data (personal data security breach), the internal protocols established in the PMPDP and in the Institute's Information Technology Policy shall be applied immediately. Moreover, a notification should be sent immediately to the Representative in the respective IICA Delegation in the Member States or to the Director of Corporate Services, in the case of Headquarters. In either instance, the notification should also be sent to the Personal Data Protection Management Team. All incidents should be documented and the established internal protocols adopted, to resolve and mitigate the possible negative effects for the relevant parties and for the Institute.

b. Risk of a personal data security breach

When a real or potential risk of a personal data security breach arises, IICA staff should immediately notify the Representative of the respective Delegation in the Member States or in the case of Headquarters, the notification should be sent to the Director of Corporate Services. In either instance, the notification should also be sent to the Personal Data Protection Management Team. Moreover, the internal protocols established in the PMPDP should be activated to mitigate the impact of the risk.

4. Transfer of and access to personal data by third parties

The Institute may transfer personal data to a third party, provided that the third party ensures a level of data protection that is equal or similar to the level provided by this Policy, that the interested party has been duly informed in this regard, and that, where applicable, consent has been obtained in a valid and legal manner.

Taking into account possible data protection risks involved in transfers to third parties, the third party must comply with the principles established in section VI.1 of this Policy.

To guarantee the protection of personal data to be transferred, IICA will include any clauses it deems relevant in legal instruments signed with third parties.

Procedures to verify compliance of data processors with the obligations established in this Policy and in the PMPDP will be applied in developing contracts with third parties that will have access to personal data.

5. General information

a. To ensure that the institutions, organizations, partners, employees, consultants and suppliers, among others, that engage in cooperation activities with IICA or that provide services to IICA, comply with the contents of this Policy, all legal instruments that establish any type of relationship with the Institute must include the clauses indicated in the PMPDP.

b. Furthermore, to contribute to the fulfillment of this Policy, legal instruments that establish any type of relationship with the Institute will include a Declaration on Personal Data Protection, which must form part of the supporting documents for the procurement of goods and services, the contracting of personnel, or any other type of legal instrument that involves the collection and/or use of personal data. The Declaration is included in the PMPDP.

c. In the event that IICA contracts a third party to carry out actions that could involve the processing of personal data beyond IICA's supervision and control, IICA must sign a Contract for Personal Data Access by Third Party, available in the PMPDP, with the supplier or counterpart.

d. 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 IICA and/or its personnel, in accordance with international law, international treaties and conventions or the national legislation of its Member States.

e. The complementary application of PMPDP procedures that regulate aspects related to personal data processing is compulsory.

VII. Responsibilities

All Institute members and employees are responsible for implementing and complying with this Policy. The Director General will designate the members of the Personal Data Protection Management Team[1], which will be responsible for ensuring that all persons involved in the Institute's activities are aware of and committed to the systematic application of this Policy and the PMPDP.

The Representatives and Administrators of the Delegations in the Member States, as well as the Director of Corporate Services at Headquarters, will oversee compliance with this Policy.

The Internal Audit Unit will conduct periodic reviews to assess the application of and compliance with this Policy and the PMPDP and will issue recommendations to the Director General and the Director of Corporate Services.

VIII. Requests and complaints related to personal data protection

Requests made to the Institute by a data subject, such as requests regarding access, rectification, objection to being the subject of individualized decisions, erasure, restriction of personal data processing, or portability, must be channeled through the IICA Delegation in his/her country of residence, or through Headquarters or the IICA Delegation that collected his/her data, if the data subject does not reside in an IICA Member State. The Institute will provide an email address for each IICA Delegation and for Headquarters, in order to promptly address and respond to these requests.

If necessary and justifiable, in compliance with IICA's Policy for the Processing of Reports and the Protection of Whistleblowers and Witnesses, the data subject may file a complaint to the Institute regarding the issues addressed in this Personal Data Protection Policy. To this end, IICA has established two channels for the confidential receipt and processing of complaints:

- IICA's official website: www.iica.int, under the REPORTS/COMPLAINTS section; and
- The email address ec.ce@iica.int

[1] The Personal Data Protection Management Team is equivalent to a Data Protection Officer, in accordance with international standards.

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

IX. Privacy Notice

IICA is the entity responsible for and in charge of processing the personal data specified in this document. Pursuant to IICA's Personal Data Protection Policy, the mechanisms through which we process personal data are secure and confidential. We declare that we apply suitable technical, organizational and technological measures to ensure that personal data is stored in such a way as to prevent unauthorized access by third parties, and, in turn, guarantee the confidentiality of the data. IICA also respects the right to the confidentiality of electronic communications.

1. Use of personal information

Your personal data will be included in a database or physical repository and may be used for the following purposes:

a. to meet the objectives of our contractual relationships;
b. to contact you and respond to any request you may have sent via IICA's websites;
c. to send you informational material about IICA, in keeping with your interests;
d. to conduct satisfaction surveys among users;
e. to address requests, complaints or claims that you have a right to make as a person that utilizes IICA's information services;
f. to manage and reply to comments or requests made through our blogs, which are open for your participation;
g. to compile general statistics; and
h. to make any other lawful, fair, just and transparent use within the scope of IICA's action.

IICA uses cookies that store general, non-personal information to measure the number of visits to our sites, the average time spent on the site, pages visited, and other similar information, and to improve content and ensure security and protection of data. To access IICA's Web pages, all users must accept the use of cookies.

IICA does not release, rent, allocate, transfer nor provide personal information to third parties without your prior consent, except when (i) it is general public knowledge at the moment it is divulged or it becomes public domain through no illegal action on the part of IICA; (ii) it is in the possession of IICA at the moment it is divulged, without IICA violating any legal obligation; (iii) it becomes known to IICA from sources other than the disclosing party, but with the legal right to divulge such Personal Information; (iv) it must be divulged by IICA in order to comply with applicable government laws or regulations.

On the iica.int website, you may consult the Personal Data Protection Policy, which set out provisions for the processing of information collected, as well as the consultation and complaint procedures that will enable you to exercise your rights.

2. Security and integrity of the information

The information you provide as a personal data subject will be stored and protected in keeping with industry and technology standards. In spite of this, the internet is not a space that is 100% secure; therefore, IICA cannot guarantee that transmissions via the Internet will be completely private or secure, and you understand that any message or information sent to IICA can be read or intercepted by third parties, even when the information is encrypted. Therefore, you agree to hold IICA harmless from any liability.

3. Your rights

You have the right, at any time, to access and request a copy of your personal information, as well as to:

1. request that your personal information be corrected, updated, revoked or eliminated, or utilized for limited purposes, and to request its portability, as well as to object to being subject to individualized decisions. All requests must be submitted via the forms available on the website iica.int;
2. update your email preferences (to whatever email address you wish to receive the information) by clicking on the hyperlink captioned “Email preferences”, which is located in the lower part of each email message sent by IICA. Once you have clicked on the hyperlink, you will be able to select which emails you prefer to receive from IICA.

4. General clauses

IICA reserves the right to amend this Privacy Notice; such amendments shall be published on its website: www.iica.int.

X. Publication

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

XI. Interpretation

Matters not addressed by this Policy or which may lend themselves to different interpretations will be clarified by the Personal Data Protection Management Team and authorized by the Director of Corporate Services.

XII. Review and adjustments

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

XIII. Validity:

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