



Inter-American Institute for  
Cooperation on Agriculture

# Procedural Manual on Personal Data Protection

January 2023

# Index

## A. TABLE OF CONTENTS

I.	Foreword.....	1
II.	Regulatory framework .....	1
III.	Applicability and scope .....	1
IV.	Objective .....	1
4.1	Specific objectives.....	1
V.	General information.....	1
VI.	Personal data processing principles .....	2
VII.	Personal data processing procedures.....	3
VIII.	Verification, evaluation and assessment .....	4
IX.	Requests and complaints related to personal data protection .....	5
9.1	Requests by data subjects to exercise their rights .....	5
9.2	Complaints related to personal data protection .....	5
X.	Incident and complaints log .....	6
XI.	Responsibilities .....	6
XII.	Publication .....	6
XIII.	Interpretation.....	6
XIV.	Review and adjustments .....	7
XV.	Validity.....	7
XVI.	Definitions .....	7
	Annex 1 – Protocols for recording IICA’s third-party personal data processing activities .....	10
1.	Introduction.....	10
2.	Objective .....	10
3.	Procedure.....	10
4.	Protocols for recording IICA’s third-party personal data processing activities .....	11
	Annex 2 – Data protection by design and by default.....	15
1.	Introduction.....	15
2.	Objective .....	15
3.	Procedure .....	15
4.	Data protection by design .....	16

4.1	Verification Questionnaire – Privacy by Design Principles .....	16
5.	Data protection by default .....	24
5.1	Implementation of appropriate “measures” .....	24
Annex 3 – Obligation to inform data subjects and to obtain their consent .....		27
1.	Introduction.....	27
2.	Objective .....	27
3.	Procedure .....	27
4.	Obligation to inform data subjects .....	27
5.	When the data subject should be informed .....	28
6.	Obligation to provide transparent information to data subjects .....	28
7.	Ways of complying with the obligation to inform data subjects.....	29
8.	Lawful basis for personal data processing .....	29
9.	Consent .....	30
9.1	Characteristics of consent.....	30
10.	Statement of Consent Model .....	33
11.	Contractual clause applicable to contracts with suppliers and consultants for the procurement of goods and services.....	33
12.	Clause to be included in tenders .....	35
13.	Clause to be included in legal instruments, excluding those with suppliers and consultants .....	35
Annex 4 – Exercising and addressing the rights of data subjects.....		37
1.	Introduction.....	37
2.	Objective .....	37
3.	Procedure .....	37
4.	Recognized rights of the data subject.....	38
4.1	Right of access .....	38
4.2	Right to rectification .....	38
4.3	Right to erasure .....	38
4.4	Right to restrict processing .....	39
4.5	Right to object .....	39
4.6	Right not to be subject to automated individual decision-making.....	40

4.7	Right to personal data portability .....	40
5.	Procedure for exercising and addressing requests regarding rights .....	44
5.1	Previous considerations .....	44
5.2	Receipt of requests .....	45
5.3	Minimum requirements of requests to exercise rights .....	45
5.4	Timeframe for responding to requests to exercise rights .....	46
5.5	Responding to a request to exercise rights .....	48
5.6	Record of requests to exercise rights.....	49
5.7	Sample forms for exercising rights.....	49
	Sample forms (for data subjects).....	51
	Sample 1: Exercising the data subject’s right of access.....	51
	Sample 2: Exercising the data subject’s right to rectification .....	53
	Sample 3: Exercising the data subject’s right to erasure.....	54
	Sample 4: Exercising the data subject’s right to restriction of processing .....	55
	Sample 5: Exercising the data subject’s right to data portability .....	56
	Sample 6: Exercising the data subject’s right to object.....	57
	Sample responses (on the part of IICA).....	58
	Sample 1: Positive response to a request to exercise the right of access .....	58
	Sample 2: Negative response to a request to exercise the right of access .....	60
	Sample 3: Positive response to a request to exercise the right to rectification .....	61
	Sample 4: Positive response to a request to exercise the right to erasure .....	62
	Sample 5: Positive response to a request to exercise the right to erasure .....	63
	Sample 6: Positive response to a request to exercise the right to restrict processing.....	64
	Sample 7: Positive response to a request to exercise the right to portability.....	65
	Sample 8: Positive response to a request to exercise the right to object .....	66
	Annex 5 – Verification of personal data processor .....	67
1.	Introduction.....	67
2.	Objective .....	67
3.	Procedure .....	67
3.1	Compliance checklist prior to hiring a processor. ....	68
3.2	Compliance checklist upon completion of a Data Processor agreement .....	70

Annex 6 – Appointment of third parties with access to third-party personal data.....	71
“Data processor” .....	71
1. Introduction.....	71
2. Objective .....	71
3. Procedure .....	71
3.1 Data processor guarantees .....	72
3.2 Personal data access agreement.....	72
3.3 Data processor security measures .....	72
3.4 Notification of Data processor-related security violations.....	73
3.5 Data return or deletion by the Data processor .....	73
3.6 Outsourcing to a Sub-processor.....	74
3.7 Record of Data processors and evidence of compliance.....	74
Sample Contract for Personal Data Access by Third Party .....	75
Annex 7 – Notification of a personal data breach .....	82
1. Introduction.....	82
2. Objective .....	82
3. Procedure .....	82
3.1 Definition, examples, and adverse effects of security incidents and breaches.....	83
3.2 Incident detection and notification.....	84
3.3 Data processors and Sub-processors .....	86
3.4 Incident log .....	87
3.5 Communication of a data breach to the data subject.....	87
Annex 8 – Retention and deletion of personal data .....	90
1. Introduction.....	90
2. Objective .....	90
3. Procedure .....	90
Annex 9 – Designation of the Data Protection Management Team .....	93
1. Introduction.....	93
2. Objective .....	93
3. Procedure .....	93
Annex 10 – Rights and obligations of IICA employees.....	96

1. Introduction.....	96
2. Purpose .....	96
3. Procedure .....	96
4. General principles.....	96
5. Rights of the employee.....	97
6. Obligations of employees .....	98
7. Explicit and documented consent.....	100
8. Sharing the personal data of IICA employees .....	100
9. Storage of personal data .....	101
10. Sensitization .....	101
11. Complaints.....	101
12. Responsibilities.....	101

## **Foreword**

This Procedural Manual on Personal Data Protection serves to instruct all staff members of the Inter-American Institute for Cooperation on Agriculture (IICA or the Institute) who are responsible for processing the personal data of the individuals or contact persons in legal entities collaborating with the Institute to ensure transparent and proper processing of their personal data, in keeping with international personal data protection principles and standards.

### **I. Regulatory framework**

The Institute is committed to the protection of personal data, which is regulated by its Personal Data Protection Policy. Therefore, this Manual is based primarily on that Policy, as well as on other institutional policies and procedures, be they manuals or guides.

From a procedural perspective, this Manual is a companion to the Personal Data Protection Policy.

### **II. Applicability and scope**

The procedures contained in this Manual apply to any and all individuals with a direct involvement with IICA, in any of its Member States or at Headquarters, and who are collaborating with the Institute to fulfil its mission.

### **III. Objective**

To provide procedural guidelines to IICA Delegations in the Member States and Units at Headquarters that are processing third-party personal data, in adherence to institutional data protection provisions.

#### **4.1 Specific objectives**

- a. To provide IICA with a regulatory framework for personal data protection appropriate to the technical cooperation challenges and aligned with international standards.
- b. To be an institution that remains true to its values and principles, promoting respect for the rights of individuals.
- c. To comply with institutional provisions contained in the Personal Data Protection Policy.
- d. To implement the guidelines contained in this Manual, in a testable, documented and verifiable manner.

### **IV. General information**

- 5.1 This Procedural Manual on Personal Data Protection is as an implementation mechanism to ensure compliance with the institutional provisions contained in the Personal Data Protection Policy.
- 5.2 Processing of personal data includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, transfer dissemination, correction or destruction of third-party personal data. This processing shall comply with the principles established in the Personal Data Protection Policy – Section VI. **Personal Data Processing Principles** and the procedures described in this manual.
- 5.3 To guarantee that institutions, organizations, partners, consultants and providers, among others, that are undertaking cooperation actions in collaboration with IICA or that are lending their services to the organization, comply with the provisions of the Personal Data Protection Policy and the procedures described in this Manual, all legal instruments that establish any kind of relationship with the Institute shall include the Clauses detailed in this Manual.
- 5.4 No provision included in this Manual 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.

## V. **Personal data processing principles**

The Institute's processing of personal data shall be in accordance with the following principles established in international standards and that are described in detail in the Personal Data Protection Policy on which this Manual is based:

- 6.1 **Principle 1:** Lawful, fair and transparent processing.
- 6.2 **Principle 2:** Personal data shall be collected for specific, explicit and legitimate purposes.
- 6.3 **Principle 3:** Adequate, pertinent and limited.
- 6.4 **Principle 4:** Accuracy.
- 6.5 **Principle 5:** Integrity and confidentiality.
- 6.6 **Principle 6:** Limitations on the storage period.



## 6.7 Principle 7: Proactive responsibility (accountability).

### VI. Personal data processing procedures

To ensure proper implementation of the IICA Personal Data Protection Policy, the following procedures have been established and are further detailed in the Annexes of this Manual; they specify actions that must be applied by Institute staff members who access or process third-party personal data.

Application of the procedures described below shall be mandatory and staff should direct any related queries to IICA's Personal Data Protection Management Team<sup>1</sup>, which was created to provide guidance on this material, in keeping with the principles in Section VI above, international standards and best practices.

It shall be the responsibility of each IICA Delegation or Unit at Headquarters that has access to or processes third-party personal data to establish internal mechanisms to guarantee compliance with the procedures described herein and to ensure proper management, verification documentation and continuous updating of information.

See below the procedures to comply with the IICA Personal Data Protection Policy:

No.	Procedure	Annex
1	Protocols for recording IICA's third-party personal data processing activities	Annex 1
2	Data Protection by design and by default	Annex 2
3	IICA's obligation to inform data subjects and to obtain their consent	Annex 3
4	Exercising and addressing the rights of personal data subjects	Annex 4
5	Verification of personal Data processor	Annex 5
6	Appointment of third parties with access to third-party personal data (data processors)	Annex 6

---

<sup>1</sup> IICA Personal Data Protection Management Team, email address: [data.protection@iica.int](mailto:data.protection@iica.int)

<b>7</b>	Notification of a personal data breach	Annex 7
<b>8</b>	Retention and deletion of personal data	Annex 8
<b>9</b>	Designation of the Data Protection Management Team or the Data Protection Officer	Annex 9
<b>10</b>	Rights and obligations of IICA employees	Annex 10

### **VIII. Verification, evaluation and assessment**

IICA shall undertake periodic reviews to verify and validate correct application of and compliance with measures established in the principles governing this Manual and that are detailed in the Personal Data Protection Policy.

The Institute should be able to demonstrate compliance, by verifying actions taken to protect personal data.

As such, IICA shall:

- 8.1 Implement a verification and evaluation process, in accordance with its policies and procedures.
- 8.2 Assign responsibilities to the individuals in charge of data-related activities or processing to comply with the Data Protection Policy and this Manual. These individuals will have the responsibility of ensuring adherence to the principles contained in the abovementioned policy.
- 8.3 Ensure that information system security measures are followed, taking into account this Manual and IICA's Information and Communication Technologies Policy.
- 8.4 Undertake a compliance review on third-party personal data processing by IICA, through the Institute's Internal Audit Unit, as part of the Institute's Annual Auditing exercise. The corresponding report and its findings shall be shared with the Data Protection Management Team, with a view to adopting corrective actions and identifying areas for improvement.

- 8.5 Identify other ways of demonstrating the Institute's compliance with third-party personal data protection, other than what is detailed in the previous point.
- 8.6 Make every effort to ensure that the Procedural Manual on Personal Data Protection is kept up to date, in accordance with international standards.

## **IX. Requests and complaints related to personal data protection**

### **9.1 Requests by data subjects to exercise their rights**

Possible requests by a personal data subject to the Institute, such as requests for access, erasure of data, objection to being subject to individualized decisions, or requests for erasure, restriction of data processing or portability, should be channeled through the IICA Delegation in his/ her country or, if it is in a different country, through the IICA Delegation that is processing his/her data.

The Institute shall provide an email for Headquarters and for each Delegation to address and respond to these requests in a timely manner. In the case of Headquarters, the responsibility of following up on requests by data subjects to exercise their rights shall fall to the Data Protection Management Team. In the IICA Delegations, the matter shall be handled by the Administrator.

### **9.2 Complaints related to personal data protection**

In necessary and justified cases, in compliance with the Procedural Manual on Personal Data Protection, the personal data subject may file a complaint with the Institute regarding the matters governed by this Manual, utilizing the mechanism dictated by the Institute's Policy for the Processing of Reports and Protection of Whistleblowers and Witnesses. IICA has established two channels for the confidential receipt and processing of complaints:

- a. IICA's official website: [www.iica.int](http://www.iica.int), under the REPORTS/COMPLAINTS section; and
- b. The email address [ec.ce@iica.int](mailto:ec.ce@iica.int)

All complaints, investigations, reports and information in relation to the complaint will be objectively examined and analyzed by the Institute's Ethics Committee, which will define how to address the issue, recommend necessary disciplinary measures and take actions appropriate to the specific circumstances.

## **X. Incident and complaints log**

The Data Protection Management Team, with the support of the Administrators at the IICA Delegations, shall maintain an up-to-date incident log involving personal data processing, as well as a log of reports or complaints received through official institutional channels.

At the very least, the log shall contain;

- a. The date on which the report or complaint was identified or received.
- b. Approach taken, indicating dates, actions undertaken and individuals responsible for actions.
- c. Date on which a response was sent to the complainant
- d. Status of the incident or report/ complaint.
- e. Date when the matter or report/complaint was finally settled.

## **XI. Responsibilities**

Implementation of and compliance with this Procedural Manual on Personal Data Protection shall be the responsibility of all Member States and staff of the Institute. The Director General shall designate a Personal Data Protection Management Team<sup>2</sup>, which shall be responsible for ensuring that all individuals involved in the Institute's activities are aware of and committed to the systematic application of the provisions of this Manual.

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

The Internal Audit Unit shall conduct annual reviews regarding the systematic application of and compliance with this Procedural Manual on Personal Data Protection and shall issue recommendations to the Director General and the Director of Corporate Services.

## **XII. Publication**

This Manual will be available in the institutional repository upon the approval of the Director General.

## **XIII. Interpretation**

Matters not addressed by this Manual or which may lend themselves to different interpretations shall be clarified by the Personal Data Protection Management Team, with prior authorization by the Director of Corporate Services.

<sup>2</sup> The Personal Data Protection Management Team, is equivalent to Data Protection Officer according to international standards.

#### **XIV. Review and adjustments**

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

#### **XV. Validity**

This Manual shall enter into force on the date that is announced by the Director General.

#### **XVI. 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 written or verbal 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 of personal data.
4. **Lawful basis:** specific situations or circumstances in which personal data may be processed without the consent of the data subject. 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 expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it 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, 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/her specific status and/or needs.

7. **Private personal data:** data that is only relevant to the data subject due to 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. **Data processor:** Individual or legal entity that is processing personal data on behalf of IICA.
11. **Personal Data Protection Management Team:** members of staff who, in accordance with international standards and best practices, are responsible for providing guidance to IICA Delegations in the Member States or Units at Headquarters that have access to or process third-party personal data, with a view to continuous management and updating of the inventory of personal information; identifying and evaluating new data collection, use or disclosure; as well as revising policies, in accordance with the recommendations from assessments or audits.
12. **Personal data leak:** a data security breach that results in the destruction, loss, alteration, unauthorized disclosure or accidental or illegal access to transferred, stored or otherwise processed personal data.
13. **Data interested party:** The owner of the personal data.
14. **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.
15. **Public interest:** Series of aspirations arising out of the collective needs of the members of a community, which differ from and therefore outweigh individual interests.
16. **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.

- 17. Justification for processing:** legitimate basis that authorizes personal data processing; it may be the consent of the data subject or any other lawful basis established in the Data Protection Policy.
- 18. 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 arrangement.
- 19. Contractual relationship:** relationship between two or more people by way of a legal instrument, which establishes the obligations of all signatories to the instrument.
- 20. 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. For the purposes of this Manual, IICA is the data controller.
- 21. Pseudonym:** information that excludes the identifying data of the affected person, which by association with additional information, would allow one to determine the identity of the individual behind the pseudonymized data.
- 22. Third party:** Any individual or legal person other than the data subject or IICA. Some examples of third parties are national or local governments, counterparts, as well as partners or allies, whether public or private.
- 23. Data subject:** An individual whose data will be subject to processing.
- 24. 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.

## Annex 1 – Protocols for recording IICA’s third-party personal data processing activities

		<b>TYPE OF DOCUMENT</b>	
		<input type="checkbox"/>	Public (available on the IICA Website)
		<input checked="" type="checkbox"/>	Private (available on IICA’s intranet)
<b>TITLE</b>		Protocols for recording IICA’s third-party personal data processing activities	
<b>APPLICATION</b>		All IICA Delegations and Units at Headquarters with access to and that process third-party personal data	
<b>FORMAT</b>		PDF	
<b>PAGES</b>		5	
<b>REF. APPROVAL</b>		(pte completar este dato)	
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

The following protocol facilitates the correct application of IICA’s mandatory Personal Data Protection Policy, which requires that a record be kept of third-party personal data processing activities identified at IICA. Please note that some concepts mentioned in this Table may require the reader to consult other procedures contained later in this Manual.

### 2. Objective

To guide Institute staff members who access or process third-party personal data on the protocols for recording information on personal data processing activities, in compliance with the guidelines of IICA’s Personal Data Protection Policy and this Manual.

### 3. Procedure

Administrators of the IICA Delegations in the Members States and the Units at Headquarters that have access to or process third-party personal data should meticulously meet the Protocols for recording IICA’s third-party personal data processing activities, described below.



#### 4. Protocols for recording IICA's third-party personal data processing activities

<b>Procurement of goods</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out with the data subject's <b>consent</b> ; that is, a written and expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it has been duly recorded.
Purpose of processing	Management of the procurement of good that guarantee the continuity of IICA's activities.
Category of data	<b>Identifying:</b> name and surname; identification document of the individual, legal representative or contact person in the case of a legal entity; address; country of origin; date of birth; nationality. <b>Contact information:</b> telephone number, email address.
Category of data subjects	Individuals and legal representatives or contact persons of legal entities that supply goods to IICA.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.

<b>Hiring of consultants</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out with the data subject's <b>consent</b> ; that is, a written and expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it has been duly recorded.
Purpose of processing	Management of the hiring of professional consultants to provide advisory services or perform specialized tasks as part of IICA's activities or projects.
Category of data	<b>Identifying:</b> name and surname, identification document, address, country of origin and nationality of the individual, legal representative or contact person in the case of a legal entity. <b>Contact information:</b> telephone number, email address, fax. <b>Academic and professional:</b> occupation, area of expertise, experience in IICA's thematic areas of work, languages, academic background, professional experience. Any other information that is strictly necessary for the service proposal or contracting process.
Category of data subjects	Individuals and legal representatives or contact persons of legal entities that provide professional services to IICA.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.

<b>Contracting for services</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out with the data subject's <b>consent</b> ; that is, a written and expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it has been duly recorded.
Purpose of processing	Management of the contracting for services to guarantee the continuity of IICA's activities.
Category of data	<b>Identifying:</b> name and surname, identification document, address, country of origin and nationality of the individual, legal representative or contact person in the case of a legal entity. <b>Contact information:</b> telephone number, email address, fax.
Category of data subjects	Individuals and legal representatives or contact persons of legal entities that provide services to IICA.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.

<b>Data subjects interested in technical information</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out with the data subject's <b>consent</b> ; that is, a written and expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it has been duly recorded.
Purpose of processing	Dissemination of communications and technical or informational publications issued by IICA or an IICA project, network or other.
Category of data	<b>Identifying:</b> name and surname, location. <b>Contact information:</b> email address.
Category of data subjects	Subscribers to IICA newsletters or technical communications.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.

<b>Data subjects interested in job opportunities</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out with the data subject's consent; that is, a written and expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it has been duly recorded.
Purpose of processing	Evaluate the professional profiles of candidates who wish to work at IICA.

Category of data	<b>Identifying:</b> name and surname, identification document, location, country of origin, date of birth and nationality. <b>Contact information:</b> telephone number, email address. <b>Academic and professional:</b> occupation, area of expertise, thematic areas, languages, academic background, professional experience, and any other information collected strictly for the purpose of evaluating the applicant's professional profile.
Category of data subjects	Individuals interested in working at IICA.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.

<b>Participants in meetings, workshops and seminars</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out with the data subject's consent; that is, a written and expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it has been duly recorded.
Purpose of processing	Participation in events overseen by IICA. Participants may register directly or receive an invitation to participate in events organized by IICA.
Category of data	<b>Identifying:</b> name and surname, identification document, location, country of origin, date of birth and nationality. <b>Contact information:</b> telephone number, email address.
Category of data subjects	Participants in events organized by IICA.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.


<b>Internships and academic and professional visits</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out with the data subject's consent; that is, a written and expressed statement in which the data subject agrees to the processing of his/her personal data. Oral consent may also be given, provided that it has been duly recorded.
Purpose of processing	Evaluate the technical or professional profiles of candidates interested in participating in an internship or academic or professional visit at IICA.
Category of data	<b>Identifying:</b> name and surname, identification document, location, country of origin, date of birth and nationality. <b>Contact information:</b> telephone number, email address. <b>Academic, technical and professional:</b> area of expertise, thematic areas, languages, academic background, technical or professional experience.

Category of data subjects	Students pursuing technical specializations, university students, undergraduates or recent graduates.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.

The following protocol applies in the case of legal instruments signed in accordance with the provisions of the Manual for the Management of External Resources.

<b>Legal instruments</b>	
Lawful basis	Pursuant to IICA's Personal Data Protection Policy, processing will be carried out based on a contractual relationship between two or more people by way of a legal instrument, which establishes the obligations of all signatories to the instrument.
Purpose of processing	Execute legal instruments and agreements signed between the parties involved.
Category of data	<b>Identifying:</b> name and surname, identification document, address, country of origin and nationality of the legal representative or contact person of the counterpart. <b>Contact information:</b> telephone number, email address.
Category of data subjects	Organizations or institutions, which may execute legal instruments or components thereof and legal agreements in which IICA is the executing agency.
Timeframe for deletion	Personal data will be deleted upon expiration of the timeframe indicated in IICA's Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.
Security measures	The security measures are set out in the Personal Data Protection Policy and Annex 2 of the Procedural Manual on Personal Data Protection.
Entity responsible	The Inter-American Institute for Cooperation on Agriculture (IICA). If a processor is used, the provisions of Annexes 5 and 6 of the Procedural Manual on Personal Data Protection will be followed.

## Annex 2 – Data protection by design and by default

		<b>TYPE OF DOCUMENT</b>	Public (available on the IICA website)
		<input checked="" type="checkbox"/>	Private (available on IICA's intranet)
<b>TITLE</b>		Data protection by design and by default	
<b>APPLICATION</b>		All IICA Delegations and Units at Headquarters with access to and that process third-party personal data	
<b>FORMAT</b>		Electronic – Word	
<b>PAGES</b>		11	
<b>REF. APPROVAL</b>		SC/DG-404, SEPTEMBER 24, 2021	
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

This procedure complies with IICA's mandatory Personal Data Protection Policy, which requires that internal procedures be adopted, with a view to implementing technical and organizational measures in line with the principles of data protection by design and by default.

**Privacy by design** is defined as the adoption of technical and organizational measures for the purpose of effectively applying data protection principles and incorporating the necessary guarantees into data processing operations, bearing in mind privacy throughout the entire lifecycle of a product or service – from creation, through usage, to completion.

**Privacy by default** is the adoption of technical and organizational measures to ensure that processing is limited to only the data needed for the specified purpose.

### 2. Objective

To define the applicable measures to guarantee the implementation of data protection principles by design and by default in the processing of third-party data by IICA.

### 3. Procedure

Administrators of the IICA Delegations in the Members States and the Units at Headquarters should incorporate privacy requirements **by design** and **by defect** into those internal processes that involve access to or processing of third-party personal data.

#### 4. Data protection by design

IICA has the obligation to adopt appropriate technical and organizational measures at the initial design, development or selection phase of any information system; in any use of applications or programs; or in any new project or service that involves third-party data processing, and shall continue this throughout the lifecycle of same.

IICA shall take into account privacy by design both in cases in which it is providing technical services on its own behalf or designing products that involve processing of third-party data, as well as in other instances in which it has outsourced personal data processing activities to an external entity.

When the development of a product—be it a system, application, service, etc.—must be outsourced to a third party, the developers or executors shall sign a **Contract for Personal Data Access by Third Party**, contained in **Annex 6** of this Manual, which shall govern the relationship involving the transfer of personal data by IICA, taking into account the concept of privacy by design in the product to be developed.

To facilitate the implementation of appropriate technical and organizational measures at the design phase, see as follows the **Verification Questionnaire – Privacy by Design Principles**.

##### 4.1 Verification Questionnaire – Privacy by Design Principles

###### Project information<sup>1</sup>

Identification	Details
Project Name	
Project Owner	

---

<sup>1</sup> Here, the term 'project' refers to the development or selection of an information system; use of applications or programs; or the development and execution of a new project of service involving third-party data processing.

Project Description	Include a brief description of the Project/ Initiative, specifying its purpose, need or the opportunity it presents for the organization. If it involves the review of an existing process, specify what modifications will be made to the current process.
IICA Unit that is the Data controller	
Intervening Entities:	
Data processor	Unit that processes data on behalf of the Data Controller.
Data access date:	

### Categorization and volume of data subjects

Category	Applicable	Volume
Data related to projects	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Data related to third parties	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Data related to consultants and suppliers	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Other types of data: <a href="#">Click or press here to enter text.</a>	<input type="checkbox"/> YES <input type="checkbox"/> NO	

### Type of data processed

Type of data	Appli- cable	Details
Identification data (such as name, address, nationality, gender): zip code, gender and date of birth.	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Information identification number (ID cards, passport number, driver's license)	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Professional data (CV, current position, professional skills, etc.)	<input type="checkbox"/> YES <input type="checkbox"/> No	Please specify
Data regarding the client's lifestyle, preferences, marital status, family make-up.	<input type="checkbox"/> YES	Please specify

	<input type="checkbox"/> NO	
Health-related data	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Biometric data	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Financial situation (financial position, income, etc.)	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Data regarding internet access (IP address, device information...)	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Geolocation data	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Policy data	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Data regarding violations, criminal sentences or security measures.	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Racial or ethnic origin	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Metadata <sup>1</sup>	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify
Other types of data	<input type="checkbox"/> YES <input type="checkbox"/> NO	Please specify

### Cookies and other identifying online personalization data

Applicable	Type of cookies
<input type="checkbox"/> YES <input type="checkbox"/> NO	Technical cookies (Used only to facilitate browsing or to provide a service requested by the user):  <input type="checkbox"/> YES <input type="checkbox"/> NO Browsing or session cookies <input type="checkbox"/> YES <input type="checkbox"/> NO Analytical cookies <input type="checkbox"/> YES <input type="checkbox"/> NO Functionality cookies

---

<sup>1</sup> «data about data», in other words, data that describes other data, allowing it to be localized and facilitating processing. For example, information on when a telephone call is made, the time, the caller's number, the call recipient's number and the duration of the call is metadata relative to that phone call and that can assist in localization or selection.



	<input type="checkbox"/> YES <input type="checkbox"/> NO Other: <a href="#">Click or press here to enter text</a>
<input type="checkbox"/> YES <input type="checkbox"/> NO	Personalization cookies (Used to control browsing and collect data on likes, habits and personal choices that enable a detailed profile to be created for each user):  <input type="checkbox"/> YES <input type="checkbox"/> NO Tracking cooking for the purpose of creating a profile regarding the user <input type="checkbox"/> YES <input type="checkbox"/> NO Others, specify: <a href="#">Click or press here to enter text</a>
<input type="checkbox"/> YES <input type="checkbox"/> NO	Third-party cookies

Indicate if other techniques to identify the online user are employed for personalization purposes.

### Purposes of personal data collection

Indicate and describe the reasons for personal data collection:

Applicable	Reason for collection	Details
<input type="checkbox"/> YES <input type="checkbox"/> NO	Management of client files	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Service provision	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Data transfers to a third party	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Statistics	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Promotion or marketing	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Profile development	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Purchasing or procurement of goods/ services	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Storage	
<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	Other:	

### Source of the data that has been collected

Indicate the source of the data that has been collected:

Applicable	Data source	Details
<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	From the data subject	
<input type="checkbox"/> YES <input type="checkbox"/> NO	From a third-party database	Specify
<input type="checkbox"/> YES <input type="checkbox"/> NO	From a publicly-accessible data source	Specify
<input type="checkbox"/> YES <input type="checkbox"/> NO	Websites (cookies, surveys...)	Specify
<input type="checkbox"/> YES <input type="checkbox"/> NO	Social media (Facebook, Twitter, etc.) or blogs	Specify

<input type="checkbox"/> YES <input type="checkbox"/> NO	Specific publications	Specify
<input type="checkbox"/> YES <input type="checkbox"/> NO	Other sources: <a href="#">Click or press here to enter text</a>	Specify

### Personal data collection methods

Indicate the manner in which the personal data is collected:

Applicable	DATA SOURCE
<input type="checkbox"/> YES <input type="checkbox"/> NO	<p><b>Directly from the personal data subject:</b></p> <p><input type="checkbox"/>YES <input type="checkbox"/>NO The data subject enters their data directly into the tool/module: for example, via a web form.</p> <p><input type="checkbox"/>YES <input type="checkbox"/>NO Other: <a href="#">Click or press here to enter text</a></p>
<input type="checkbox"/> YES <input type="checkbox"/> NO	<p><b>Indirectly by:</b></p> <p><input type="checkbox"/>YES <input type="checkbox"/>NO Tool that enables IICA to collect data: Specify: <a href="#">Click or press here to enter text</a></p> <p><input type="checkbox"/>YES <input type="checkbox"/>NO Other: <a href="#">Click or press here to enter text</a></p>

### Means of accessing personal data

Applicable	How data can be accessed	Details
<input type="checkbox"/> YES <input type="checkbox"/> NO	Website (through the internet)	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Specific tool, information system	Please specify.
<input type="checkbox"/> YES <input type="checkbox"/> NO	Mobile device: via the web or a mobile app?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Other	Please specify.

Applicable	Individuals with access to the data	Reason
<input type="checkbox"/> YES <input type="checkbox"/> NO	Employees and collaborators: Specify Area/Unit.	

<input type="checkbox"/> YES <input type="checkbox"/> NO	External consultants: Identify Area/Company to which services are being provided.	
<input type="checkbox"/> YES <input type="checkbox"/> NO	External Suppliers: Identify Area/Company to which services are being provided.	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Other: <a href="#">Click or press here to enter text</a>	

Indicate:

- The reasons and justification for accessing data:
- Whether or not the participants will need to use all of the data:

### Informing and obtaining the consent of the data subjects to process their data

Indicate how the data subjects were advised about the data processing	
<input type="checkbox"/>	Privacy notice on the website or intranet site:
<input type="checkbox"/>	Privacy and security notice in the service contract:
<input type="checkbox"/>	Privacy notice in the tool or module
<input type="checkbox"/>	Other: Please specify: <a href="#">Click or press here to enter text</a>
Indicate how approval for data use and processing is recorded	
<input type="checkbox"/>	It is not recorded:
<input type="checkbox"/>	It is recorded in a signed document
<input type="checkbox"/>	An intermediary or other operator records it
<input type="checkbox"/>	It is provided by indicating in the tool/module
<input type="checkbox"/>	Other: Please explain: <a href="#">Click or press here to enter text</a>

### Type of personal data processing

Indicate how personal data is processed:

Data processing method	
<input type="checkbox"/>	Manually (documents and other paper-based systems).
<input type="checkbox"/>	Electronic systems
<input type="checkbox"/>	Both

Indicate how personal data will be used:

Applicable	Personal data use
------------	-------------------

<input type="checkbox"/> YES <input type="checkbox"/> NO	Providing a service, pursuant to a contract.
<input type="checkbox"/> YES <input type="checkbox"/> NO	Sending email, traditional or other correspondence. Explain: <a href="#">Click or press here to enter text</a>
<input type="checkbox"/> YES <input type="checkbox"/> NO	For transfer to third parties. Explain: <a href="#">Click or press here to enter text</a>
<input type="checkbox"/> YES <input type="checkbox"/> NO	Anonymizing data for statistical or similar purposes.
<input type="checkbox"/> YES <input type="checkbox"/> NO	Other, explain: <a href="#">Click or press here to enter text</a>

### Media for transferring personal data

Indicate the media that will be used to transfer data from the source of collection to other databases, tools, information systems
<input type="checkbox"/> Via IICA's technological platform <input type="checkbox"/> Via the internet. <input type="checkbox"/> In analog form <input type="checkbox"/> Through a physical medium (device). <input type="checkbox"/> Other, specify: <a href="#">Click or press here to enter text</a>

### Providers

Indicate who the providers are and how they will manage the personal data:

Applicable	Personal data use	Observations
<input type="checkbox"/> YES <input type="checkbox"/> NO	Activities to be outsourced:	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Does the provider offer cloud computer services?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Is the personal data processed using the provider's information tools?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Is the provider storing the data?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Is the provider storing the credentials for managing the authentication and authorization systems to access the data?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Is the provider processing and storing safe copies of the data and applications?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Is the provider developing the logical access control systems (information	

	authentication) in the processing systems and in the electronic data access archives?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Is the provider outsourcing services to other entities or professionals that allows them to access IICA personal data?	
<input type="checkbox"/> YES <input type="checkbox"/> NO	Although the service that the provider offers may not entail personal data processing, does it allow for occasional access to this data (for example, cleaning services, facility maintenance, courier services, etc.)?	

### Technical/organizational measures

Indicate all the technical and organizational security measures applicable to the information systems involved in the process.

Organizational or technical security measure	Applicable	Systems in which they are applied/ observations
Encryption (hard drives, magnetic tape, etc.) on servers	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Logical access controls on the operational system and applications (administrators and users)	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Application and database access logs	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Safe copy (indicate frequency)	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Recovery testing of planned copies	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Elimination of temporary files	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Business continuity procedure	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Management and notification of incidences	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Encrypted communications	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Encrypted information	<input type="checkbox"/> YES <input type="checkbox"/> NO	

### Personal data archiving and storage

<b>Indicate how data will be archived</b>
<input type="checkbox"/> Automatic archiving

<input type="checkbox"/> Manual archiving
<b>Indicate who will host the data in electronic format.</b>
<input type="checkbox"/> The Data controller
<input type="checkbox"/> The service provider (organization or individual) to which this service has been outsourced
<input type="checkbox"/> Other: <a href="#">Click or press here to enter text</a>

**Procedure to block or erase personal data**

<a href="#">Please indicate if data is blocked</a> <a href="#">Click or press here to enter text</a>
<a href="#">If so, indicate the data blocking procedure</a> <a href="#">Click or press here to enter text</a>
<b>Please indicate the procedure to erase data</b>
<input type="checkbox"/> Automatic deletion process.
<input type="checkbox"/> Manual deletion process.
<input type="checkbox"/> Automatic anonymization process.

**Data retention period**

<b>Maximum data retention period for this project:</b> <a href="#">Click or press here to enter text</a>
<b>Justification for the data retention period:</b> <a href="#">Click or press here to enter text</a>
<input type="checkbox"/> Legal reasons (compliance with obligations), specify: <a href="#">Click or press here to enter text</a>
<input type="checkbox"/> Business needs, specify: <a href="#">Click or press here to enter text</a>
<input type="checkbox"/> Other, specify: <a href="#">Click or press here to enter text</a>

**5. Data protection by default**

Closely linked to privacy by design is privacy by default. In order to comply with this requirement, while adhering to the principle of integrity and confidentiality, all information systems, applications, programs, projects and services involving third-party personal data processing shall apply the strictest privacy protection guarantees possible, in order to protect the personal information of the subjects whose data is being processed in as wide a sphere as possible.

**5.1 Implementation of appropriate “measures”**

IICA shall adopt “appropriate privacy measures”—by design and by default—bearing in mind the nature, scope, context and purposes of the data processing, as well as the risks to the rights and freedoms of the data subjects.

Thus, IICA shall apply technical and organizational measures to guarantee that, by design and by default, only the third-party personal data that is strictly necessary for each specified purpose of the processing is processed, adhering to the following criteria:


- a. **Data minimization:** Only the minimum amount of personal data needed to produce the product or service and fulfill its purpose shall be collected, thus guaranteeing that only the personal data needed for each specific processing purpose will be processed. Thus, an analysis will have to be undertaken to determine which data is truly necessary, ensuring that the processing tools do not allow for storage of information that is not appropriate, relevant or that may be excessive for the stated purpose.
- b. **Pseudonymization of personal data:** Personal data shall not be accessible to users whose functions do not require it. Systems containing personal data shall be designed in such a way that allow one to restrict access and shall be configured to prevent it, by default, except in in cases where processing is justified. Data pseudonymization enables data to be processed in a way that prevents it from being directly attributed to an identifiable individual or legal entity (for example, identifying providers or grants via an alphanumeric code).
- c. **Transparency:** Data subjects shall be informed in a clear, concise and understandable manner that their data will be processed.
- d. **Access control:** Systems containing personal data shall allow for restrictions to be placed on personal data access by users or user profiles, in accordance with their needs, so that only staff members who truly need to access the data to carry out their functions will be able to do so. Similarly, users’ ability to facilitate access by third parties to this type of information shall be limited.
- e. **Data retention periods:** The possibility of accessing data shall be time-bound (in the case of blocking), preventing access beyond the time need to fulfill the purposes that justify its processing. Personal data shall only be kept after this period when there is a legitimate interest, legal obligation, vital interest, public interest or contractual relationship. IICA has established protocols for appropriate blocking and deletion of data, as described in **Annex 9 – Retention and deletion of personal data**, once the purpose for which it was collected has been achieved, as established in the same annex.

- f. **Personal data encryption:** An analysis of the personal data processed, by category or type of processing, may be protected by employing encryption or other similar mechanisms, as a security measure against possible unauthorized access.

Additionally, the Institute should implement other measures deemed necessary for proper protection of personal data stored in IICA's information systems, applications, programs, projects or services.



## Annex 3 – Obligation to inform data subjects and to obtain their consent

	<b>TYPE OF DOCUMENT</b>		Public (available on the IICA website)
			<input checked="" type="checkbox"/> Private (available on IICA's intranet)
<b>TITLE</b>	IICA's obligation to inform data subjects and to obtain their consent		
<b>APPLICATION</b>	All IICA Delegations and Units at Headquarters with access to and that process third-party personal data		
<b>FORMAT</b>	Electronic - Word		
<b>PAGES</b>	9		
<b>REF. APPROVAL</b>			
<b>VERSION</b>	<b>DATA</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

This procedure complies with IICA's mandatory Personal Data Protection Policy, which requires that IICA fulfill its obligations to inform data subjects that their personal data will be processed and to obtain their consent, when this is the manner that the personal data processing will be justified. The obligation to inform and to obtain consent shall be in keeping with specific requirements as described in this procedure.

### 2. Objective

To inform the staff who collect personal data about the manner in which data subjects should be informed of the conditions under which IICA is processing their data, and about obtaining their consent, when this is a necessary condition for processing.

### 3. Procedure

Administrators of the IICA Delegations in the Members States and the Units at Headquarters shall adhere to procedures that ensure compliance with the obligation to inform data subjects that their data will be processed, as well as the need to obtain their consent, when this is the basis to justify processing of their personal data.

This procedure establishes the way in which consent shall be obtained, when this is a necessary condition for processing, as well as the consequences or withdrawing this consent.

### 4. Obligation to inform data subjects

Whenever IICA intends to collect personal data, it shall inform the data subject of at least the following:

- 4.1 The purpose of processing
- 4.2 IICA's identity and contact information.
- 4.3 The lawful basis for processing (contract, consent of the data subject, legitimate interest, legal provision, etc.).
- 4.4 The possibility of exercising his/her rights to access, rectification, suppression, restriction of processing, objection and portability of data.
- 4.5 The right to withdraw consent at any time.
- 4.6 IICA's legitimate interests, in instances in which processing is based on legitimate interests.
- 4.7 The recipients or categories of recipients of the information.
- 4.8 The duration of and criteria for keeping the information, as indicated in **Annex 8** of this Manual.
- 4.9 The existence of automated decision-making or profiling.
- 4.10 The right to file a complaint or to make a report to the Institute, through the channels established in IICA's Policy for the Processing of Reports and the Protection of Whistleblowers and Witnesses, as specified in the Reporting/ Complaints section of the IICA website – [iica.int](http://iica.int). For cases in which IICA has not obtained the data from the data subject his/herself (because it was obtained from a legitimate transfer or publicly accessible sources), the data subject shall be informed.

## **5. When the data subject should be informed**

When the data is to be obtained directly from the data subject, the information shall be made available to him/her.

The data subject will not need to be informed if IICA already has the information, nor in cases when the information was not provided directly by the user, if:

- 5.1 Communicating with them is impossible or requires undue effort.
- 5.2 The data should remain confidential due to a secret legal obligation.

## **6. Obligation to provide transparent information to data subjects**

IICA shall inform data subjects in a **concise, transparent, intelligible, easily accessible** manner, using **clear and simple language**.

Thus, IICA shall be take into account the following:

- 6.1 Avoid complex formulas and unclear information that includes reference to external legal texts.
- 6.2 Information clauses should explain the relevant content in a clear manner that can be understood by all data subjects, regardless of their knowledge about the material.
- 6.3 Information should be provided in writing, including for electronic media, where appropriate.

## 7. Ways of complying with the obligation to inform data subjects

The Institute's procedures to collect information may vary greatly and must be incorporated into all of IICA's activities involving access to and processing of personal data. Thus, the means of informing the data subjects shall be adapted to the specific circumstances of each method for collecting or recording data.

Outlined below is an example of the minimum amount of information that must be provided:

Title	Information
Data controller	Inter-American Institute for Cooperation on Agriculture (IICA)
Purpose of processing	Simple description of the processing purpose
Justification for processing	Lawful basis for processing
Recipients of the personal data transfers (at the national and international levels)	Identification, where applicable, of expected data sharing or transfers
Rights of the data subjects	Indication of the possibility to exercise one's rights
Data source	Source of the data, if not provided directly by the data subject

## 8. Lawful basis for personal data processing

IICA shall have a **lawful** basis to process personal data, as defined by the Protection Data Policy. Acceptable lawful bases, according to IICA are:

- 8.1 The **consent** of the data subject.

- 8.2 The performance of a **contract** to which the subject is party.
- 8.3 The fulfillment of a **legal obligation** of IICA.
- 8.4 Protection of the **vital interests** of the data subject or another individual.
- 8.5 The fulfillment of an objective pursued in the **public interest**.
- 8.6 To satisfy a **legitimate** interest of IICA or a third party, provided that these interests do not override the fundamental interests, rights or freedoms of the data subject, who is entitled to protection of his/her personal data.

## 9. Consent

Personal data processing shall be established primarily with the consent of the data subject, as a means of providing legal grounds for this processing. Consent shall be given **specifically** for each of the purposes for which processing will be undertaken.

### 9.1 Characteristics of consent

The consent provided to IICA by the data subject shall be **freely given, informed, specific and unambiguous** and shall be applicable to all processes in which personal data is obtained from third parties.

For consent to be **unequivocal**, data subjects must demonstrate their agreement through a statement or an affirmative action. Detailed at the end of this annex, is a **Statement of Consent Model**, which may be modified only in those IICA Member States with legislation that requires additional information or utilizes a different model. Moreover, the IICA Data Protection Management Team should be advised accordingly, by sending an email to [data.protection@iica.int](mailto:data.protection@iica.int).

The consent given by the interested party shall only be considered valid when expressly and specifically provided by the data subject, whether in writing or by any other permissible means of demonstrating consent, even by verbal means that clearly reveal his/her intention. However, in all cases it requires an explicit and specific action by the data subject. Under no circumstances shall IICA accept implied consent or omission as consent.

#### a. Types of consent

- i. **Express consent:** Consent that is freely given, informed, specific and unambiguous, in which the data subject agrees to processing for a number of purposes, without the need to provide explicit consent for each and every purpose.
- ii. **Explicit consent:** Consent that is freely given, informed, specific and unambiguous for data to be processed for a specific purpose, or where applicable, for the processing of specific types of personal data, requiring therefore a voluntary and stated indication by the data subject, whether that means by selecting a checkbox or by another similar action to indicate the specific purpose or type of data to be processed.

IICA must always obtain explicit consent in the following instances of personal data processing:

- a) When processing **sensitive personal data**.
- b) When adopting automated decision-making.
- c) When transferring data to a Data processor outside of the Institute.
- d) When processing data that calls for data enrichment with information from third party databases.

## **b. Data collection and obtaining consent**

IICA shall determine the means of informing data subjects, depending on what method is used to collect or log the data (whether by telephone, through web forms, contracts, data collection forms in paper-based systems, etc.).

IICA Delegations in the Member States or Units at Headquarters whose data processing requires the collection of personal data shall utilize the information clauses that have been duly approved by IICA and that are set out at the end of this Annex.

IICA shall inform and obtain the consent of data subjects, bearing in mind the following means of justifying personal data processing:

- i. **Information collection:** IICA shall inform data subjects about the conditions governing personal data processing and explaining the relevant information.

In situations in which personal data processing does not require the consent of the data subject, given the existence of another lawful basis, once that obligation has been met, the personal data may be processed.

- ii. **Obtaining express consent:** In all cases in which no other lawful basis exists, the express consent of the data subject must be obtained.

In cases in which the specified data processing does not require the consent of the data subject, there will be no need to stipulate the right to object to processing (However, as it has been explained, if there is any doubt that a lawful basis exists, consent should be requested.

When consent is sought for various purposes, under no circumstances will failure to consent to one of them imply a denial of service, if the service does not necessitate processing.

## **c. Verification of compliance with the obligation to inform and obtain consent**

IICA must demonstrate that it has informed the data subject and obtained his/her consent.

To this end, IICA shall retain digital, electronic or physical proof of the information clauses and/or contracts that have been submitted, facilitated, signed, accepted and/or shown, regardless of the method used.

In accordance with the channel through which the procedure was done, IICA shall ensure that it has sufficient and valid proof to enable it to effectively prove that it has fulfilled its obligation to inform, and where applicable, to obtain the freely given, informed, specific and unambiguous consent directly from the data subject.

If this was via the telephone, it is advisable that calls be recorded, and that the Institute retain copies of the documents accepted and/or signed by the data subjects, as well as the electronic logs generated by the platforms through which the procedure took place.

Mindful of the fact that consent must be verifiable and that individuals collecting personal data must be able to demonstrate that data subjects provided their consent, IICA has committed to conducting a periodic review of its consent record systems, through its institutional bodies, so that, in the event that, if required, it will be able to verify that data subjects have been informed and provided their consent.

To that end, each IICA Delegation in the Member States or Unit at Headquarters shall implement the necessary technical and organizational measures to demonstrate that consent has been properly obtained.

#### **d. Withdrawing consent**

IICA shall guarantee the data subjects' right to withdraw consent, providing them with a **simple and free** medium through which they may do so.

The Institute shall include a link on its website for the purpose of withdrawing consent, providing an email address for that purpose, so that the matter may be addressed at the level of each IICA Delegation or at Headquarters.

If a data subject withdraws consent, IICA shall be obliged to discontinue processing of his/her data and to respond to the data subject.

If the data of the data subject has been shared with a third party, IICA shall advise the third party about the withdrawal of consent. Once the third party has responded, IICA shall disable all the data stored on the data subject.

In any case, the withdrawal of consent cannot be applied retroactively.

## 10. Statement of Consent Model

In compliance with the provisions of the Personal Data Protection Policy of the Inter-American Institute for Cooperation on Agriculture, hereinafter called IICA, I declare that:

I have been explicitly informed that the data provided to IICA will be processed internally for its exclusive/limited purposes in a database owned and protected by IICA.

I understand that this information shall be used solely for the stated purposes and that I will be advised of any change in these conditions, through the established communication channels. Similarly, I commit to directly informing IICA about any change in this information and accept that omitting to do so will release IICA from any liability regarding the accuracy of said information.

IICA has advised that its database is administered in a decentralized manner, and that whenever necessary, it may provide greater details about the personal data that is housed therein. This request should be made by sending a signed note to xxxx@iica.int<sup>1</sup>.

To indicate my agreement with the above declaration, I hereby sign this document on [City, Country] on [day, month, year].

Name:

ID:

Signature:

Authorized email address for correspondence:

## 11. Contractual clause applicable to contracts with suppliers and consultants for the procurement of goods and services

The following clause must be included in the contracts that IICA signs with suppliers and consultants for the procurement of goods and services.

---

<sup>1</sup> IICA Delegations in the Member States and Units at Headquarters shall indicate the official email address.

If the contract with the supplier/consultant indicates that IICA shall transfer personal data to a third party for processing, the contract included in section 3.2. of Annex 6, below, must also be signed.

[CLAUSE IN THE CONTRACT] - Data of the parties to the contract

1. Each of the Parties shall be advised that the information of the data subject or the contact person of the representatives and employees that are processed within the scope of this contract, as well as other information exchanged during the provision of services, shall be processed by the other Party to facilitate the development, execution and management of the contractual relationship for service provision. Data shall be processed specifically to ensure performance of the contractual relationship and shall be kept for the duration of the contract and even after, until all obligations derived hereunder are delivered.
2. The respective personal data controllers shall be each of the companies provided with the data of the interested parties, whose contact information is included in the preamble of this contract.
3. The Parties may share personal data with: (i) Public Administrations and legal authorities to comply with IICA's legal and fiscal obligations; (ii) auditing firms to comply with legal obligations regarding account auditing or due to any legitimate interest consistent with proper governance of the Company; and/ or (iii) third parties involved in managing the contractual activities, such as other IICA units, where necessary for the performance of the contract or at their request , and/or with providers that require access to personal data to provide services that have been outsourced to them by the Parties.
4. In cases in which the Parties must engage the services of providers in countries that do not have data processing legislation equivalent to IICA's Personal Data Protection Policy, the contract will be finalized only after all the requirements established by IICA's personal data protection regulations have been satisfied, while also applying the necessary guarantees and safeguards to preserve data privacy.
5. IICA may send the contact data of the representatives and employees of the other Party to other IICA delegations and offices, where necessary for the execution or performance of a contract, and/or where necessary, at their request.
6. The data subjects may submit their request for access to their personal data, rectification, suppression, portability and restriction of processing or their objection to processing to the registered office of each Party and/or by sending it to the following email addresses: [...] and [...].



## **12. Clause to be included in tenders**

[CLAUSE IN THE CALL FOR TENDERS]. - PERSONAL DATA INCLUDED IN THE TENDER

1. In compliance with applicable data protection legislation, this is to advise that the personal data of the legal representative and/or contact persons that are indicated in the bid proposal shall be processed as personal data, for the purpose of managing the ongoing bidding process, and where applicable, for the performance of the contract.
2. In the event that the bid proposal includes the personal data of other individuals (whether persons employed to the bidding entity or persons from other entities that are involved in the bid proposal that has been presented), the bidder shall inform all of them that their data will be processed, in accordance with the terms contained in this clause, thereby releasing IICA from all liability.
3. As the Data controller, IICA guarantees that data subjects may exercise their rights of access, rectification, withdrawal and objection to the personal data provided for these purposes, by sending a written request, with a digital certification or a copy of their identification document to IICA's Data Protection Management Team, using the established mechanisms of the Institute, namely the Reporting/ Complaints section on its website [iica.int](http://iica.int) or by sending an email to: [ec.ce@iica.int](mailto:ec.ce@iica.int).

## **13. Clause to be included in legal instruments, excluding those with suppliers and consultants**

The following clause must be included in the legal instruments that IICA signs with its counterparts and partners.

If the legal instrument indicates that IICA shall transfer personal data to a third party for processing, Annex 6.3.2, below, must also be signed.


General Clause:

IICA is seeking to provide adequate protection of the personal data to which it has access in carrying out its activities and implements strict measures to address reports of improper processing of personal data. To that end, among other measures, it has established a Personal Data Protection Policy.

[NAME OF COUNTERPART] acknowledges that he/she has read, understood and accepts the mandatory application of this Policy in the execution of this agreement. The Policy is available on the [iica.int](http://iica.int) website.

IICA commits to addressing any query regarding the scope of this Policy and is providing the following email for this purpose: [data.protection@iica.int](mailto:data.protection@iica.int)

## Annex 4 – Exercising and addressing the rights of data subjects

		<b>TYPE OF DOCUMENT</b>	<input checked="" type="checkbox"/> Public (available on the IICA website)
			<input type="checkbox"/> Private (available on IICA's intranet)
<b>TITLE</b>		Exercising and addressing the rights of data subjects	
<b>APPLICATION</b>		All IICA Delegations and Units at Headquarters with access to and that process third-party personal data	
<b>FORMAT</b>		Electronic – Word	
<b>PAGES</b>		29	
<b>REF. APPROVAL</b>		SC/DG-404, SEPTEMBER 24, 2021	
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

This procedure has been established to comply with the provisions of IICA's Personal Data Protection Policy and this Manual regarding requests to exercise and address rights to access, rectification, erasure, restriction of processing, objection, portability of data and the right to not be subject to automated individualized decisions.

### 2. Objective

To address, process and manage requests to exercise the rights established in the IICA's Personal Data Protection Policy.

### 3. Procedure

Rights of access, rectification, suppression, restriction, objection, portability of data and the right to not be subject to automated individualized decisions, while also entitling individuals to be informed of, to modify and to suppress their personal data, as well as to request that it be processed for a limited time period. The data subjects are also entitled to ensure that they are not subject to decisions, based solely on automated processing. The rights recognized in this Policy allow individuals to defend their privacy and to control the use that is made of their personal data.

The guidelines contained herein shall be respected at all times by third parties that are serving as processors and by IICA staff, in particular those whose functions involve addressing and managing requests from the public or from data subjects. These guidelines ensure proper processing and handling of requests from data subjects to exercise the rights outlined in the IICA Personal Data Protection Policy.

The procedure to exercise the rights and address the requests of data subjects are described in **Section 5 – Procedure for exercising and addressing requests regarding rights**, contained in this Annex.

#### **4. Recognized rights of the data subject**

##### **4.1 Right of access**

The right of access enables the interested party or data subject to obtain information regarding whether his/her personal data is being processed by IICA. If that is the case, the data subject has the right to access and obtain a copy of his/her personal data. Specifically, IICA must provide the following information to the data subject:

- a. The purpose(s) of the processing.
- b. The categories of personal data being processed (personally identifiable information, data on personal characteristics, employment data, etc.).
- c. The recipients of the data (to whom the data has been or will be disclosed).
- d. The period for which the data will be stored, or the criteria used to determine that period, if it differs from the provisions established in this Manual.
- e. The source of the data, if it was not provided by the data subject.
- f. The existence of automated decision-making, including profiling, providing information about the logic involved and the consequences of such processing.
- g. Where personal data is transferred to third parties, information about the appropriate safeguards relating to the transfer.

##### **4.2 Right to rectification**

The data subject may exercise the right to rectification when he/she considers that his/her data is inaccurate or incomplete, in which case IICA shall modify or update the data, in accordance with the data subject's request.

##### **4.3 Right to erasure**

The right to erasure enables the data subject to request that his/her personal data be erased under any of the following circumstances:

- a. The personal data is no longer required for the purposes for which it was initially collected or processed.
- b. The data subject formally withdraws the consent on which the processing is based, for cases where he/she consented to the processing of his/her personal data for one or several specific purposes; except for cases where it is established that the data subject cannot stop the processing of personal data.
- c. The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- d. The personal data has been unlawfully processed.

- e. The personal data must be erased to comply with a legal obligation that applies to IICA.

The right to erasure **shall not apply** when processing is necessary:

- a. To exercise the right of freedom of expression and information.
- b. To meet a legal obligation that requires the processing of data by IICA, or to comply with a task carried out in the public interest or in the exercise of official authority vested in IICA.
- c. For reasons of public interest in the area of public health.
- d. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as this right is likely to render impossible or seriously impair the achievement of the objectives of that processing.
- e. For the establishment, exercise or defense of legal claims.

#### **4.4 Right to restrict processing**

The data subject shall have the right to restrict IICA from processing the data it holds where one of the following conditions applies:

- a. The data subject has exercised his/her right to rectification or to object and IICA is in the process of determining whether to address this request.
- b. The processing is unlawful, which would result in erasure of the data, but the data subject opposes this.
- c. The data is no longer needed for processing, which would also result in erasure, but the data subject requests restriction of processing because he/she needs the data for the establishment, exercise or defense of legal claims.

During the period of time that this restriction applies, and with the exception of storage, IICA shall only process such data:

- a. With the data subject's consent.
- b. For the establishment, exercise or defense of legal claims.
- c. To protect the rights of another individual or legal entity.
- d. For reasons of important public interest, to protect the rights of another individual or legal entity, or for reasons of public interest.

#### **4.5 Right to object**

The data subject has the right to object to his/her personal data being processed:

- a. On grounds relating to his/her particular situation, where the processing of personal data is necessary for the performance of a task carried out for reasons of public interest or in the exercise of official authority vested in IICA; or necessary to satisfy legitimate interests

sought by IICA or a third party, provided that they do not override the interests, rights and freedoms of the data subject with respect to data protection (particularly when the data subject is a child), including profiling based on those provisions.

- b. Where the purpose of processing such personal data is to disseminate information related to IICA's work.
- c. Where personal data is processed for scientific or historical research purposes or statistical purposes, or on grounds relating to his/her particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

#### **4.6 Right not to be subject to automated individual decision-making**

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or affecting him/her. However, IICA may base a decision on automated processing only if it:

- a. Is necessary for entering into or performance of a contract.
- b. Is based on the data subject's explicit consent.

In the abovementioned cases, IICA may make these types of decisions despite the objection of the data subject.

#### **4.7 Right to personal data portability**

The data subject shall have the right to receive the personal data that he/she provided to IICA, in a structured, commonly used and machine-readable format, and shall have the right to transmit that data to another controller. Therefore, when the data subject exercises his/her right of portability, IICA must adequately respond to such a request.

Furthermore, if required by the data subject, IICA must directly transmit his/her personal data to another data controller, where technically feasible.

In particular, the right to data portability shall cover the personal data directly provided by the data subject during the relationship with IICA, as well as personal data derived from the service provided and inherent to it (consumption, schedules, etc.), excluding data derived from IICA's own processing and following the application of IICA's own methodologies.

- a. **Right to receive personal data:** In general terms, the right to data portability can be understood, on the one hand, as the right of the data subject to receive his/her personal data processed by IICA and to store it for subsequent personal use on a private device, without transmitting it to another data controller. In this regard, the right to portability can be understood to mean a right that complements the right of access—a simple way for the data subject to manage and use his/her personal data him/herself.

If the data subject wishes to receive his/her personal data from IICA, the Institute must provide it in a structured, commonly used and machine-readable format.

- b. **Right to transmit personal data from one data controller to another data controller:** The right to portability of personal data also includes the right of data subjects to request the transfer of their personal data from one controller (i.e. IICA) to another controller, without hindrance. In this regard, IICA must provide data subjects with the possibility of transferring, copying or transmitting the personal data it holds to a third party, where technically feasible.
- c. **Responsibility for processing:** IICA will not be held responsible for the processing of personal data handled directly by the data subject himself/herself or by a third party that receives such data at the request of the data subject, once IICA has made the data available following the instructions of the requesting party.

In this regard, the right to portability of personal data does not oblige IICA to retain personal data for longer than necessary or beyond the specified retention period. Therefore, IICA will not be obliged to retain such data simply to respond to a possible request for data portability.

- d. **Data portability versus other rights of the data subject:** Exercising the right to data portability does not affect any other rights of the data subject. In other words, the data subject may continue to use and benefit from IICA's services even after having exercised the right to data portability.

Data portability will not automatically involve the erasure of data from IICA's systems, nor will it affect the original retention period that applied to the data that has been transmitted. The data subject may therefore exercise his or her rights with respect to IICA for as long as IICA continues to process his/her data. Therefore, if a data subject discovers that the personal data he/she requested to exercise the right to portability does not fully satisfy his/her request, IICA must fully satisfy any subsequent requests for personal data in accordance with the data subject's right of access.

- e. **How and when to apply the right to data portability:** In order for a data subject to exercise the right to data portability, processing operations must be based on the data subject's consent, or on a contract to which the data subject is a party. Furthermore, this right may only be applied when data processing is carried out through automated means, which excludes data processing on paper.

A data subject may only exercise his/her right to portability for data relating to the person in question and for data that he/she provided to IICA.

- f. **Data affected:** The right to data portability applies only to data of a personal nature. Therefore, any anonymous data or data that does not relate to the data subject is excluded from this right.

Another condition in order to exercise the right to portability is that the data must have been consciously and actively provided by the data subject him or herself. Nevertheless, IICA must also include any personal data generated and collected through users' activities in response to a request for data portability.

With respect to data provided by the data subject, it is important to distinguish between two different data categories, depending on their origin, to determine whether they are covered by the right to data portability:

- i. Data actively and consciously provided by the data subject: for example, name, address or telephone number.
- ii. Observed data that was "provided" by the data subject based on his/her relationship or involvement with IICA: for instance, location data when a user searches for information through an IICA web page or application.

With respect to the right to data portability, IICA shall only take into account data provided by the data subject or observed on the basis of his/her relationship or involvement with IICA, but not "inferred" or "deduced" data. In other words, the right to portability only includes data "provided by the data subject", meaning data that is related to the data subject's activity or based on the observation of a person's behavior, but not the subsequent analysis of such behavior.

**g. The right to portability shall not adversely affect the rights and freedoms of third parties**

**i. Regarding personal data pertaining to other data subjects**

Personal data transmitted by IICA to another data controller in response to the exercise of the right to portability may not include personal data of other data subjects in cases where such data may be processed in a manner that adversely affects the rights and freedoms of such data subjects.

**ii. Regarding data covered by intellectual property and trade secrets**

The impossibility of interfering with the rights and freedoms of third parties when exercising the right to data portability also includes trade secrets or intellectual property and, in particular, copyrights protecting computer rights, with a view to protecting IICA's business model and the data controllers to whom data is transferred. Therefore, in addressing requests to exercise the right to data portability, IICA must take into account the abovementioned rights; however, such considerations must never entail a refusal to provide information to the data subject.

Consequently, although IICA must take into account the intellectual property rights and trade secrets of certain information, such rights may not serve as the basis for a refusal to respond to



a portability request by the data subject, in so far as IICA must use the necessary means to transmit the data in a manner that does not make information covered by trade secrets or intellectual property rights publicly available.

## **h. Security of the data**

IICA will process personal data in a manner that ensures its security, including protection against unauthorized or unlawful processing activity and against its accidental loss, destruction or damage, through the application of appropriate technical or organizational measures when such data is under the Institute's responsibility. IICA will not be liable in any way for the processing carried out by a new data controller, where the data subject has requested portability from IICA to transfer data to a third party or new data controller.

## **i. Information provided to data subjects**

In order to comply with the right to data portability established in IICA's Personal Data Protection Policy, the Institute must inform data subjects regarding the availability of this right.

## **5. Procedure for exercising and addressing requests regarding rights**

### **5.1 Previous considerations**

With respect to a data subject's ability to exercise the rights established in IICA's Personal Data Protection Policy, the following shall be taken into account:

- a. The Institute must adopt measures to verify the identity of those exercising their rights, by requesting that they submit proof of identity.
- b. The data subject must exercise these rights him or herself, unless he/she is disabled or a minor, in which case, these rights may be exercised by a legal representative, who must provide proof of this condition (by means of a document that grants him/her the power to serve as representative).
- c. These rights may also be exercised through a voluntary representative who has been expressly designated, in writing, to exercise this right. In this case, a form of ID must be provided for both the represented party and the representative, to clearly certify their identities, along with a document in which the former confers the latter with power of representation.
- d. Requests to exercise these rights will be denied if no form of identity is provided for the data subject or, where applicable, for the representative and the corresponding represented party.

- e. IICA must provide visible, accessible and simple procedures and forms, as defined in this procedure, in order to facilitate the exercise of rights by data subjects.
- f. IICA must provide electronic means through which data subjects can submit requests to exercise their rights.
- g. When a data subject submits a request through electronic means, IICA will provide information through electronic means, unless the data subject requests that it be provided through another means.
- h. In cases where IICA processes a substantial amount of information about a data subject, the Institute will request that he/she specify the information he/she wishes to access.

Exercise of these rights must be free of charge for the data subject, except where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive nature. IICA will keep a copy of all of these requests and record the reason for which they are considered unfounded or excessive. In these cases, the data subject will be informed that his/her request will be addressed at a cost.

- i. In the case of requests to exercise the right to rectification, erasure or restriction of processing, IICA must inform each of the recipients to which the modified personal data was transferred of the concrete operation that was carried out, unless this proves impossible or involves disproportionate efforts. Furthermore, if requested by the data subject, IICA must inform him/her of the recipients of this data.

## **5.2 Receipt of requests**

IICA's website will provide a link for each Delegation in its Member States, enabling users to access an institutional email address through which they can submit requests to exercise their rights in a simple, free-of-charge manner.

## **5.3 Minimum requirements of requests to exercise rights**

In order to be processed by IICA, all requests to exercise rights must meet at least the following requirements:

#### MINIMUM REQUIREMENTS – REQUEST TO EXERCISE RIGHTS

- Name, last name and photocopy of the data subject's identity document* If the data subject is represented by a third party: <ul style="list-style-type: none"><li>• Name, last name and photocopy of the data subject's identity document.</li><li>• Name, last name and photocopy of the representative's identity document.</li><li>• Accreditation document for the representative.</li></ul> * The photocopy of the identity document may be substituted by any other valid means of identification.
- Concrete request being made.
- Email address to receive notifications, date and signature of the person submitting the request.
- Supporting documentation pertaining to the request being made, as applicable.
- In the case of requests to exercise the right to access video surveillance footage, the data subject must also provide information regarding the moment the image was taken as well as a photograph that enables him/her to be identified in the footage.

IICA will respond to all requests from a data subject to exercise his or her rights, unless the Institute is processing personal data for a purpose that does not require the identification of the data subject and it can demonstrate that it cannot identify the data subject. Furthermore, where IICA has reasonable doubts regarding the identity of a data subject, it may request additional information to confirm his/her identity.

However, where a data subject does provide additional information that allows for identifying him/her, IICA may not refuse to respond to the data subject's request. Furthermore, where the data collected is linked to pseudonyms or unique identifiers, IICA may implement appropriate procedures to enable an individual to submit a request for data portability and to receive data relating to that request.

In any case, IICA will implement an authentication procedure to determine, with certainty, the identity of the data subject.

#### 5.4 Timeframe for responding to requests to exercise rights

IICA shall resolve and respond to a data subject's request to exercise his/her rights within **one calendar month**. This period may be extended by **two additional calendar months in the case of particularly complex requests**, and the data subject must be informed of such extensions within one month of receipt of the request, stating the reasons for the delay.

If the request is not valid or does not meet the minimum requirements, IICA will reject it and will respond to the data subject indicating the reason for which the request was rejected or requesting the necessary documentation to remedy the formal deficiencies and be able to respond to the request to exercise rights.

If IICA decides not to process the data subject's request, it shall inform the data subject of the **reason for rejecting the request**, no later than **one calendar month** following receipt of the request.

IICA shall, in all cases, respect the obligation to respond within the established timeframes, even in cases where the response is negative.

As a first step, IICA will verify whether the request received complies with the minimum requirements set out in section **5.3 - Minimum requirements of requests to exercise rights**, detailed above.

If the request is accepted and it meets the minimum requirements, IICA will follow the steps indicated below to process the request:

- a. Identify the IICA systems in which the data subject's data is processed.
- b. Execute the right requested in the corresponding systems or applications, based on the analysis carried out in point a. above, as follows:
  - i. **Right of access**: extraction of data requested by the data subject.
  - ii. **Right to rectification**: modification of the data requested by the data subject and/or completion of incomplete data.
  - iii. **Right to erasure**: elimination or blocking of data requested by the data subject.
  - iv. **Right to object**: blocking the use of the data subject's data for commercial activities or the transfer of data to other entities.
  - v. **Right to restrict processing**: suspension of processing of the data subject's data.
  - vi. **Right to data portability**: transmission of data to the data subject him or herself or to another data controller.
  - vii. **Right not to be subject to individualized decision-making**: decision-making will not be based solely on automated processing.
- c. Identify which persons may store the data subject's documentation in temporary files or non-automated systems (on paper). Request the identified documentation, based on the needs associated with the right exercised by the data subject.

- d. Carry out, if applicable, the necessary actions in the temporary files or non-automated systems, based on the right requested through the documentation obtained in point c. above.
- e. Respond once the right exercised by the data subject has been processed.
- f. File all of the documentation collected when processing the right and record the request made by the data subject in the record of requests.

Regarding the exercise of rights in the context of video surveillance files, IICA must also take the following into account:

- a) The right to rectification is not possible due to the nature of the data (images taken in actual life that reflect an objective fact).
- b) The right to object also presents considerable difficulties, namely the impossibility of not taking images of the data subject in terms of the video surveillance systems used for private security purposes, as the need to provide security would override the request.
- c) With respect to the right to access data, as provided for in this Procedural Manual, the data subject must provide, as supporting documentation, an up-to-date image that allows for identifying him/her and certifying that his/her image has been captured on file. Accessing these images is virtually impossible without compromising the image of a third party; therefore, when exercising and addressing this right, access may be provided by means of a certified text that indicates, as precisely as possible and without affecting the rights of third parties, the data that has been processed.

## **5.5 Responding to a request to exercise rights**

IICA must respond to the data subject to accept or reject the request within the established timeframe. In either case, the response will be sent via e-mail, with acknowledgement of receipt.

Once a response has been sent to the data subject, the IICA Delegation in the corresponding Member State or Headquarters will update the record of requests described in section **5.6 – Record of requests to exercise rights** below.

The Institute will ensure that the data requested by the data subject is transferred through secure electronic or digital means.

A data subject's right to data portability shall not oblige IICA to adopt or maintain processing systems that are technically compatible with those of other organizations.

Where a request for portability involves a large volume of data or a complex data structure, IICA shall provide the data in a summarized format using control panels that enable the data subject to transfer subsets of the personal data rather than the entire catalog.

## **5.6 Record of requests to exercise rights**

Requests to exercise rights received by IICA must be recorded in a control system. This shall be the responsibility of the Administrator of the corresponding IICA Delegation in the Member States or the officer(s) of the corresponding Unit at Headquarters who have access to or who process personal data. The samples are included in section 5.7 below.

The record must include at least the following fields:

- a. Name and last name of the data subject.
- b. Identity document of the data subject.
- c. Right exercised.
- d. Means through which the request to exercise a right was received.
- e. Date on which the data subject submitted the request to IICA.
- f. Date on which the right was executed by IICA.
- g. Date on which a response was provided to the data subject.

## **5.7 Sample forms for exercising rights**

The validated forms included at the end of this annex must be made available to data subjects to enable them to submit requests to exercise the right of access, right to rectification, right to erasure, right to restrict processing, right to portability and/or the right to object, provided that the formal and substantive requirements established in this procedure are met.

### **a. Relevant documents**

- i. Request to exercise the right of access.
- ii. Request to exercise the right to rectification.
- iii. Request to exercise the right to erasure.
- iv. Request to exercise the right to restrict processing.
- v. Request to exercise the right to portability.
- vi. Request to exercise the right to object.

### **b. Sample responses to requests to exercise rights**

The end of this Annex includes sample responses with which IICA can correctly address and respond to requests to exercise data subjects' **right of access, right to rectification, right to erasure, right to restrict processing, right to portability and/or the right to object.**

i. **Relevant documents:**

- a) Positive response to a request to exercise the right of access where data was processed by IICA.
- b) Negative response to a request to exercise the right of access where data was not processed by IICA.
- c) Positive response to a request to exercise the right to rectification.
- d) Positive response to a request to exercise the right to erasure through data blocking.
- e) Positive response to a request to exercise the right to erasure through the deletion of data.
- f) Positive response to a request to exercise the right to restrict processing.
- g) Positive response to a request to exercise the right to portability.
- h) Positive response to a request to exercise the right to object.



## Exercising of Personal Data Protection rights

### Sample forms (for data subjects)

#### Sample 1: Exercising the data subject's right of access

##### INFORMATION ABOUT THE DATA CONTROLLER

- **Data Controller: Inter-American Institute for Cooperation on Agriculture (hereinafter, "IICA")**
- **Legal identification number of IICA:** (identification number)
- **Registered office: (address of the IICA Delegation in the corresponding country or Headquarters)**

##### PETITIONER'S DATA

I, the undersigned, [...], of legal age, residing in [...], town [...] P.O. Box [...] province [...], identity card number [...], of which a copy is attached, exercise my right of access, by means of this document, in accordance with the provisions of IICA's Personal Data Protection Policy, and, consequently,

##### I HEREBY REQUEST

That the right of access to my data be provided free of charge within a maximum period of one month following receipt of this request. This period may be extended by IICA for an additional two months if necessary, depending on the complexity and number of requests received.

That the information be sent via email.

That, in the event that the Data Controller decides that the request submitted is not applicable, that I be informed within a maximum period of one month following receipt of the request.

Furthermore, I request that the information include, in a legible and intelligible form, confirmation as to whether or not IICA is processing data concerning me and, if so, that the following information be provided to me:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom my personal data has been or will be disclosed;
- the proposed storage period of my personal data or, if not possible, the criteria used to define that period;

- the existence of the right to request from IICA the rectification or erasure of personal data or restriction of processing of personal data about me, or to object to such processing;
- where the data is not collected from me, all available information on its origin; and
- the existence of automated decision-making, including profiling, and, at least in such cases, meaningful information on the logic used, as well as the importance and envisaged consequences of such processing for me.

In [...], at [...] of [...] of [...]

Signed [...]

Identity document [...]

The right of access involves a request for information regarding personal data processed by IICA. Requests to exercise this right are submitted to the Data Controller, who holds the data. This right may also be exercised through a legal representative, in which case, in addition to submitting the data subject's identity card or other proof of identity, an identity card or other proof of identity must be provided for the representative, along with a document that serves as proof of his/her authority to represent the data subject.

## Sample 2: Exercising the data subject's right to rectification

### INFORMATION ABOUT THE DATA CONTROLLER

- **Data Controller: Inter-American Institute for Cooperation on Agriculture (hereinafter, "IICA")**
- **Legal identification number of IICA: (identification number)**
- **Registered office: (address of the IICA Delegation in the corresponding country or Headquarters)**

### PETITIONER'S DATA

I, the undersigned, [...], of legal age, residing in [...], town [...] P.O. Box [...] province [...], identity card number [...], of which a copy is attached, exercise my right to rectify the attached data, by means of this document, and provide the corresponding justification, in accordance with the provisions of IICA's Personal Data Protection Policy, and, consequently,

### I HEREBY REQUEST

That the personal data for which the right is being exercised be rectified, within a maximum period of one month following receipt of the request, and that I be notified in writing of the result of the rectification carried out.

That, in the event that the Data Controller decides that not all or only part of the proposed rectifications can be made, that I be informed of the grounds for such a decision within a maximum period of one month following receipt of the request.

In [...], at [...] of [...] of [...]

Signed [...]

Identity document [...]

The right to rectification involves a request submitted to the Data Controller to ensure that personal data truthfully reflects the data subject's current situation. The data subject must specify the data to be rectified. This right may also be exercised through a legal representative, in which case, in addition to submitting the data subject's identity card or other proof of identity, an identity card or other proof of identity must be provided for the representative, along with a document that serves as proof of his/her authority to represent the data subject.

### Sample 3: Exercising the data subject's right to erasure

#### INFORMATION ABOUT THE DATA CONTROLLER

- **Data Controller: Inter-American Institute for Cooperation on Agriculture (hereinafter, "IICA")**
- **Legal identification number of IICA: (identification number)**
- **Registered office: (address of the IICA Delegation in the corresponding country or Headquarters)**

#### PETITIONER'S DATA

I, the undersigned, [...], of legal age, residing in [...], town [...] P.O. Box [...] province [...], identity card number [...], of which a copy is attached, exercise my right to erasure, by means of this document, in accordance with the provisions of IICA's Personal Data Protection Policy, and, consequently,

#### I HEREBY REQUEST

That the personal data for which the right is being exercised be erased, within a maximum period of one month following receipt of this request, and that I be notified in writing of the result of the erasure undertaken.

That, in the event that the Data Controller decides that not all or only part of the data for which the right is being exercised can be erased, that I be informed of the grounds for such a decision within a maximum period of one month following receipt of the request.

In [...], at [...] of [...] of [...]

Signed [...]

Identity document [...]

The right to erasure involves a request to delete data that is no longer needed or relevant for the purpose for which it was collected. Requests for partial erasure of data must specify the data that should be erased. Data will be blocked or, in other words, identified and set aside to prevent its processing. This right may also be exercised through a legal representative, in which case, in addition to submitting the data subject's identity card or other proof of identity, an identity card or other proof of identity must be provided for the representative, along with a document that serves as proof of his/her authority to represent the data subject.

## Sample 4: Exercising the data subject's right to restriction of processing

### INFORMATION ABOUT THE DATA CONTROLLER

- **Data Controller: Inter-American Institute for Cooperation on Agriculture (hereinafter, "IICA")**
- **Legal identification number of IICA: (identification number)**
- **Registered office: (address of the IICA Delegation in the corresponding country or Headquarters)**

### PETITIONER'S DATA

I, the undersigned, [...], of legal age, residing in [...], town [...] P.O. Box [...] province [...], identity card number [...], of which a copy is attached, exercise my right to restrict processing, by means of this document, in accordance with the provisions of IICA's Personal Data Protection Policy, and, consequently,

### I HEREBY REQUEST

That processing of the personal data for which the right is being exercised be restricted, within a maximum period of one month following receipt of this request, and that I be notified in writing of the result of the restriction carried out.

That, in the event that the Data Controller decides that total or partial restriction of processing is not possible, that I be informed of the grounds of such a decision within a maximum period of one month following receipt of the request.

In [...], at [...] of [...] of [...]

Signed [...]

Identity document [...]

The right to restrict processing is the right to restrict processing of data that is no longer needed or relevant for the purpose for which it was collected. Requests for partial restriction of processing must specify the data involved. Data will be blocked or, in other words, identified and set aside to prevent its processing. This right may also be exercised through a legal representative, in which case, in addition to submitting the data subject's identity card or other proof of identity, an identity card or other proof of identity must be provided for the representative, along with a document that serves as proof of his/her authority to represent the data subject.

## Sample 5: Exercising the data subject's right to data portability

### INFORMATION ABOUT THE DATA CONTROLLER

- **Data Controller: Inter-American Institute for Cooperation on Agriculture (hereinafter, "IICA")**
- **Legal identification number of IICA: (identification number)**
- **Registered office: (address of the IICA Delegation in the corresponding country or Headquarters)**

### PETITIONER'S DATA

I, the undersigned, [...], of legal age, residing in [...], town [...] P.O. Box [...] province [...], identity card number [...], of which a copy is attached, exercise my right to data portability, by means of this document, in accordance with the provisions of IICA's Personal Data Protection Policy, and, consequently,

### I HEREBY REQUEST

That portability be granted for the personal data for which the right is being exercised, and that the data be received from/transmitted to IICA in a structured, commonly used and machine-readable format, within a maximum period of one month following receipt of this request, and that I be notified in writing of the result of the portability carried out.

That, in the event that the Data Controller decides not to grant the proposed portability, that I be informed of the grounds of such a decision within a maximum period of one month following receipt of the request.

In [...], at [...] of [...] of [...]

Signed [...]

Identity document [...]

The right to portability is a data subject's right to receive his/her data in a structured, commonly used and machine-readable format, and to transmit that data to another controller without hindrance on the part of the Data controller to which the data was provided. This right may also be exercised through a legal representative, in which case, in addition to submitting the data subject's identity card or other proof of identity, an identity card or other proof of identity must be provided for the representative, along with a document that serves as proof of his/her authority to represent the data subject.

## Sample 6: Exercising the data subject's right to object

### INFORMATION ABOUT THE DATA CONTROLLER

- **Data Controller: Inter-American Institute for Cooperation on Agriculture (hereinafter, "IICA")**
- **Legal identification number of IICA: (identification number)**
- **Registered office: (address of the IICA Delegation in the corresponding country or Headquarters)**

### PETITIONER'S DATA

I, the undersigned, [...], of legal age, residing in [...], town [...] P.O. Box [...] province [...], identity card number [...], of which a copy is attached, exercise my right to object, by means of this document, in accordance with the provisions of IICA's Personal Data Protection Policy, and, consequently,

### I HEREBY REQUEST

That, within a maximum of one month following receipt of this request, processing be terminated based on the right to object, and for the following reason(s):

- If the purpose of the processing is to conduct marketing activities.
- If the purpose of the processing is the adoption of a decision regarding, me, as the data subject, and that is based solely on automated processing of personal data.

That, in the event that the Data Controller decides not to grant the proposed objections, in part or in full, that I be informed of the grounds of such a decision within a maximum period of one month following receipt of the request.

In [...], at [...] of [...] of [...]

Signed [...]

Identity document [...]

The right to object involves a request submitted to a given Data controller to cease the processing of specific personal data. This right is requested from the Data Controller who holds the data. This right may also be exercised through a legal representative, in which case, in addition to submitting the data subject's identity card, an identity card must be provided for the representative, along with a document that serves as proof of his/her authority to represent the data subject.

## Exercising Personal Data Protection rights

### Sample responses (on the part of IICA)

#### Sample 1: Positive response to a request to exercise the right of access (Where data is processed by the Data Controller, i.e. IICA)



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to access data held by the Data Controller: INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [Legal Identification No.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with IICA's Data Protection Policy regarding exercising the right of access, we hereby inform you that, as at the date of the abovementioned request to exercise the right of access, IICA is processing personal data of which you are the owner.

Information on the data processed is provided below:

- (i) We hereby inform you that we have obtained your data from [...]
- (ii) The data categories we process are [...]
- (iii) Your data is being processed for the following purposes:
  - [...]
  - [...]
- (iv) IICA will retain your personal data for the following periods:
  - For [the purpose of [...] your data will be retained [...]. It will not be possible to define the exact period during which your personal data will be retained; however, we inform you that your data will be retained for the period in which the contract is in force and, following its termination, for the limitation period for any liabilities arising from the contract].
  - For [the purpose of [...] your data will be retained [...]. It will not be possible to define the exact period during which your personal data will be retained; however, we inform you that your data will be retained for the period in which the contract is in force and, following its termination, for the limitation period for any liabilities arising from the contract].



- (v) Your data has been transferred to:
- [...] for the purpose of [...]
  - [...] for the purpose of [...]

IICA does not make automated decisions, including profiling. We also inform you that, at any time, data subjects may exercise the right to rectification, right to erasure, right to restrict processing, right to portability and the right to object to the processing of personal data, in accordance with current regulations, as well as to withdraw consent initially granted, in accordance with the provisions of IICA's Data Protection Policy.

We understand that the information provided to you through this document meets the requirements to exercise your right of access.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,

IICA

**Sample 2: Negative response to a request to exercise the right of access  
(Where data is not processed by the Data controller, i.e., IICA)**



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to access data held by the Data Controller: INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [LEGAL IDENTIFICATION NO.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with IICA's Data Protection Policy regarding exercising the right of access, we hereby inform you that, as at the date of the abovementioned request to exercise the right of access, IICA is not processing personal data of which you are the owner.

Furthermore, we inform you that, at any time, data subjects may exercise the right to rectification, right to erasure, right to restrict processing, right to portability and the right to object to the processing of personal data, in accordance with current regulations, as well as to withdraw consent initially granted.

Please note that this letter is being sent in response to your request.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,

IICA

### Sample 3: Positive response to a request to exercise the right to rectification



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to rectify data held by the Data Controller: INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [LEGAL IDENTIFICATION NO.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with the provisions of IICA's Data Protection Policy regarding exercising the right to rectification, we hereby inform you that we have proceeded to rectify and update the data you have requested.

Furthermore, we inform you that, at any time, data subjects may exercise the right of access, right to erasure, right to restrict processing, right to portability and the right to object to the processing of personal data, in accordance with current regulations, as well as to withdraw consent initially granted.

Please note that this letter is being sent in response to your request.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,

IICA

**Sample 4: Positive response to a request to exercise the right to erasure  
(through data blocking)**



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to erasure of data held by the INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [LEGAL IDENTIFICATION NO.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with the provisions of IICA's Personal Data Protection Policy regarding exercising the right to erasure, it is important to clarify that total erasure of this data at this date could be detrimental to the legitimate interests of IICA or third parties. Therefore, the data has been blocked and will be retained only for the purpose of dealing with any liabilities arising from the processing, during the limitation period. Once this period has expired, the data will be definitively deleted.

Therefore, from the moment in which the data is blocked, IICA will not process your data in any way, except to meet legal requirements.

Furthermore, we inform you that, at any time, data subjects may exercise the right of access, right to rectification, right to restrict processing, right to portability and the right to object to the processing of personal data, in accordance with current regulations, as well as to withdraw consent initially granted.

Please note that this letter is being sent in response to your request.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,

IICA

## Sample 5: Positive response to a request to exercise the right to erasure

(through the deletion of data)



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to erasure of data held by the INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [LEGAL IDENTIFICATION NO.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with the provisions of IICA's Personal Data Protection Policy regarding exercising the right to erasure, we hereby inform you that we have proceeded to erase the data you have requested.

Therefore, in accordance with legislation currently in force, as of the moment of erasure, IICA does not possess any personal data of which you are the owner.

Furthermore, we inform you that, at any time, data subjects may exercise the right of access, right to rectification, right to restrict processing, right to portability and the right to object to the processing of personal data, in accordance with current regulations, as well as to withdraw consent initially granted.

Please note that this letter is being sent in response to your request.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,

IICA

## Sample 6: Positive response to a request to exercise the right to restrict processing



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to restrict the processing of data held by the INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [LEGAL IDENTIFICATION NO.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with the provisions of IICA's Personal Data Protection Policy regarding exercising the right to restrict processing, we hereby inform you that we have proceeded to restrict processing, based on the terms presented in your request.

Please note that this letter is being sent in response to your request.

Furthermore, we inform you that, at any time, data subjects may exercise the right of access, right to rectification, right to portability, right to erasure and the right to object to the processing of personal data, in accordance with current regulations, as well as to withdraw consent initially granted.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,

IICA

## Sample 7: Positive response to a request to exercise the right to portability



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to portability of data held by the INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [LEGAL IDENTIFICATION NO.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with the provisions of IICA's Personal Data Protection Policy regarding exercising the right to data portability, we hereby inform you that we have proceeded to grant you the right to portability, based on the terms presented in your request.

Please note that this letter is being sent in response to your request.

Furthermore, we inform you that, at any time, data subjects may exercise the right of access, right to rectification, right to restrict processing, right to erasure and the right to object to the processing of personal data, in accordance with current regulations, as well as to withdraw consent initially granted.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,

IICA

## Sample 8: Positive response to a request to exercise the right to object



[...], on [...] of [...] of 2021

Dear Sir/Madam,

We hereby inform you that, in accordance with IICA's Data Protection Policy, you have exercised your right to object to the processing of data held by the INTER-AMERICAN INSTITUTE FOR COOPERATION ON AGRICULTURE (hereinafter, "IICA"), [LEGAL IDENTIFICATION NO.] and [Registered office] (address of the IICA Delegation in the corresponding country or at Headquarters).

In accordance with the provisions of IICA's Personal Data Protection Policy regarding exercising the right to object to data processing, we hereby inform you that we have proceeded to grant you the right to object, based on the terms presented in your request.

Please note that this letter is being sent in response to your request.


Furthermore, we inform you that, at any time, data subjects may exercise the right of access, right to rectification, right to restriction of processing, right to erasure and the right to portability of your personal data, in accordance with current regulations, as well as to withdraw consent initially granted.

To request any clarification or to make a suggestion, you may contact us at our email address xxxxxxxx@iica.int (specific address for the corresponding Delegation).

Kind regards,  
IICA



## Annex 5 – Verification of personal data processor

	<b>DOCUMENT TYPE</b>		Public (available on the IICA website)
			<input checked="" type="checkbox"/> Private (available on IICA's intranet)
<b>TITLE</b>	Verification of personal data processor		
<b>APPLICATION</b>	All IICA Delegations and Units at Headquarters with access to and that process third-party personal data		
<b>FORMAT</b>	Electronic - Word		
<b>PAGES</b>	4		
<b>APPROVAL REF.</b>	SC/DG-404, SEPTEMBER 24, 2021		
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

The present procedure is established to comply with the provisions of the IICA Personal Data Protection Policy, with regards to ensuring the hiring of data processors who offer sufficient guarantees of compliance with the obligations in data protection regulations, particularly regarding the application of appropriate technical and organizational guarantees to ensure the rights of data subjects.

### 2. Objective

To define the procedure to be followed to verify that third-party personal data processors fulfil the obligations established in the IICA Personal Data Protection Policy and the present Manual, and that they have at their disposal sufficient technical, organizational and security measures in relation to the personal data processing tasks assigned to them by IICA.

### 3. Procedure

This procedure defines the steps to be followed to ensure that processors—i.e., those that have been assigned any type of personal data processing task on behalf of IICA or those that provide services to IICA—have at their disposal sufficient technical, organizational and security measures to guarantee the rights of data subjects. Processors may be goods or services suppliers who have access to personal data under the responsibility of IICA, be it the personal data of individuals or the contact information of legal entities.

Staff members of the Institute whose roles include managing the new procurement of goods or services, or managing new grants, must ensure compliance with the present compliance verification procedure for IICA data processors.

### 3.1 Compliance checklist prior to hiring a processor.

At the beginning of every contractual relationship and **prior to** signing the **Contract for Personal Data Access by Third Party** with the supplier or partner in question, which is described in **Annex 6** below, the compliance checklist must be completed by processors of data under the responsibility of IICA, as follows:

#### Compliance checklist for processors of data under IICA's responsibility.

<b>DATA PROCESSOR:</b> <a href="#">Click here to write text.</a>		
<b>REVIEW DATE FOR THIS PROCEDURE:</b> <a href="#">Click here to write a date</a>		
<b>PART I – EXISTENCE OF CONTRACT SIGNED IN ACCORDANCE WITH IICA PERSONAL DATA PROTECTION POLICY</b>		
Area to verify	Applicable	Detail
1. Is there an agreement or other legal instrument between the processor and Controller?	<input type="checkbox"/>	Parties: <a href="#">Click here to write text</a> and <a href="#">Click here to write text</a>
2. The contract establishes:		
2.1 The <b>object</b> of the processing	<input type="checkbox"/>	Cf Clause: <a href="#">Click here to write text.</a>
2.2 The <b>duration</b> of the processing	<input type="checkbox"/>	Cf Clause: <a href="#">Click here to write text.</a>
2.3 The <b>type of personal data</b>	<input type="checkbox"/>	Cf Clause: <a href="#">Click here to write text.</a>
2.4 The <b>categories of stakeholders</b>	<input type="checkbox"/>	Cf Clause: <a href="#">Click here to write text.</a>
<b>PART II – COMPLIANCE CHECKLIST OF OBLIGATIONS ESTABLISHED IN THE CONTRACT</b>		
1. Have the instructions provided to the processor regarding the processing of the data been duly documented?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>
2. Has the processor provided a copy of the confidentiality documents signed by the individuals in its/his/her organization who are processing the assigned data?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>
3. Has the processor confirmed that it/he/she has adopted adequate security measures for processing the assigned data? In particular, has the processor provided	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>

security certifications in accordance with international information security management standards regarding the systems to be used in the assigned processing activity?		
4. In instances involving a sub-processor, has the processor identified all the sub-processors tasked with processing data for the assigned activity?		
5. In instances involving a sub-processor, has the processor provided a copy of the contracts signed by all the sub-processors involved in processing the data for the assigned activity?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>
6. In instances in which the processor collects data for IICA, has the processor provided a copy of the information and consent documents signed by all the data subjects, in accordance with the information and consent templates provided by IICA?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>
7. Has the processor received requests for the exercise of rights of access, rectification, erasure, objection, portability and restriction of data related to the processing assignment? If so, has the processor notified IICA of them in due time and form?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>
8. At any time, have incidents or security violations occurred in the processor's processing systems in relation to the data processing functions? If so, has the processor notified IICA of them in due time and form and has it/he/she collaborated at all times to take action and resolve the incident?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>
9. If the assigned processing activity must be subject to risk analysis, has the Data processor collaborated appropriately in producing said analysis?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>
10. Has the Data processor at any time been asked to provide other evidence of compliance with their contractual obligations? If so, has the processor responded satisfactorily to said request?	<input type="checkbox"/>	Describe the evidence of compliance: <a href="#">Click here to write text.</a>


### 3.2 Compliance checklist upon completion of a Data Processor agreement

Once the contractual relationship between IICA and the Data processor has ended, the compliance checklist of data processor obligations will need to be completed.

#### Compliance checklist of Data processor obligations to be completed upon termination of the contractual relationship with IICA

<b>DATA PROCESSOR:</b> <a href="#">Click here to write text</a>		
<b>RELATIONSHIP END DATE:</b> <a href="#">Click here to write text</a>		
<b>PROCESS REVIEW DATE:</b> <a href="#">Click here to write text</a>		
Item	Done	Details
1. Has the Data processor destroyed or returned all personal data subject to processing?	<input type="checkbox"/>	Describe the chosen procedure: <a href="#">Click here to write text</a>
2. Is there documentary evidence of the Data processor's adherence to the chosen destruction or return procedure?	<input type="checkbox"/>	Describe the evidence provided by the Data processor: <a href="#">Click here to write text</a>
3. If the Data processor needs to store the data to demonstrate compliance with legal or contractual obligations, has it/he/she provided evidence of security measures to protect the personal data?	<input type="checkbox"/>	Describe the evidence provided by the Data processor: <a href="#">Click here to write text</a>
4. If the Data processor needs to store the data to demonstrate compliance with legal or contractual obligations, has it/he/she confirmed the maximum period for which the data will be stored?	<input type="checkbox"/>	Indicate the term established by the Data processor: <a href="#">Click here to write text</a>

## Annex 6 – Appointment of third parties with access to third-party personal data “Data processor”

	<b>DOCUMENT TYPE</b>		<input type="checkbox"/> Public (available on the IICA website)
			<input checked="" type="checkbox"/> Private (available on IICA's intranet)
<b>TITLE</b>	Appointment of third parties with access to third-party personal data - “Data processor”		
<b>APPLICATION</b>	All IICA Delegations and Units at Headquarters with access to and that process third-party personal data		
<b>FORMAT</b>	Electronic – Word		
<b>PAGES</b>	10		
<b>APPROVAL REF.</b>	SC/DG-404, SEPTEMBER 24, 2021		
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

In certain situations, the Institute will need to contract with third parties to process personal data under IICA’s responsibility to provide services.

“Data processing” means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as the collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparing or combining, restricting, erasing or destructing such personal data.

### 2. Objective

To develop the guidelines that IICA is to follow when contracting with third parties who, by means of a services agreement, will have access to personal data owned by or under the responsibility of IICA.

### 3. Procedure

As stated in **Annex 5** above, **Data processor** means a goods or services provider who is to process personal data on behalf of the Data controller, in this case IICA.

Therefore, IICA herein is the **Data controller** who shall determine the purposes and means of processing the personal data to which it has access to carry out its activities.

The Institute shall ensure that any third parties with which it contracts and that will have access to the personal data under IICA's responsibility are regulated by means of an agreement that establishes the rights and obligations of both parties regarding the processing of data.

### **3.1 Data processor guarantees**

IICA shall only contract with data processors that offer sufficient and appropriate guarantees to apply technical and organizational measures so that the data processing will comply with the guidelines set forth in the Institute's Personal Data Protection Policy and this Manual, in order to ensure the protection of the rights of the data subjects. Such guarantees shall translate, *inter alia*, into expertise, reliability, resources, and security.

To that end, the adherence by the Data processor to an approved code of conduct or certification mechanism may be used as an element to demonstrate the existence of sufficient guarantees for the fulfillment of its/his/her data protection obligations. However, such adherence shall not exempt it/him/her from signing an agreement with IICA.

### **3.2 Personal data access agreement**

The processing of or access to personal data by a Data processor will be governed by a binding agreement between the Data processor and IICA.

Prior to outsourcing the design and development of IT systems, applications, programs and services, the existence of personal data processing, as described in **Annex 6** above, shall be analyzed. In such cases, in addition to the usual legal instrument that is executed to contract the services or products required by IICA or its projects, a **Contract for Personal Data Access by Third Party** shall be executed as detailed below.

### **3.3 Data processor security measures**

The Data processor (third-party) agreement shall transfer the obligation to take all necessary technical and organizational measures to ensure, specifically, a level of security appropriate to the risk.

The following security measures are to be taken by the third party with regards to personal data processing:

- a. Identify and document the duties and obligations of the personnel with access to the data;
- b. Define and implement a user identification and authorization procedure;
- c. Define and implement a data access control procedure;
- d. Define and implement an incident logging procedure;

- e. Define and implement a backup procedure;
- f. Implement an inventory and check-in/check-out procedure for all support material and documents;
- g. Define archive criteria and storage devices;
- h. Define and implement periodic security checks to regularly test, assess, and evaluate the effectiveness of technical and organizational measures to ensure processing security;
- i. Define and implement physical access controls;
- j. Define and implement a service continuity plan, when required by the service type;
- k. Define and implement a pseudonymization procedure for personal data where technically feasible; and
- l. Define responsibilities given fault or willful misconduct.

### **3.4 Notification of Data processor-related security violations**

The Data Processor agreement shall stipulate that, in the event of a breach of the Data processor's systems that could affect the data under IICA's responsibility, the Data processor shall notify IICA within 24 hours of becoming aware of any such breach.

The Data processor shall provide IICA with at least the following information:

- a. A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the approximate number of personal data records concerned;
- b. A description of the likely consequences of the personal data breach; and
- c. A description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

### **3.5 Data return or deletion by the Data processor**

The Data processor agreement shall incorporate a clause that stipulates that, upon completion of the contracted services or at the request of IICA and within a maximum period of 90 days<sup>1</sup>, the Data processor shall delete or return such information containing personal data transmitted to it by IICA for the provision of services, as well as all support material, media or documents containing personal data, without retaining any copy thereof or of the information provided or generated.

---

<sup>1</sup> *Except in specific justified cases when such period may vary based on the type of services for which the third party was contracted by IICA.*

Likewise, IICA may require that the Data processor provide a certificate attesting to the confidential delivery and/or destruction of such data, as well as the absence of copies thereof, within the period specified by IICA.

### **3.6 Outsourcing to a Sub-processor**

The Data processor agreement shall further stipulate that the Data processor is prohibited from outsourcing any data processing-related services to third parties without the prior written authorization of IICA.

In the case of written authorization, the Data processor shall inform IICA of any intended changes concerning the addition or replacement of Data processors, thereby giving IICA the opportunity to object to such changes.

When a Data processor outsources to a Sub-processor to carry out certain processing activities on behalf of IICA, its/he/she shall impose, by means of a written agreement, the same data protection obligations as set forth in the agreement between IICA and the Data processor, particularly with regard to the provision of sufficient guarantees for the application of technical and organizational measures and the definition of legal responsibilities given fault or willful misconduct.

It shall be established that, should the Sub-processor fail to meet its/his/her data protection obligations, the initial Data processor shall be fully liable to IICA for the fulfillment of said obligations.

### **3.7 Record of Data processors and evidence of compliance**

To ensure the compilation of all the necessary proof of registration and compliance, the Administrators of the different IICA Delegations in the Member States and the responsible individuals at the different Units at Headquarters, who contract with third parties to provide goods or services to IICA that will enable them to access or process personal data under IICA's responsibility, shall create and maintain a record for the purpose of identifying the status of third parties as Data processors. This record shall contain the following information on each of the Data processors, including documentary evidence:

- a. Identity of the provider;
- b. Contract for Personal Data Access by Third Party signed by the Data processor;
- c. Start and end date of the agreement signed with the provider;
- d. Authorized sub-processors based on such agreement (if the agreement is assigned as per paragraph f above);
- e. Compliance checklist (see **Annex 6**);



- f. Compliance checklist upon termination of the relationship with the Data processor (see **Annex 6**); and
- g. Documentary evidence of compliance with each of the points of control established in **Annex 6** above.

IICA, through its internal structure and mechanisms, shall verify that the aforementioned record is properly updated and that it contains sufficient evidentiary elements. Should there be deficiencies in the documentary evidence established herein, the individual responsible for the relationship with the Data processor in question shall be required to immediately take the necessary corrective measures.

### Sample Contract for Personal Data Access by Third Party



By and between **the Inter-American Institute for Cooperation on Agriculture (IICA)**, hereinafter **the Institute**, represented herein by Mr. **[Name of IICA Officer]**, in his capacity as **[Director of [Office name] / IICA Representative to [Country]**, with ID number **[number]**, residing at **[address]**, and the following individual/legal entity: **[Name]**, ID number **[number]**, represented herein by Mr. **[Name]**, ID number **[number]**, in his capacity as **[capacity]**, with general power of attorney, hereinafter referred to as **[Name]**; who do hereby agree to enter into this Contract for Personal Data Access by Third Party, in accordance with the following Statements and Clauses:

#### STATEMENTS

**The Institute and [third party] declare:**

- That this **Contract for Personal Data Access by Third Party** shall be governed by the **[name of agreement between the parties that establishes the contract for the design and development of IT systems, applications, programs and services]**, executed by the parties on **[date]**, for **[purpose]**.
- That the **Inter-American Institute for Cooperation on Agriculture (IICA)** has a Personal Data Protection Policy and Personal Data Protection Procedures Manual.
- That hereinafter, IICA shall be referred to as the **Data controller** who shall determine the purposes and means of processing the personal data to which it has access to carry out its activities.
- That hereinafter, **[third party]** shall be referred to as the **Data processor**, i.e., the goods or services provider that is to process the personal data on behalf of the Data controller, in this case IICA.



## CLAUSES

### ONE:

1. Purpose. To agree on the rights and obligations of the Parties as regards the processing of data for the performance of the **[name of the agreement between the parties that establishes the contract for the design and development of IT systems, applications, programs and services] Agreement**, which is an integral part hereof.
2. Duration. **[Pursuant to the [name of the agreement between the parties that establishes the contract for the design and development of IT systems, applications, programs and services] Agreement, plus any time required for the return or deletion of third-party data].**
3. Nature and purpose of the processing.
4. Type of personal data to be processed by the Data processor. **[Description based on the type of service for which the Data processor is contracted.**
5. Data subject categories.
6. Obligations and rights of IICA and the Data processor.

#### 6.1 Data processor:

- a. To process the personal data in accordance with the written instructions of IICA.
- b. To guarantee that any individuals authorized to process personal data have undertaken to respect confidentiality or are subject to a statutory confidentiality agreement.
- c. To take all necessary technical and organizational measures in accordance with IICA's Data Protection Policy, to ensure, specifically, a level of security appropriate to the risk, as well as to defend the rights of data subjects, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, which may include:
  - i. The pseudonymization and encryption of personal data;
  - ii. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of the data processing systems and services;
  - iii. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
  - iv. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- d. To respect the conditions set forth in this Contract when outsourcing to a Sub-processor.

- e. To assist IICA in fulfilling its obligation to respond to requests to exercise the rights of the data subjects, taking into account the nature of the process and using the appropriate technical and organizational measures whenever possible.
- f. To keep under its control and custody all personal data to which it/he/she has access for the purpose of providing the service and to not disclose, transfer or otherwise disclose it to other individuals outside the service, even for the purpose of safekeeping.
- g. To assist IICA in ensuring compliance with its obligations regarding personal data security, taking into account the nature of the process and the information available to the Data processor.
- h. **Guarantees provided by the Data processor:** The **Data processor** has sufficient and appropriate guarantees to implement technical and organizational measures, such that the processing of data conforms to IICA's Personal Data Protection Policy, which is available on IICA's website, and to guarantee protection of the rights of the data subjects. Such guarantees comprise, at a minimum, expertise, reliability, resources, and security. Should the **Data processor** adhere to an approved code of conduct or certification mechanism, the Data Processor undertakes to inform **IICA** thereof.
- i. **Data processor security measures:** The **Data processor** shall adopt all necessary technical and organizational measures to ensure, specifically, a level of security appropriate to the risk. As such, it/he/she undertakes to:
  - i. Identify and document the functions and duties of personnel with access to the data;
  - ii. Define and implement a user identification and authorization procedure;
  - iii. Define and implement a data access control procedure;
  - iv. Define and implement an incident logging procedure;
  - v. Define and implement a backup copy procedure;
  - vi. Implement an inventory and media and document input and output control procedure;
  - vii. Define archive criteria and storage devices;
  - viii. Define and implement periodic safety controls to regularly test, assess, and evaluate the effectiveness of technical and organizational measures to ensure processing safety;
  - ix. Define and implement physical access controls;
  - x. Define and implement a service continuity plan, when required by the service type; and
  - xi. Define and implement a personal data pseudonymization procedure where technically feasible.
- j. **Collaboration in notifying security violations:** The **Data processor** undertakes to notify IICA within 24 hours after becoming aware of a personal data breach. The Data processor shall provide IICA with at least the following information:
  - i. A description of the nature of the violation including, if possible, the categories and approximate number of affected data subjects, as well as the approximate number of personal data records in question;

- ii. A description of the likely consequences of the data breach; and
  - iii. A description of the measures taken or proposed to remedy the data breach, including, where appropriate, measures taken to mitigate the possible negative effects.
- k. To delete or return all personal data upon completion of the services subject to the **[name of agreement between the parties that establishes the contract for the design and development of IT systems, applications, programs and services] Agreement** or when required by IICA, within a maximum period of **[90 days (except in specific cases when this period may vary based on the type of services for which the third party was contracted by IICA)]**; the Data processor shall delete or return all such information containing personal data transmitted by IICA for the provision of services, as well as all media or documents containing personal data without retaining any copy of the information provided or generated.

Likewise, the Data processor shall, in the event the information is destroyed, conduct the process formally, securely, and confidentially, taking all necessary technical and organizational measures to ensure that the data is not recoverable and, as such, not usable at a later date nor accessible by unauthorized third parties.

IICA may require that the Data processor provide a certificate supporting the confidential delivery and/or destruction of such information, as well as the absence of copies thereof within the time frame specified by IICA.

In any event, the Data processor shall be responsible for executing and demonstrating the aforesaid procedure at the request of IICA, in which case the Data processor shall be liable for any non-compliance resulting from the failure to adopt the necessary measures or to execute the process as set forth herein.

Should the **Data processor** have the legal obligation to retain certain data for a period of time, such data shall remain blocked and unusable for any other purpose, being retained solely for the purposes established or by reason of any possible liabilities that may arise from the processing thereof and for such time as may apply thereto, after which it shall be deleted.

- l. **Rights of access, rectification, erasure, restriction, objection, and data portability:** The **Data processor** shall assist IICA in responding to requests to exercise the rights of access, rectification, erasure, objection, restriction of processing, data portability, and the right to not be subject to a decision based solely on automated processing (including profiling).

Should a data subject exercise his/her rights directly with the Data processor and/or authorized Sub-processor, the request shall be forwarded to IICA immediately or within no more than one working day following the date of receipt thereof, together with other information that may be relevant to resolve the request, as applicable, so that IICA may be able to resolve the request in accordance with its internal mechanisms.

The Data processor shall take all necessary measures to ensure such requests are forwarded to IICA in the time frame specified, along with any information required by IICA to effectively respond to the rights exercised.

- m. **Outsourcing:** The **Data processor** shall not outsource any data processing-related services for which it/he/she was contracted without the prior written authorization of IICA. In the case of written authorization, the Data processor shall inform IICA of any intended changes concerning the addition or replacement of Data processors, thereby giving IICA the opportunity to object to such changes.

When a Data processor outsources to a Sub-processor to carry out certain data processing activities on behalf of IICA, it/he/she shall impose, by means of a written agreement, the same data protection obligations as those set forth herein, particularly as regards the provision of sufficient guarantees for the application of technical and organizational measures.

Should the Sub-processor fail to meet its/his/her data protection obligations, **[third party]** shall continue to be fully liable to IICA for the fulfillment of such obligations of the Sub-processor.

- n. **Other obligations:** The **Data processor** shall:

- i. Keep a written log of all processing categories carried out on behalf of IICA. The activity log shall contain:
  - a) The processing categories conducted on behalf of IICA; and
  - b) An overview of the technical and organizational security measures implemented to ensure personal data protection.
- ii. Support IICA in assessing the impact on data protection, where appropriate.
- iii. Make available to IICA the information necessary to demonstrate compliance with the obligations set forth herein and allow and contribute to the conduct of audits, evaluations or reviews by IICA or by an authorized third party. Such requests shall be made with the appropriate advance notice and shall cause the least possible inconvenience for the Data processor.

7. Contract rescission: IICA reserves the right to terminate this agreement in advance in the event of non-compliance or defects in compliance by the **Data processor** with its/his/her obligations arising from the processing of personal data, in which case IICA shall be released from all liability.
8. Dispute resolution: Any dispute between the Parties concerning the interpretation, application or performance hereof shall be resolved by mutual agreement between the Parties within thirty working days.

Should the dispute continue, the Parties shall submit unconditionally and irrevocably to the procedure and ruling of an Arbitration Committee composed of the following: two arbitrators appointed and financed by each of the Parties individually and a third party appointed and financed by the Parties by mutual agreement. It is understood that the Arbitration Committee shall decide all procedural matters in cases where the Parties disagree. The decision of the Arbitration Committee shall be final, not subject to appeal, and legally binding on the Parties.

9. Privileges and immunities: Nothing in or related to this Agreement shall be considered an express or implied waiver of the immunities and privileges, exemptions and facilities enjoyed by IICA and its staff in accordance with international law, international treaties or conventions or the national legislation of its Member States.

In witness whereof, we sign two original copies on the \_\_\_\_\_ day of the month of \_\_\_\_\_ of the year 20\_\_.


\_\_\_\_\_  
For the Institute

\_\_\_\_\_  
Individual or Representative of  
legal entity

**[Director [ ] or Representative]**  
IICA Representative to [Country]  
[ID number]

[Name]  
[ID number]

## Annex 7 – Notification of a personal data breach

	<b>DOCUMENT TYPE</b>		<input type="checkbox"/> Public (available on the IICA website)
			<input checked="" type="checkbox"/> Private (available on IICA's intranet)
<b>TITLE</b>	Notification of a personal data breach		
<b>APPLICATION</b>	All IICA Delegations and Units at Headquarters with access to and that process third-party personal data		
<b>FORMAT</b>	Electronic - Word		
<b>PAGES</b>	7		
<b>APPROVAL REF.</b>	SC/DG-404, SEPTEMBER 24, 2021		
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

The Institute undertakes to notify all data breaches as well as to prevent the alteration, loss or destruction of personal data and to facilitate the detection of security violations.

### 2. Objective

To develop the course of action to take should an incident occur, whether automated or otherwise; to determine the protocol to follow after resolution to prevent reoccurrence; and to define what constitutes a breach and the course of action to be taken by IICA and by each of the different entities involved in the processing of personal data.

### 3. Procedure

The Institute shall report all personal data breaches (also known as security violations).

Should the data breach be likely to pose a high risk to the rights or freedoms of data subjects, the Institute shall also have the obligation to communicate such breach to those affected.

To prevent the alteration, loss or destruction of personal data, as well as to facilitate the detection and notification of security violations, the following incident notification, management and recording procedure has been developed under which any event considered to be an incident is to be duly recorded in a log created for that purpose.



### 3.1 Definition, examples, and adverse effects of security incidents and breaches

- a. **Incident** is understood to be any anomaly that affects or may affect data security, including its confidentiality, integrity or availability. By way of example, an incident is considered to be any of the following:
- i. Collection of personal data without the authorization of the affected individual and without having informed him/her of his/her rights;
  - ii. Use of personal data for any purpose other than that for which it was collected;
  - iii. Circumvention of access control systems;
  - iv. Accidental erasure of personal data;
  - v. Failure by the Data processor to comply with instructions to recover the data;
  - vi. Failure to comply with the deadlines established for resolving and responding to requests by data subjects to exercise their rights;
  - vii. Unlawful use of personal data;
  - viii. Failure of the backup management system;
  - ix. System failures or viruses;
  - x. Theft of equipment and/or data files; and
  - xi. Exposed passwords, whether accidental or fraudulent.
- b. A personal data **breach** is any breach of security leading to:
- i. The accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed; or
  - ii. The unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

Specifically, a security breach includes, but is not limited to, the following:

- i. Insecure destruction of a significant amount of personal data contained in physical format (such as not using a shredder or specific containers for that purpose);
- ii. Unauthorized access to IICA databases (including by its own staff);
- iii. Theft of IICA computers;
- iv. Web service vulnerability affecting all of IICA's clients, including first name, last name, account number, etc.;
- v. Phishing malware (email attacks): the sender assumes the identity of a known company and invites the user to download a file, thereby installing malware on the computer and encrypting all data. Generally, a financial sum is demanded to restore the data (usually in virtual currency);

- vi. Insecure communications and data theft: stealing of information such as banking credentials or confidential information; and
  - vii. Outdated software that may become a breeding ground for malware.
- c. The **adverse effects** of security incidents or violations include, but are not limited to:
- i. Changes in the continuity of data processing;
  - ii. Loss of data that may affect the integrity of the documents under IICA's responsibility;
  - iii. Identity theft;
  - iv. Misuse of payment data; and
  - v. Financial and moral repercussions for the data subjects.
- d. However, the following incidents shall not be considered **data breaches**:
- i. Incidents that do not affect personal data, i.e., data not relating to an identified or identifiable individual;
  - ii. Incidents that do not affect the processing of personal data undertaken by the Data controller or Data processor; and
  - iii. Incidents that occur in processing activities carried out by an individual in a personal and domestic setting.

### **3.2 Incident detection and notification**

Failure to take prompt and appropriate measures in response to a personal data breach could lead to physical, material or non-material damage to individuals, such as the loss of control of their personal data or the restriction of their rights, discrimination, identity theft, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage.

Any person who renders services to IICA and detects an anomaly in the system, data files or IT equipment and/or in the personal data processed shall bring it to the immediate attention of the System Administrator and Personal Data Protection Management Team with the aim to prevent the possible incident from negatively impacting the security with which the personal data is processed or stored.

Communication shall be made through the fastest and most reliable means possible in order to maintain the security, confidentiality, and normality within IICA's organizational and technical scope (through the notification channel available for this purpose).

Any person who notifies an incident shall provide the information necessary for IICA to proceed with its recording and control and, if possible, implement a response plan to interrupt and eliminate the incident.

Prior to recording the incident in the corresponding log, the System Administrator shall notify the internal or external technicians responsible for security management and system, equipment and file maintenance.

The System Administrator and Personal Data Protection Management Team shall ensure that the technicians respond to the detected incidents as soon as possible and shall personally monitor their activity and the remediation of the anomaly.

Should IICA's Personal Data Protection Management Team consider and be able to demonstrate, in accordance with the principle of proactive responsibility, the unlikelihood that a security breach would constitute a risk to the rights and freedoms of natural persons, it shall only record the relevant information. For example, when a data intrusion and breach cannot adversely affect personal data or an individual's privacy; or when the extracted data is properly encrypted and incomprehensible and, consequently, the data intrusion and breach cannot adversely affect personal data or an individual's privacy.

IICA's risk assessment shall consist of the consideration of the extent to which the incident, given its characteristics, the type of data affected or the type of consequences it may have for the affected data subjects, could damage their rights or freedoms.

It shall be considered that a security violation has occurred when there is certainty that one has taken place and IICA has sufficient knowledge of its nature and scope. The mere suspicion of a breach shall not be considered a security violation.

However, should IICA detect that due to its characteristics, a possible security violation could have a significant impact, it shall provide notification of such breach within 72 hours of becoming aware of it, even when there is only evidence of a possible irregular situation with regard to data security.

Where IICA acts as Data controller and contracts with a service provider who shall have access to the data, it must include in the agreement signed with the service provider (Data processor on behalf of IICA) the obligation to alert and inform IICA immediately upon detecting a personal data breach and to assist IICA in ensuring compliance with its data security obligations. Should such alert not be made immediately, the Data processor shall be liable to IICA and the appropriate sanctions shall be applied.

The table below shows the main factors considered by IICA in determining the scope, risk, and notification of a security breach:

Type of data breach
Nature, sensitivity, and volume of personal data affected
Ease of identification
Severity of the consequences for the rights and freedoms of individuals
Particular characteristics of the Data processor
Number of data subjects affected
General considerations

**3.3 Data processors and Sub-processors**

Should the breach occur by fault of a Data processor, it/he/she shall alert and inform IICA immediately upon confirmation of the personal data breach. To that end, the contract signed between IICA and the Data processor shall include the obligation to assist IICA in ensuring compliance with its data security obligations. Likewise, should a Data processor acquire the services of a Sub-processor, a written agreement shall exist that sets forth such obligations as determined by the Data controller and that releases IICA from all liability with regards to the Sub-processor and for its/his/her actions.

The Data processor shall notify the Data controller without undue delay of any personal data breaches of which it/he/she becomes aware. Such notification shall include at least:

- a. A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the approximate number of personal data records concerned;
- b. The name and contact details of the data protection officer or other contact point where more information can be obtained;
- c. A description of the likely consequences of the personal data breach; and
- d. A description of the measures taken or proposed to be taken by the Data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where and in so far as it is not possible to provide the information at the same time, the information may be provided in phases without undue delay.

Where the Data processor has outsourced to a Sub-processor, the former shall impose on the latter, by means of an agreement or other legal instrument, the same data protection obligations as set out in the agreement or other legal instrument between the Data processor and Data controller, especially the provision of sufficient guarantees to implement appropriate technical and organizational measures. Therefore, should the security breach occur by fault of the Sub-processor, it/he/she shall be obliged, under the same terms as those set out for the Data processor, to notify without undue delay any personal data breach of which it/he/she becomes aware.

### **3.4 Incident log**

The Data controller shall record and document all personal data breaches, including the facts related thereto, its consequences, and any corrective action taken, in the incident log detailed herein or by electronic means containing the same fields as the aforementioned log.

All information relating to the incident shall be recorded in the incident log. This log shall be completed in full and each piece of required information shall be recorded accurately.

The incident log shall include at least the following fields:

- a. Incident type;
- b. Incident status (open/closed);
- c. Time it occurred;
- d. Person who made notification;
- e. Person to whom notification was made;
- f. Its consequences, if any;
- g. Person who conducted the data recovery process;
- h. Data restored; and
- i. Data recorded manually during the recovery process.

It is the sole responsibility of the System Administrator to maintain and comply with the measures adopted to resolve any possible incidents. To that end, the System Administrator shall be responsible for maintaining the incident log with all of the fields reflected in the model incident management and notification log.

Upon resolution of the incident, the System Administrator shall take the necessary steps to prevent any similar situations from occurring in which the integrity of the systems and data could be compromised.

### **3.5 Communication of a data breach to the data subject**

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, and where IICA acts as Data controller, it shall communicate the personal data breach to the data subject without undue delay. In other words, IICA shall notify the affected individuals of a security breach when such breach could have a negative impact on their personal data or privacy.

A security breach shall be considered high risk when it is likely to cause damage to the data subject. For example, where confidential information, such as passwords or participation in certain activities, is disclosed; where sensitive data is widely disseminated; or where the affected persons could suffer financial damage.

The purpose of IICA's obligation to communicate the occurrence of a personal data breach to the data subject is to allow the data subject time to react and to take action as soon as possible.

IICA's communication to the data subject shall describe in clear and plain language the nature of the personal data breach and provide recommendations for the affected individual to mitigate any potential adverse effects. In particular, such communication shall contain at least the following:

- a. Name and contact details of the Personal Data Protection Management Team or other contact point where more information can be obtained;
- b. The likely consequences of the personal data breach; and
- c. A description of the measures taken or to be taken by IICA to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

However, IICA shall not be required to communicate with the data subject if any of the following conditions are met:


- a. IICA has implemented appropriate technical and organizational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; or
- b. IICA has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize.

For example, IICA shall not be required to notify the data subjects when:

- a. A personal data breach affects confidentiality only and the data was encrypted securely using advanced technologies and the decryption key was not tampered with and was created such that no unauthorized persons could discover it using technological means;

- b. The data and passwords are hashed (using a mathematical algorithm that transforms incoming data into a series of outgoing characters) and salted and the hash value was calculated using an advanced cryptographic key hash function and the key used to hash the data was not tampered with and was created such that no unauthorized persons could discover it using technological means.

## Annex 8 – Retention and deletion of personal data

	<b>DOCUMENT TYPE</b>		Public (available on the IICA website)
			<input checked="" type="checkbox"/> Private (available on IICA's intranet)
<b>TITLE</b>	Retention and deletion of personal data		
<b>APPLICATION</b>	All IICA Delegations and Units at Headquarters with access to and that process third-party personal data		
<b>FORMAT</b>	Electronic - Word		
<b>PAGES</b>	3		
<b>APPROVAL REF.</b>	SC/DG-404, SEPTEMBER 24, 2021		
<b>VERSION</b>	<b>DATA</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

Personal data must be appropriate, relevant, and limited to what is necessary for the purposes for which it is processed. Specifically, this requires guaranteeing that the period of retention is limited to a strict minimum.

IICA shall proceed to delete or block the data in cases in which one or more of the circumstances established for a data subject to exercise his/her right of erasure occur.

### 2. Objective

To retain data in a form that permits identification of the individual for no longer than is necessary for the purposes for which it was processed.

### 3. Procedure

In accordance with the Personal Data Protection Policy, IICA shall ensure that personal data is **appropriate, relevant, and limited** to what is necessary for the purposes for which it is processed.

In its capacity as Data controller, IICA has established a retention limit, as specified in Section **3.6 – Retention period**. The Institute shall take all reasonable measures to guarantee that any inaccurate personal data is rectified or deleted.

The blocking and permanent deletion of personal data shall be recorded in a control or log.

In compliance with the regulating principles on the processing of personal data defined in the Personal Data Protection Policy, the following is established:



### **3.1 Limitation of the retention period**

Data shall be retained in a form that permits identification of the individual for no longer than is necessary for the purposes for which it was processed, as indicated in section **3.6 – Retention period** below.

### **3.2 Data quality (suitability)**

Data shall only be maintained while it continues to be necessary for the purpose for which it was collected. Once it has ceased to be necessary, it must be deleted and remain blocked, and only during the limitation period of said responsibilities. When this period has ended, the data must be deleted.

### **3.3 Blocking third-party personal data**

Blocking implies the retention of data, permitting access solely to certain persons authorized by the Data Protection Management Team or those involved in the protection of personal data as part of their functions.

IICA must keep personal data blocked for the time in which one or more of the listed circumstances occur:

- a. it must retain the data for the exercise of freedom of expression and information;
- b. it must comply with a legal obligation required by data processing;
- c. it is processing the data in the public interest or for scientific or historical research purposes, insofar as the deletion of the data would render impossible or gravely hinder the attainment of the goals of said processing.

### **3.4 Deletion of third-party personal data**

In accordance with the right of erasure, IICA shall proceed to eliminate personal data when any of the following circumstances occurs:

- a. when it is no longer necessary in relation to the purposes for which it was gathered or otherwise processed;
- b. when the data subject withdraws their consent on which the processing is based;
- c. when the data subject opposes the processing of its data and no legitimate reasons prevail;
- d. where it has been processed illegally.

### **3.5. Effects of the deletion of third-party personal data**

Deletion shall lead to the definitive destruction of data, in manner that guarantees that the information cannot be recovered, in any way, by IICA or by third parties, where relevant.

In cases in which data remains in a **non-digital format (on paper)**, IICA shall destroy it using a shredder and may delegate this task, whenever it deems this appropriate, to a supplier who must, in all cases, certify each document destruction process that is carried out. In these instances, the supplier shall sign a **Contract for Personal Data Access by Third Party (Annex 6)** with the assigned Data Processor, guaranteeing that, once the data has been destroyed, a certificate is provided accrediting that said work was done.

In cases in which the data is in a **digital format (electronic)**, deletion shall guarantee that the data cannot be recovered subsequently, by any means, covering all databases, archives and safe copies, regardless of where the data was housed, whether in software on company systems, in a SaaS service (Software as a Service), in external storage devices or on IICA's own equipment.

Provision must be made for the possibility that the personal data may have to be **blocked**, prior to deleting it completely, preventing its widespread processing and only enabling access to carry out administrative or judicial requirements and/or to comply with obligations of a strictly legal nature.

### **3.6 Retention term**


IICA has established a term of **(10) ten years** as of the date for termination of the processing and/or contractual relationship with the Institute (as a supplier, partner, grant executor, among others), unless this term must be modified when a particular and special circumstance arises that requires an adjustment.

This term may vary in the following cases:

- a. where there exists in the IICA Member States a national regulation regarding third-party data protection that differs from IICA's Personal Data Protection Policy, but which is applicable to Institute, while respecting IICA privileges and immunities;
- b. where due to the nature of the contractual relationship with the Institute, a term different to the abovementioned term has been established between the parties;
- c. where there exists a special situation that justifies a term different to the abovementioned one, and the parties have clearly expressed their agreement.

In circumstances in which two or more terms may be applicable for the same processing activity, IICA shall not proceed to definitive deletion until the end of the longest term.

## Annex 9 – Designation of the Data Protection Management Team

	<b>DOCUMENT TYPE</b>		<input type="checkbox"/> Public (available on the IICA website)
			<input checked="" type="checkbox"/> Private (available on IICA's intranet)
<b>TITLE</b>	Designation of Data Protection Management Team or data protection officer		
<b>APPLICATION</b>	All IICA Delegations and Units at Headquarters with access to and that process third-party personal data		
<b>FORMAT</b>	Electronic - Word		
<b>PAGES</b>	3		
<b>APPROVAL REF.</b>	SC/DG-404, SEPTEMBER 24, 2021		
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
1.0	[April 2022]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

To comply with the Data Protection Policy and the present Manual, IICA shall establish a Data Protection Management Team that routinely and systematically examines the data processing undertaken by the Institute, and independently issues its observations to the Institute's authorities.

### 2. Objective

To define the Data Protection Management Team, describe how to establish and appoint it, indicate what functions correspond to it and outline its position in the Institute.

### 3. Procedure

In accordance with international standards, IICA shall appoint a Data Protection Management Team as part of its staff, which is the equivalent to a Data Protection Officer, given the need to protect third-party data and its processing.

The function and level of authority of this Team is justified by the nature of the Institute and its scope, which requires that data processing be routinely and systematically observed, both on a large scale and individually, given that the Institute, in providing goods and services and awarding grants, has access to a considerable amount of third-party personal data on a national, regional and hemispheric level.

#### 3.1 Governance

The Data Protection Management Team shall be responsible for the governance of third-party personal data processing in the Institute.

This role shall include ensuring alignment between the Data Protection Policy, this Manual and the guidelines for compliance by third-party data collectors and holders.

The factors that will determine the Data Protection Management Team's ability to play a clear and effective role are as follows. It must:

- a. be physically accessible to the Institute's staff via a direct line or by any secure means of virtual communication,
- b. be capable of communicating effectively with data subjects and cooperating with the relevant review bodies, which means that communication must be made in the language used,
- c. adopt a multidisciplinary approach,
- d. have a wide range of knowledge and institutional experience,
- e. have access to and interaction with other areas of IICA necessary for carrying out its functions,
- f. have the capacity to propose, act and to enjoy the support of the Institute to execute decisions and measures adopted in the corresponding Units,
- g. have the necessary resources to carry out its activity, as well as to access personal data and processing operations,
- h. maintain independence and autonomy in exercising its functions, in developing proposals for improvements and in employing mechanisms to inform the senior Management of the Institute,
- i. have access to personal data and processing procedures, maintaining the obligation of confidentiality or secrecy,
- j. act as a mediator within the Institute, working with the relevant work groups responsible for data processing activities, and
- k. be consulted promptly if a violation of data or other incident occurs.
- l. The Institute shall notify all relevant staff and review bodies once the Data Protection Management Team has been appointed, in order to ensure that those involved, the data subjects and the review bodies can contact the Team easily, directly and confidentially.
- m. The Data Protection Management Team shall not be held personally liable in the event of a breach of data protection regulations, as it is the responsibility of IICA to guarantee and demonstrate that third-party data processing is being undertaken by the Institute, as the Data controller, in compliance with institutional regulations.

### **3.2 Functions of the Data Protection Management Team**

IICA shall designate a Data Protection Management Team which shall be responsible for coordinating, carrying out necessary actions and providing guidance for implementing the IICA Personal Data Protection Policy and the present Manual, with the support of the Administrators in IICA Delegations in the Member States and the Units at Headquarters that have access to or process third-party personal data.

The functions of the Data Protection Management Team are to:

- a. Facilitate and promote compliance with third-party data protection regulations.


- b. Promote the use of tools, systems, platforms and methodologies that allow the Institute to comply with the principles for third-party personal data processing, abiding by international standards.
- c. Promote the design and implementation of procedures that involve third-party personal data processing.
- d. Organize training and knowledge transfer exercises so that IICA staff have access to third-party personal data, and do so in compliance with the Data Protection Policy and the present Manual.
- e. Manage assessments, monitoring and auditing undertaken with the corresponding Units in the Institute, devising actions for improvement where weaknesses are identified in these processes.
- f. Maintain document secrecy and confidentiality in relation to the performance of their functions.
- g. Coordinate with IICA Delegations in the Member States and Units at Headquarters to maintain an up-to-date Data Processing Register, by adding, modifying or excluding content from the Register.
- h. Maintain an up-to-date incident log regarding personal data processing; and a log of reports or complaints received through the official institutional channels and their handling until the conclusion of the incident, report or complaint.
- i. Notify the Director of Corporate Services and the Director General in a timely manner of relevant aspects in data protection processing that may constitute real or potential risks for the Institute.
- j. Issue an annual report to the Director of Corporate Services and the Director General indicating the tasks performed by the Data Protection Management Team or Data Protection Officer regarding third-party personal data processing, for the year ending.
- k. Assess the effectiveness of technical and organizational measures for guaranteeing processing security.
- l. Support all institutional actions or those carried out by the review bodies of the Institute regarding issues that involve personal data processing.
- m. Safeguard IICA's institutional interests, ensuring the scope of responsibility and institutional defense.

### **3.3 Designation of the Data Protection Management Team**

The members of the Data Protection Management Team may perform other tasks and functions within the Institute, provided that these do not lead to a conflict of interest. The absence of a conflict of interest is closely tied to the requirement to act independently, while also serving as an internal advisor and supervisor.

Furthermore, this role may not be performed by staff members involved in decision-making about when and how to process data (e.g., systems managers, human resources managers or any management position in general).

## Annex 10 – Rights and obligations of IICA employees

	<b>TYPE OF DOCUMENT</b>	<input type="checkbox"/>	Public (available on the IICA website)
		<input checked="" type="checkbox"/>	Private (available on IICA's intranet)
<b>TITLE</b>	Rights and obligations of IICA employees with respect to personal data protection		
<b>APPLICATION</b>	All IICA Delegations and Units at Headquarters with access to and that process personal data.		
<b>FORMAT</b>	Electronic - Word		
<b>PAGES</b>	7		
<b>REF. APPROVAL</b>	SC/DG-xxx		
<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	
2.0	[30.January.2023]	Inter-American Institute for Cooperation on Agriculture	

### 1. Introduction

IICA, in fulfilling its mission to encourage, promote and support the efforts of its Member States to achieve agricultural development and rural well-being through technical cooperation of excellence, must collect and process personal data (from employees, institutions, organizations, partners, consultants and suppliers, among others).

Employees are required to provide all relevant personal data needed within the context of their contractual relationship with IICA, which shall be collected and processed in keeping with the provisions established in IICA's Personal Data Protection Policy and the guidelines set out in the Procedural Manual on Personal Data Protection. Therefore, IICA may request personal data from its employees, in keeping with its legal obligations in each Member State and institutional regulations.

### 2. Purpose

To identify, define and specify IICA's responsibility in processing the personal data of its employees and the rights that support this.

### 3. Procedure

This Annex establishes the guidelines for collecting and storing the personal data of employees.

### 4. General principles

The personal data of employees shall be processed in line with the principles established in the Personal Data Protection Policy and the guidelines set out in the Procedural Manual on Personal Data Protection.

IICA considers personal data protection to be a fundamental right, which recognizes the right of data subjects to control their data, and therefore, the need to gain their consent to collect it. IICA employees may not waive their personal data protection rights. Any document or declaration that waives this right shall be considered null and void.

## **5. Rights of the employee**

- 5.1 Employees' personal data shall be processed in an impartial and legal manner and shall be limited exclusively to matters directly related to their work relationship with the Institute.
- 5.2 Due diligence shall be exercised by IICA when processing the data collected from its employees.
- 5.3 When processing the personal data of employees, the Institute shall apply the principles outlined in the Personal Data Protection Policy.
- 5.4 All IICA employees must provide their explicit and written consent for the Institute to collect and process their personal data, as described in Section 7. This consent must be included in an employee's work contract or appended as an addendum to the contract.
- 5.5 Employees shall have the right to be informed prior to the processing of their personal data. Moreover, in principle, employees are the ones that should provide all the personal data on themselves that may be required by the Institute.
- 5.6 If the Institute has the need to disclose the personal data of an employee to a third party, the employee shall be asked to sign a statement of consent. The statement should specifically state the name of the individuals, institutions or organizations that will receive the data, the specific data that will be sent, the purpose for collecting the data and the timeframe within which the data may be used. This consent will not be required in instances in which the Institute has been legally summoned to disclose this information.
- 5.7 IICA is not authorized to collect data on employees referring to: ethnic origin or race, political opinions, religious or philosophical convictions, or trade union affiliations, nor can it process 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.

- 5.8 In exceptional circumstances, IICA may collect personal data on the above-mentioned matters, provided that the data directly affects a work-related decision.
- 5.9 Medical data may only be collected in accordance with national legislation, while respecting medical confidentiality and the general principles of health and safety at work, and only when needed to:
- 5.9.1 decide if an employee may occupy a specific job;
  - 5.9.2 comply with health and safety requirements at work; or
  - 5.9.3 determine the employee's right to social security and its benefits.
- 5.10 IICA shall not process the personal data of an employee other than what was requested or in cases in which the data subject may have misinterpreted what was asked of him/her.
- 5.11 IICA shall not use polygraphs, lie detectors or other similar means or procedures to determine the truthfulness of the data.
- 5.12 Genetic tests shall not be conducted by the Institute on its employees or shall be limited to instances that are explicitly authorized by national legislation.
- 5.13 Toxicological studies shall be conducted only in accordance with national legislation or international standards.
- 5.14 When employees are subject to surveillance measures, they must be told in advance about the justification for doing so, the times when this is taking place, the methods and technology that will be used and the data that will be collected. Furthermore, IICA shall limit its intrusion into the private lives of employees as much as possible.
- 5.15 Secrecy in monitoring shall only be allowed when there is sufficient reason for suspicion of criminal activity or serious offenses.
- 5.16 Continuous surveillance is only permissible if required for reasons of health, security or the protection of institutional assets.

## **6. Obligations of employees**



- 6.1 IICA employees should inform and familiarize themselves with the scope of the Data Protection Policy and the procedures contained in this Manual.
- 6.2 Within IICA, the personal data of employees shall be made available solely to specific authorized users, with access limited to the information that is needed to carry out their respective tasks.
- 6.3 All employees that have access to the personal data that is processed or that are involved in its processing shall be bound to maintain strict confidentiality regarding official matters, even when processing data for legal or judicial matters. In the IICA delegations in the Member States, the Representative is in charge of and responsible for providing the personal data of employees when it is required for legal or judicial actions, whereas at Headquarters, that responsibility shall be assumed by the Human Talent Division. However, in both cases, the relevant individuals shall have the opportunity to make the relevant consultations, both within the Institute or, when necessary, to entities outside of the Institute, for the sole aim of acting in accordance with IICA's Personal Data Protection Policy.
- 6.4 The processing of sensitive personal data shall be permissible only when needed to comply with an IICA mandate and when it is in line with the Personal Data Protection Policy. Moreover, this processing shall be undertaken utilizing the technical and organizational measures described in this Manual.
- 6.5 IICA as the data controller that will receive and process the personal data of its employees may only engage the services of data "processors"<sup>1</sup> that provide the necessary commitments and guarantees to comply with the requirements established in this Manual and established in **Annex 6** of this Procedural Manual on Personal Data Protection.
- 6.6 Depending on the purpose for processing the data, IICA employees may share with specific third parties (associates, government entities or duly authorized service providers), the information needed for the provision of its services.
- 6.7 Employees shall refrain from circulating information with the personal data of other employees to which they have access in order to perform their functions.

---

<sup>1</sup> **Personal data processor:** Individual or legal entity that is processing data on behalf of IICA.

6.8 The responsibility to respond to data subjects' exercise of their rights (to access, rectification, suppression, restriction of processing, objection and portability of personal data) shall be assigned explicitly to specific employees, who shall undertake this function, pursuant to the provisions of **Annex 4** of this Manual. This process shall be determined by the requests from the respective data subjects and shall be documented by the employee responsible.

## **7. Explicit and documented consent**

7.1 All employees must provide explicit and written consent to authorize the processing of their personal data, essentially to ensure that they have been given sufficient information about what data will be collected and how it will be processed.

7.2 To ensure that explicit and written consent has been given by the employee, all work contracts shall include the following clause:

“CLAUSE XX: The Employee declares that he/she is aware of and understands IICA’s Personal Data Protection Policy and its Manual. The Employee understands, accepts, and thereby authorizes IICA to collect and process any personal data that may be required during the term of this work contract, if it is for a justifiable purpose. All IICA employees are covered by this Policy regarding the collection and processing of their personal data”.

## **8. Sharing the personal data of IICA employees**

8.1. The stipulation that employees’ personal data may only be processed for purposes relevant to their work relationship with IICA must also be respected when this data is shared with others outside of the Institute. Thus, the sharing of data for commercial or marketing purposes is prohibited, unless employees have given their expressed consent.

8.2. Employees must accept when personal data is shared in order to comply with legal obligations, such as data related to employer and work obligations, as well as information needed for work safety and health, judicial procedures or the application of the penal code.

8.3. In all cases, IICA shall specifically indicate to those with whom the personal data of employees will be shared that they may only use this data for the stated purposes and instruct them to verify that they have complied with these instructions. This does not apply to routine sharing of information in fulfillment of national labor regulations.

## **9. Storage of personal data**

- 9.1. The guidelines contained in Annex 8 of this Manual govern the storage of personal data.
- 9.2. Personal data protected by medical confidentiality shall only be held in the care of a person bound by secrecy and kept separate from all other personal data.

## **10. Sensitization**

IICA, by way of its Personal Data Protection Management Team, shall provide training to its employees and shall adopt the appropriate measures to ensure the effective application of the Personal Data Protection Policy and the Procedural Manual on Personal Data Protection.

## **11. Complaints**

Employees, who, based on the provisions of the Personal Data Protection Policy and its corresponding Manual, consider that the processing of their data has been inappropriate, have the right to file a complaint.

The complaint should be filed in accordance with the procedure outlined in sub-section 9.2 (**Complaints related to personal data protection**) of this Manual, which falls under section IX (**Requests and complaints related to personal data protection**).

All complaints received by the Institute for the presumed breach of the aforementioned Policy shall be immediately investigated, ensuring the strictest confidentiality, while always aiming to protect those filing the complaints and to follow due process.

All individuals are bound to collaborate fully with the Ethics Committee in charge of undertaking the investigation and must maintain the confidentiality of the case.

## **12. Responsibilities**

The failure of an employee to comply with the Personal Data Protection Policy and this Manual may constitute improper conduct (if it is the result of grave negligence, recklessness or a deliberate act), for which the Institute shall be empowered to impose disciplinary measures, in keeping with institutional regulations on the matter.