Personal Data Protection Policy

Version 1

Effective Date: December 1, 2018

Document Control

The Head of Knowledge Management Unit will be responsible for the periodic review of this document.

Document Responsibility

Title	Personal Data Protection Policy
Directorate	Office of the Director General
Unit	Knowledge Management Unit
Manager	Head of Knowledge Management Unit
Applicable to	All Staff

Document Revision History

Version	Endorsed By	Meeting Reference	Date Endorsed	Approved By	Meeting Reference	Date Approved	Effective Date	Sections Modified
1	Senior Leadership Team	SLT-SI-10-18	15-Oct-18	Board of Trustees	BOT68-D28	30-Nov-18	1-Dec-18	New Policy

Table of Contents

1. Purpose

1.1. The International Centre for Research in Agroforestry (ICRAF) needs to gather and use certain personal data about individuals to effectively perform its work.

1.2. These can include personal data from staff, consultants, partner organizations, suppliers, research participants, donors and other individuals that ICRAF has a relationship with or may need to contact.

1.3. ICRAF is committed to complying with international data protection laws. Ensuring data protection is the foundation of trustworthy research, development partnerships and responsible leadership. The Personal Data Protection Policy sets a globally applicable data protection and security standard for our Centre and regulates the sharing of information between the Centre and our partners. It provides one of the necessary framework conditions for cross-border data transmission among its regional programmes and partners worldwide. The policy also ensures an adequate level of data protection as prescribed by global best practices, and is applicable in countries that do not yet have adequate data protection laws.

2. Scope

2.1. This is a Centre-wide Policy and is applicable to all staff located in all countries where the Centre operates.

2.2. Every staff member who is processing personal data is obliged to handle these data confidentially and be compliant with this policy.

2.3. Every staff member will sign a statement to this effect and shall receive a guideline developed by from the data protection officer (DSB) from the Human Resources Unit.

2.4. The DSB needs to be informed about the responsibilities of staff members and their work place in order to prepare for the necessary training by the DSB and to assess the possible need for additional controls.

3. Definitions

3.1. **Consent** means freely given, specific, informed and unambiguous indication by a data subject that signifies agreement to the processing of personal data relating to them.

3.2. **Controller** means a person that determines the purpose and means of processing personal data. For purposes of this Policy, the Controller shall mean ICRAF.

3.3. **Data Protection Officer** means the person responsible for overseeing the data protection policy, strategy and implementation to ensure compliance.

3.4. **Data Subject** means an identified or identifiable natural person capable of having personal data.

3.5. **Personal Data** means any information relating to a Data Subject who can, directly or indirectly, be identified by reference to an identifier. This covers anything from images, location data, email address, name or identification number.

3.6. **Processing** means any operation or set of operations performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.7. **Processor** means a person or legal entity who processes personal data on behalf of the Controller.

3.8. **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Source: GDPR, Art. 4, § 5).

3.9. **Sensitive Personal Data** means "special categories of personal data" that specifically include genetic data, ethnicity, sexual orientation or religion, and biometric data where processed to uniquely identify an individual.

4. Policy Statement

4.1. This Personal Data Protection Policy comprises the internationally-accepted data privacy principles without replacing existing national laws where the Centre operates. It supplements the national privacy laws. Relevant national laws will take precedence if there is a conflict with this Personal Data Protection Policy, or if it has stricter requirements than this Policy. The content of this Personal Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

4.2. This Policy is underpinned by the following principles, which state that data shall:

4.3. **Fairness and lawfulness:** Be processed fairly and lawfully. ICRAF shall ensure that all personal data processed will be done through one of the following legal bases:

4.3.1. **Consent**: The individual has given clear consent for you to process their personal data for a specific purpose.

4.3.1.1. Requires a positive opt-in. No pre-ticked boxes or default consent.

4.3.1.2. Requires a very clear and specific statement of consent.

4.3.1.3. Consent can be withdrawn at any time.

4.3.1.4. Consent of the data subject will not be required in certain circumstances, for example to protect certain vital interests.

4.3.1.5. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

4.3.1.6. Where communications are sent to data subjects based on their consent, the option for the data subject to revoke their consent should be clearly available and systems should be in place to ensure such revocation is accurately reflected in ICRAF's system.

4.3.2. **Contract**: The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

4.3.3. **Legal obligation**: The processing is necessary for you to comply with the law (not including contractual obligations).

4.3.4. **Vital interests**: The processing is necessary to protect someone's life.

4.3.5. **Public task**: The processing is necessary for ICRAF to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

4.3.6. **Legitimate interests**: The processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Three-step processes for consideration before processing personal data under this heading comprise:

4.3.6.1. Purpose

4.3.6.2. Necessity

4.3.6.3. Balancing of interests

4.3.7. **Transparency:** Be processed transparently – data subjects must be informed of how their data is being handled.

4.3.7.1. The DSB maintains a record of all personal data processing activities in the responsibility of the Centre. The staff member responsible for the relevant processing activities shall document and report them to the DSB in good time according to requirements specified by the DSB.

4.3.8. **Restriction to a specific purpose**: Only be processed for the purposes for which it was collected.

4.3.9. **Data economy:** Be adequate, relevant and not excessive.

4.3.10. **Factual accuracy:** Be accurate and kept up-to-date.

4.3.11. **Deletion:** Not be retained for any longer than is necessary.

4.3.12. **Confidentiality:** Be processed in accordance with the rights of data subjects.

4.3.13. **Data security**: Be processed in a manner that ensures appropriate security of the personal data.

4.4. **Personal Data Storage**

4.4.1. ICRAF shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4.4.2. ICRAF shall take every opportunity to ensure that the data is accurate:

4.4.2.1. ICRAF will make it easy for data subjects to update the information that it holds about them.

4.4.2.2. Personal data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

4.4.2.3. Personal data shall be updated as errors are discovered.

4.4.3. To ensure that personal data is kept for no longer than necessary, ICRAF shall put in place an archiving procedure for each area in which personal data is processed and review this process biennially.

4.4.3.1. The archiving policy shall consider what data should/must be retained, for how long, and why.

4.4.3.2. Save for a lawful purpose, in no event shall ICRAF store personal data for longer than 10 years after the contact with the data subject has ceased.

4.4.3.3. Personal data may also be anonymized in case other details of a data subject are required for use after the 10-year mark. For example, for surveys and analysis.

4.5. **Security of Processing**

4.5.1. ICRAF shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, among others where applicable:

4.5.1.1. Pseudonymisation and encryption of personal data;

4.5.1.2. Assurance of ongoing confidentiality, availability and resilience of processing systems and services;

4.5.1.3. Assurance of restoring the availability and access to personal data in a timely manner;

4.5.1.4. Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.6. **Personal Data Breach**

4.6.1. In the event of a personal data breach, the Centre shall, where required by law, inform a supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

4.6.2. The notification referred to in paragraph 4.6.1 shall at least describe:

4.6.2.1. The nature of the personal data breach;

4.6.2.2. The name and contact details of the data protection officer or another contact point where more information can be obtained;

4.6.2.3. The likely consequences of the personal data breach;

4.6.2.4. The measures taken or proposed to be taken by the Centre to address the personal data breach.

4.6.3. The Centre shall document any personal data breaches, comprising the facts relating to the data breach, its effects and the remedial action taken.

4.7. **Transfer of Personal Data**

4.7.1. ICRAF shall ensure appropriate safeguards are in place before transferring personal data out of the organization's control.

4.7.2. These safeguards may include:

4.7.2.1. Legally binding agreement with standard data protection clauses

4.7.2.2. Binding policy positions

4.7.2.3. Compliance with an approved code of conduct from a supervisory authority

4.7.3. Data transfers without applying the safeguards above are forbidden unless:

4.7.3.1. Made with the individual's informed consent

4.7.3.2. Necessary for the performance of a contract between the individual and the organization or for pre-contractual steps taken at the individual's request

4.7.3.3. Necessary for the performance of a contract made in the interests of the individual between the controller and another person;

4.7.3.4. Necessary for important reasons of public interest

4.7.3.5. Necessary for the establishment, exercise or defence of legal claims

4.7.3.6. Necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent, or

4.7.3.7. Made from a register which is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

4.8. **Rights of Data Subjects**

4.8.1. **Right to be informed** – Typically through a Privacy Notice. ICRAF will be transparent about the use of personal data, e.g., for staff or consulting contracts, collection via web forms, surveys and questionnaires.

4.8.2. **Access** – Individuals upon request to the Data Protection Officer will be provided with access to their personal data and other supplementary information including the fact that the data is being processed. Information should be accessed for free.

4.8.3. **Rectification** – If data is inaccurate or incomplete, the individual can request for the same to be rectified.

4.8.4. **Erasure** – This is also known as the Right to be Forgotten. Individuals may request that their personal data be removed. This is not absolute. A Controller can legally decline a request for some specific reasons including:

4.8.4.1. Right of Freedom of Expression and Information

4.8.4.2. To comply with a legal obligation

4.8.4.3. Public interest

4.8.4.4. Archiving purposes

4.8.4.5. Exercise or defence of legal claims

4.8.5. **Restrict Processing** – To block the further processing of data. The Controller may still be able to store the data.

4.8.6. **Data Portability** – The right to receive the data in a format that can be easily transferred to another organization.

4.8.7. **To Object** to their data being used for processing. If the organization has a legitimate right to process the data, then the individual cannot object. For example, an individual can't prevent the organization they work for from keeping the personal information required for personnel management.

4.9. **Record of Processing Activities**

4.9.1. To ensure its processing of data is lawful, fair and transparent, ICRAF shall maintain a record of all processing activities under its responsibility.

4.9.2. Each organisational unit shall appoint at least one individual who is responsible to collect and document the necessary information about data processing activities in the respective unit.

4.9.3. Upon request, the Centre will make the record of processing activities available to the relevant government agencies.

4.10. **Procurement of IT Systems and Services**

4.10.1. The Centre shall ensure that tender specifications for the procurement of IT systems and services include data protection elements.

4.10.2. If the procurement of an IT system or service involves a new mechanism to process personal data, then the Data Protection Officer needs to be informed in good time. The procurement can only proceed with a by the DSO. The DSO advises the respective unit if a data protection impact assessment (DPIA) needs to be conducted.

4.10.3. It is not permitted to process personal data using IT systems and services that are designated for private use. The official use of privately owned IT systems needs to be approved by the ICT Unit.

4.10.4. As part of its IT asset management, the ICT Unit maintains a detailed inventory of all IT systems and services to ensure strong IT security and compliance. The inventory is accessible to the DPO at all times.

5. Roles and Responsibilities

5.1. The Director General is responsible for determining the purposes and means of the processing of personal data within the meaning of this Policy and shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing of

personal data is performed in accordance with this Policy. Those measures shall be reviewed and updated where necessary.

5.2. The heads of the relevant organizational units process personal data only on behalf of the Director General with the sufficient guarantees to implement appropriate technical and organisational measures that meet the requirements of this policy to process personal data and to ensure that the rights of data subjects are protected.

5.2.1. The Centre has appointed a Data Protection Officer (DPO) based in the Knowledge Management Unit at ICRAF Headquarters.

5.2.2. The tasks of the DPO include, but are not limited to the following:

5.2.2.1. Inform and advise the Director General as the controller, the relevant organizational unit as the processor and its employees who process personal data pursuant to this policy;

5.2.2.2. Monitor compliance with this policy, with national or other data protection provisions and with policies of the Director General's Office or the relevant organizational unit in relation to the protection of personal data;

5.2.2.3. Maintain inventories of information provided by data controllers and data protection focal points, including data transfer agreements, specific instances of data sharing of ICRAF with third parties, data protection impact assessments, data breach notifications and complaints by data subjects;

5.2.2.4. Provide advice where requested and actively encourage data controllers and other relevant actors to undertake measures aimed at compliance with this Policy;

5.2.2.5. Monitor and report on compliance with this Policy;

5.2.2.6. Liaise with the relevant supervisory authorities as necessary under this Policy.

5.2.3. The Data Protection Officer shall submit an annual data protection report, through the Deputy Director General of Research, to the Director General.

5.2.4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Policy.

5.2.5. The DPO shall be bound to by secrecy or confidentiality concerning the performance of his/her tasks, in according with Centre policies.

5.2.6. The DPO may fulfil other tasks and duties. The Director General as the controller or the head of a data processing organizational unit ensure that any such tasks and duties shall not result in a conflict of interests.

6. Review

6.1. This Policy will be reviewed every three years or earlier if required by the Legal Office.

6.2. Any changes made to the Policy will be presented to the Senior Leadership Team for endorsement and thereafter submitted to the Board of Trustees for approval.

7. Related Documentation

7.1. Human Resources Policy and Procedures Manual

7.2. ICT Privacy and Acceptable Use Policy

7.3. Research Data Management Policy

7.4. Research Ethics Policy

7.5. Research Misconduct Policy

7.6. Risk Management Policy