Food and Agriculture Organization of the United Nations

administrative circular

No. 2022/06
Date: 8 July 2022

DATA PROTECTION POLICY

I. INTRODUCTION

1. As stipulated in Article I of its Constitution, one of the functions of FAO is "*to collect, analyze, interpret and disseminate information relating to nutrition, food and agriculture*".[1] The Strategic Framework 2022-31 further indicates that one of FAO's core functions is to "*assemble, analyse, monitor and improve access to data and information, in areas related to FAO's mandate"* and "*advocate and communicate at national, regional and global levels, including to consumers, leveraging the Organization's knowledge, data, position as UN specialized agency, and trusted role as neutral broker*".[2]

2. Data is a strategic asset for delivering the mandate of FAO. FAO should be able to utilize this asset, without undermining or putting it at risk. A data protection policy is essential to ensure the protection of data processed by FAO and guarantee its value, use, and integrity.

3. Any data[3] used or processed by FAO, or transferred to a third party by FAO, must be processed correctly and consistently throughout the data lifecycle, that is, from initial collection, storage to deletion.

4. Unauthorized disclosures, misuse and improper processing of data, as well as the processing of poor-quality data, expose the Organization to legal, financial, operational and reputational risks. A properly implemented data protection policy contributes to enhancing trust in the Organization and its work. It is imperative that any data held by FAO, or entrusted by FAO to a third party, is appropriately protected.

5. In order to mitigate risks and enhance protection, this present Policy sets out the FAO Data Protection FIRST Principles, which are detailed in part III of this Policy. These overarching principles are aligned with international data protection standards and controls, including those of the United Nations system[4] and are applicable to the entire lifecycle of data processing: how data is collected, how data must be kept and processed, and how and when it should be deleted.

---

[1] Constitution, Article I (1).
[2] FAO Strategic Framework 2022-31, paragraph 43.
[3] See paragraph 9 below and Annex I "*Definitions*".
[4] See, for example, the "*Data Strategy of the Secretary General for Action by Everyone, Everywhere: With Insight, Impact and Integrity*" and the "*UN Principles on Personal Data-Protection Privacy*".

6. As further detailed under section III, the Data Protection FIRST Principles are:

- ✓ **F**airness
- ✓ **I**ntegrity
- ✓ **R**esponsibility
- ✓ **S**ecurity
- ✓ **T**ransparency

7. The Data Protection FIRST Principles, together with the obligations arising from them, are high-level and are neutral with respect to technology. They provide, therefore, for flexibility in their daily application. Personnel should translate the Principles into measures and tools that fit their specific business needs while, at the same time, ensuring a proportionate level of protection of the data that they process. Supplementary operational guidance will be issued under this Policy addressing specific types of activities requiring data processing.

II. SCOPE AND APPLICATION

8. Given FAO's legal status as a UN specialized agency enjoying privileges and immunities and the non-applicability of national or regional laws to its activities, this Policy establishes the overarching principles and the rules that govern FAO's processing and protection of data. [5]

9. This Policy does not apply to public data, as described under paragraph 14, nor to anonymized data, as defined in Annex I. This Policy applies to all other data, in any form[6], including non-personal data and personal data, disclosed by a legal or natural person to FAO or originating from FAO.[7]

10. This Policy applies to all activities and operations involving the processing of data by FAO and by third parties in their dealings with FAO. All personnel must process data in accordance with this Policy. All other internal rules and policies addressing specific aspects of data protection must be implemented and interpreted in accordance with this Policy. In the case of any inconsistency, this Policy will prevail.

11. The present Policy sets the minimum standards for protecting data generated by FAO or entrusted to FAO by a legal person or an individual (i.e. a data provider). It also establishes the internal corporate mechanisms to oversee the implementation of the Data protection FIRST Principles and to monitor the Policy so that it remains fit for purpose. The definitions of the terms used in this Policy are provided in **Annex I.** Examples on how to apply the Data Protection FIRST Principles are set out in **Annex II**.

---

[5] This Policy is to be applied having due regard to FAO's Basic Attributes, including its intergovernmental status and neutrality and the authority to provide a neutral platform where nations can call on each other for dialogue and knowledge exchange, as well as its authority to request any Member to submit information relating to the purpose of the Organization. See the FAO Basic Texts, including, *inter alia*, Articles I and VI of the Constitution, and the FAO Strategic Framework 2022-31.

[6] Digital or paper forms.

[7] This Policy applies regardless of whether data is provided by the individual whose data is being processed, or by a different entity (for example, where a Member provides information concerning individuals located within its jurisdiction).

III. THE FIVE DATA PROTECTION FIRST PRINCIPLES

1. FAIRNESS

"We process data on a legitimate basis and for a specified purpose only. We only collect and keep the minimum amount of data we need"

1.1 Key points Fairness means FAO processes data in ways that the data provider would reasonably expect. This requires identifying a legitimate basis for the processing, as well as a well-defined business purpose. FAO should also collect only the minimum data elements necessary for such purpose. Once this purpose has been fulfilled, the data should no longer be retained.

1.2 Responsibilities

1.2.1 Legitimate Basis — Personnel may only process data as part of FAO activities undertaken within the context of its mandate and in line with its legal framework. In addition to confirming the above, personnel must establish one of the following legitimate bases to process data: (*i*) the prior informed consent[8] of the data provider given either by a written or oral statement or by another clear affirmative action of the data provider; [9] (*ii*) the vital interests of an individual in the event that the prior informed consent cannot be obtained;[10] or (*iii*) the need to implement a legal agreement concluded prior to processing (for example, to implement the terms of a concluded contract of employment).

1.2.2 Purpose Specification — The specific purpose for processing the data must be identified prior to collection.

1.2.3 Further Processing — Data may only be processed for a new purpose if such processing complies with one or more of the following: (*i*) is compatible with the initial purpose; (*ii)* has its own legitimate basis; (*iii*) is based on a new expression of consent, if consent provided the initial legitimate basis; (*iv*) relates to statistical or research related activities in furtherance of FAO technical mandate; (*v*) for archiving purpose in accordance with Manual Section 601 on Records and Archives Management.

[8] The prior informed consent of the data provider, often supported by other legitimate bases, is the preferred basis for processing data. In some cases, however, obtaining the prior informed consent may be impractical, e.g. due to an emergency. Therefore, in case of exceptional emergency circumstances, and limited to the duration of such circumstances, personnel may process data on the basis of implicit consent. Personnel must, in such a case, ensure that data providers were provided with sufficient information on the data processing by FAO. Once the emergency circumstances have come to an end, personnel must ensure to obtain promptly the informed consent of the data provider. The reasons for not obtaining the prior informed consent must be fully recorded and regularly reviewed to confirm that circumstances precluding the prior informed consent have not changed. Exceptional circumstances of this nature do not exempt personnel from complying with all other elements of this Policy.

[9] A data provider may withdraw consent. Guidance on addressing withdrawal of consent is found in paragraph 33.c. See also processing of sensitive data under paragraph 24 below.

[10] In exceptional circumstances, where it is not possible to obtain the prior informed consent - for example, when processing is necessary to protect an individual's life, integrity, health, or security or that of another person - data may be processed based on the basis of the vital interest. The reasons for not obtaining the prior informed consent must be fully recorded and regularly reviewed to confirm that circumstances precluding consent have not changed. For example, exceptional circumstances of this nature do not exempt personnel from complying with all other elements of this Policy.

1.2.4 Necessity	To the extent practicable, only the minimum amount of data that is needed to achieve the specific purpose should be collected and processed. Data that is unnecessary, irrelevant or excessive in relation to that purpose should not be collected or processed.
1.2.5 Retention	Data must be retained only for the duration needed to achieve the purpose for which the data was collected. When that purpose has been achieved, and unless data is processed for statistical, research or archiving purposes, the data must be deleted or anonymized, as appropriate, within a reasonable period following the achievement of the purpose. Data may be stored for a longer period than the period necessary for the fulfilment of the purpose for which they were collected, to the extent that there is a legitimate purpose for retaining the data (such as complying with retention periods imposed by the FAO rules or agreements with beneficiary countries and resource partners).
1.2.6 Retention and deletion processes	Personnel must implement appropriate standards, processes and tools to ensure the limited retention and subsequent deletion of the data.
1.2.7 Retention by a Third Party	When data is to be transferred to a third party, personnel must ensure that the third party is contractually obliged to destroy or return to FAO all the data transferred once the purpose of the data transfer is achieved or upon termination or expiry of the agreement under which the data was transferred, unless the third party has the explicit consent from the data provider to continue processing.

2. INTEGRITY

"*We verify that data is accurate. We delete or rectify any inaccurate or unreliable data*"

2.1 Key points	Integrity means implementing processes and controls aimed at ensuring the overall accuracy of the data. This is required to ensure effective use and interpretation. Prior to collection and throughout the data lifecycle, personnel should adopt reasonable measures to ensure the accuracy and reliability of the data they process. If, for any reason and at any time, it is determined that data is inaccurate or misleading, immediate steps must be taken to ensure that it is rectified or deleted.
2.2 Responsibilities	
2.2.1 General obligation	Personnel are individually responsible for the accuracy of the data they process. To that effect, personnel must take all reasonable steps to ensure the accuracy of the data.
2.2.2 Recording and Deletion	All reasonable steps must be taken to: (*i*) record and process only accurate data, and (*ii*) ensure that any inaccurate data is promptly deleted or rectified.
2.2.3 Review	Processes must be put in place to regularly review the accuracy of data, with the aim of preventing and minimizing errors or inconsistencies.

3. RESPONSIBILITY

"*We proactively comply with the Data Protection FIRST Principles and are able to demonstrate our compliance*"

3.1 Key points

All personnel must comply with the Data Protection FIRST Principles and must be able to demonstrate that they have taken reasonable measures to ensure compliance with this Policy, as well as related guidelines and procedures defined by the Organization.

3.2 Responsibilities

3.2.1 General Obligation

Adequate and proportionate measures must be adopted to ensure and demonstrate that the processing of data is performed in accordance with this Policy. Before processing data, measures must be taken to design the processing operation in such a way as to prevent or minimize the risks to the data provider and to the Organization. These measures must also ensure that only the data necessary to achieve the specific purpose will be collected. Those measures must be regularly reviewed, and updated as required.

3.2.2 Evidence of compliance

While dependent upon the specific data processing activity in question, actions that may demonstrate compliance include, but are not necessarily limited to, the following:

- Maintain up-to-date records of processing activities which should include, at a minimum, information on the purpose of the processing, the data processed, the confidentiality level and, as appropriate, recipients of the data (both internal and external), envisaged retention periods and the security measures put in place.
- Undertake, prior to processing, an assessment ("a data protection impact assessment") identifying, addressing and mitigating risks in the event of a processing operation that is likely to result in a high risk[11] for the data provider or the Organization. To assess whether processing presents a high risk, personnel shall determine the likelihood and severity of any potential harm to the data provider or the Organization. When it is determined that a processing operation will likely result in a high risk for the data provider or the Organization, the Data Protection Unit[12] should be consulted for advice and guidance on possible mitigation measures and implementation.
- Design the processing in such a manner to prevent, avoid, or minimize the identified risks.
- Implement processes and procedures for handling and responding to requests from data providers.
- Implement processes, methods and techniques to ensure a level of security proportionate to the confidentiality level, classified in accordance

[11] Examples of a data processing that may result in a high risk for a data provider or FAO include, but are not limited to, the implementation of new systems or technologies, or the processing of sensitive data.

[12] See paragraph 45 below.

with Section IV below. Such steps may include anonymization, pseudonymization or encryption (see **Annex I**).

4. SECURITY

"We protect data by adopting reasonable measures against external and internal threats"

4.1 Key points

FAO is responsible for the data that it processes and personnel must adopt reasonable security measures to protect it. These measures should preserve the confidentiality of the data against unauthorized disclosure or use, uphold the integrity of the data by preventing unauthorized modification, and ensuring only authorized access. All personnel are individually responsible for assessing the risks arising from a specific processing operation and ensuring that reasonable security measures are in place.

4.2 Responsibilities

4.2.1 General obligation	Personnel must protect the data they process in conformity with relevant Manual Sections and related administrative issuances.
4.2.2 Appropriate security measures	Based on the level of confidentiality of the data, appropriate organizational, physical, and technical security measures, procedures and controls must be taken to safeguard data. Such security measures, procedures, and controls must, at all times, be proportionate and responsive to the risks identified by personnel through the assessment conducted pursuant to paragraph 3.2.1.
4.2.3 Review	Personnel should periodically review and, as necessary, update the security measures they have implemented pursuant to paragraph 4.2.2 above.
4.2.4 Use of ICT resources	All ICT systems, including Management Information Systems, used for the handling or storage of data that falls within the scope of this Policy must be managed in compliance with Manual Section 505 and any other relevant provisions of the Administrative Manual.
4.2.5 Storage	Taking into account the level of confidentiality, data must be stored in appropriate locations and in a manner that protects it from accidental or unauthorized processing, loss or corruption. If data is to be processed or stored by a cloud service provider, the FAO Cloud Adoption Strategy and Cloud Computing Guidelines and Risk Assessment Process apply.
4.2.6 Access to data	Taking into account the level of confidentiality attributed to the data, access to the data may only be authorized and granted to those who have a need to know in order to fulfil the processing purpose. A register of the names of authorized persons and the access rights they have been granted must be maintained. Personnel must confirm, prior to transferring data to third parties for processing, that the third parties' security measures are at least as comparable to those that are required for data of the same confidentiality classification in FAO.

5. TRANSPARENCY

"We are clear and open about what data we process, why, and how we use such data. We can explain this in clear terms to the data provider"

5.1 Key points	The transparency principle means being clear and open with data providers at the time of collection, i.e. "*what*" data FAO intends to process, "*why*" the processing is required, and "*how*" the data will be processed. The level of information to be provided will vary depending on the nature of the data and the operational context.
5.2 Responsibilities	
5.2.1 General obligation	Personnel are responsible for providing, as appropriate, the data provider with sufficient, relevant and up-to-date information about the processing of their data, including the possibilities for data providers making requests related to their data as detailed in paragraph 33 below.
5.2.3 Tools promoting transparency	Appropriate tools, such as information notices, must be applied, informing the data provider about the processing of their data throughout the data lifecycle. Such tools must be regularly reviewed to ensure that the information provided to the data provider remains relevant and up to date.
5.2.5 Exceptions	If information is not provided, the Data Protection Unit must be consulted. The reasons for not providing any information must be fully recorded and regularly reviewed, to confirm that the circumstances supporting the decision to not provide information have not changed.[13]

IV. CLASSIFICATION OF DATA AND LEVELS OF CONFIDENTIALITY

12. Personnel are responsible for classifying data on the basis of content, sensitivity, and risks associated with their inappropriate disclosure.

13. There are four confidentiality levels, each reflecting the sensitivity and related risks that may arise from unauthorized use or disclosure of the data that are processed by personnel.

14. Data must be classified under one of the following four confidentiality levels:

[13] For example, in emergency situations due to security and logistical constraints, it may not be possible to provide information immediately to data providers at the time of collection.

Confidentiality Level	Description and risks exposure	Examples
Public Data	Data that are not sensitive as it has been approved by FAO to be made available to the public at large.[14] Risks: **NONE** The unauthorized access or inappropriate disclosure of the data would not reasonably be expected to cause damage to FAO or to the data provider.	• Published reports, statistics, or press releases.
Internal Data	Data that, due to their preparatory or incomplete nature, or need for internal approval, may not be disclosed outside FAO. Risks: **MEDIUM** The unauthorized access or inappropriate disclosure of the data could reasonably be expected to cause damage to the data provider or to FAO (such as, but not limited to, undermining FAO's independent decision-making processes).	• Internal communications. • Project documents, project narrative and financial reports where there may be a need for the data provider to consent to the release of such information. • Draft technical documents under preparation, still subject to validation and approval for public release.
Confidential Data	Data that are sensitive in nature. Risks: **HIGH** The unauthorized access or inappropriate disclosure of the data would cause harm or damage to the data provider or to FAO. Damage to FAO could consist of damage of a financial, legal, strategic, operational or reputational nature.	• Personal Data • Information on technical assistance to specific countries and donor agreements with Members. • Microdata for which a data provider specifies that it is not to be disclosed. • Lists of attendees at FAO organized training events and other documents which include personal data such as names, email address, job titles, and phone numbers. • Due diligence and risk assessment screening. • Staff selection processes.

[14] Public data may be made freely available to the public in accordance with FAO's Open Access Policy, and other open data provisions related to statistical databases.

Confidentiality Level	Description and risks exposure	Examples
Strictly Confidential Data	Data that are highly sensitive in nature. It may also include data which, because of its content or the circumstances of its creation or communication, becomes and must be classified as sensitive. Risks: **VERY HIGH** The unauthorized access or inappropriate disclosure of the data would place the data provider at risk of serious harm or cause exceptionally grave damage to the data provider or to FAO. Damage to FAO could consist of grave and irreversible damage of a financial, legal, strategic, operational or reputational nature.	• Personal data, which could put data providers at serious risks of harm, including endangering of life. This includes personal data that reveals, amongst others, race or ethnicity, religion, health, genetic or biometric data of an individual. • Documents on investigatory, disciplinary or appeals proceedings. • Documents referred to FAO by Members or third parties under a condition of confidentiality. • Procurement related documents which a vendor indicates contain commercially sensitive information.

15. Data may only be released to any external party or to the public following established authorization or publication procedures.

16. When implementing specific security measures and controls, personnel must assess, on a case-by-case basis, the level of protection that must be afforded to the data they process in light of the nature of the data, and the risks identified for a specific processing operation. Personnel must adopt appropriate security measures that are proportionate and responsive to the level of confidentiality identified.

17. If, prior to transferring data to FAO, a data provider has applied a level of confidentiality to their data, FAO personnel must process that data in accordance with that confidentiality level. If a data provider has not set a confidentiality level, the data is nonetheless classified as confidential unless otherwise agreed between FAO and the data provider.

18. In order to ensure a level of protection proportionate and responsive to the level of confidentiality, personnel must regularly review the level of classification and adjust it if appropriate. If no confidentiality level has been attributed to the data by FAO personnel or by the data provider, the data will be classified as confidential.

19. In case of any doubt or uncertainty regarding the level of confidentiality, personnel should consult their Head of office, the FAO Representative or the Assistant Director-General/Regional Representative, or the Data Protection Unit, as appropriate, for guidance.

V. DUTY OF CONFIDENTIALITY

20. The utmost discretion must be observed in handling data throughout the data lifecycle. Personnel are accountable when processing data, including when transferred to a third party. They are bound by the duty of confidentiality. This duty of confidentiality is established in accordance with Staff Regulation 301.1.5, the Standards of Conduct for the International Civil Service, at paragraph 39, and the Code of Ethical Conduct paragraph 5.12, and applies to all personnel. Non-observance of these provisions by personnel, when dealing with internal, confidential or sensitive information made known to them by reason of their official function may be subject to disciplinary or other administrative action.

21. Personnel must ensure the confidentiality of the data they collect, access or process. Data may only be accessed or transferred for the processing purpose and must not be disclosed to any other person, including to a third party or to other FAO personnel, unless the recipient has been expressly authorized to access or receive the data subject to security measures that are appropriate for the level of confidentiality of the data.

VI. SPECIFIC APPLICATION OF THE DATA PROTECTION FIRST PRINCIPLES

Provision of information to data providers

22. Prior to collection of data, or within a reasonable period from the collection, the data provider must be given, at a minimum, the following information: (*i*) the data that will be processed; (*ii*) the purpose for which the data will be processed; (*iii*) whether the data will be transferred to a third party; (*iv*) how to request access, verification, rectification, deletion, or object to the use of their data; (*iv*) how to lodge a complaint [with the Data Protection Unit] with regard to their data, for example, if they are unsatisfied with the response to their earlier request; and (*v*) the identity and contact of a FAO focal point for data related queries or requests.

23. Where personal data is processed, the information provided to a data provider must be provided in clear and understandable language, and in a format appropriate to the age, literacy and vulnerability of the data provider.

Processing of sensitive data

24. **Adoption of appropriate measures**. Specific measures and safeguards for ensuring the proper use and protection of sensitive data must be put in place, taking into account the processing and operational context and the Data Protection FIRST Principles.

25. **Assessment of necessity**. Before collecting sensitive data, personnel must explore the possibility of achieving the processing purpose without processing sensitive data.

26. **Legitimate Grounds**. Processing of data must be undertaken as part of FAO activities pursuant to its mandate and in line with its legal framework. Additionally, personnel may only process sensitive data based on one of the following legitimate grounds appropriate to the specific circumstances: (*i*) the explicit consent of the data provider; or (*ii*) the protection of the vital interests of a data provider.

27. **Guidance**. When processing sensitive data that is likely to result in high risk to data providers and FAO, guidance from the Data Protection Unit should be sought, as appropriate as regards the appropriate action.

Data transfers

28. **Data received by FAO**. Personnel must ensure the data received is being transferred to FAO on an appropriate legitimate basis, such as consent of the data provider.

29. **Data transferred by FAO to a third party**. Personnel must only transfer data to a third party on the condition that the third party affords a level of protection that is the same or comparable to FAO's own rules and policies, including this Policy.

30. **Assessment of protection afforded by a third party**. Based on the level of confidentiality attributed to the data, personnel must, prior to transfer, assess the level of protection afforded by the third party. This will require an assessment of the third party's technical and organizational security safeguards, the risks and benefits associated with the transfer, and any other elements relevant to the transfer. If it is determined that the third party cannot afford a level of protection that is the same or comparable to measures that would be applied by FAO to the data, in consultation with the Data Protection Unit, appropriate measures to mitigate potential risks must be identified, or the data must not be transferred.

31. **Contractual arrangements**. The transfer of data should take place on the basis of a written contractual arrangement or, as appropriate, by incorporating relevant safeguards in contractual arrangements entered into pursuant to the applicable rules and guidelines in place for each type of arrangement, for example Manual Section 501, 507, 701, and the FAO Strategy for Partnerships with the Private Sector (non-exhaustive list). There may be limited exceptions to the requirement of contractual instruments, but these must be reasonable in the circumstances and the justification therefore, including protective measures taken, must be recorded.

32. **Means of Transfer**. Data must only be transferred by means that ensure its adequate protection. The means of transfer should be determined based on the confidentiality level of the data. In line with Section 1.2.7 above, personnel must, in consultation with the Data Protection Unit, as appropriate, ensure that the third party will destroy or return to FAO all the data transferred once the purpose of the data transfer is achieved.

Requests by data providers

33. **Type of Requests**. A data provider must be able to request access, correction and deletion of their data processed by FAO, or object to the processing of their data by FAO.

a) Access. A data provider may request confirmation of whether their data is being processed and, if that is the case, request access to their data.

b) Correction. A data provider may request the correction or updating of their data.

c) Deletion. A data provider may request the deletion of their data where (i) the data is no longer necessary for the processing purpose, or (ii) the data provider withdraws their consent to the data processing and there is no other legitimate basis for processing.

d) Objection. A data provider may object to, at the time of data collection, the processing of their data. FAO Personnel must inform the data provider of the possible consequences of its objection, as appropriate.[15]

34. **Implementation**. Personnel shall ensure that requests for access, correction, deletion and objection are received, recorded, validated, handled, and responded to in a timely and efficient manner. If legitimate grounds exist for satisfying a request, personnel must take appropriate action to fully or partially accommodate the request received.

[15] For example, if a FAO beneficiary would object to the processing of its data within the context of cash transfers activities, FAO must not process their data. If FAO's assistance can no longer be provided without this data, it will need to inform the beneficiaries correspondingly.

35. **Restrictions**. Following consultation with the Data Protection Unit, the requests of data providers may be rejected or restricted on the basis of (*i*) the security and safety of personnel, third parties or data providers, (*ii*) the rules and related directives on confidentiality and information disclosure, including this Policy, or (*iii*) the request is unclear or unreasonable.

36. **Special provisions**. This Policy does not restrict the rights of the Office of the Inspector General under its Charter to access any data held by the Organization. It also does not create new rights of access to data managed and processed by the Office of the Inspector General, the Ethics Office and the Ombudsman.

Data breaches

37. As soon as they become aware of a data breach, personnel processing the data must immediately consult their Head of office, the FAO Representative or the Assistant Director-General/Regional Representative as appropriate. A determination must be made as to whether the data breach results in risk to the data provider or to FAO. The identified risk shall be evaluated, a summary record of the analysis will be maintained and reported to the Data Protection Unit to advise on mitigatory action.

38. When the data breach results in a risk to the data provider, such breach will be notified to the data provider as well as the measures implemented to mitigate the risk, unless the Data Protection Unit determines that notification would not be necessary or appropriate.

VII. RESPONSIBILITIES AND OVERSIGHT

The Oversight Advisory Committee

39. The Oversight Advisory Committee (OAC), in accordance with its terms of reference, exercises independent oversight in the context of the implementation of the present Policy.

Data Protection Oversight Committee

40. The Data Protection Oversight Committee exercises oversight across the Organization for data protection activities, and monitors the implementation of this Policy. It is accountable to the Director-General, and reports and advises the Director-General on data protection matters.

41. The Data Protection Oversight Committee is comprised of:

a) Chair: A Deputy Director-General appointed by the Director-General.

b) Members: Director of CSI (IT Division), Legal Counsel (Legal Office), [Ethics Officer (Ethics Office), Director of Logistic Services (CSL), Director of Human Resources (CSH), Director of Project Support (PSS)], and two members from decentralized offices appointed by the Director-General.

42. The Data Protection Oversight Committee provides direction across the Organization for data protection activities. It shall:

a) monitor the operationalization and implementation of the Policy and recommend, as appropriate, the development of supplementary instruments;

b) receive reports on implementation and, as appropriate, recommend amendments to the Policy;

c) review this Policy at least every three years, taking into account lessons learned from its implementation and any changes in organizational structures, complementary policies, and any other FAO or UN system developments that would have an impact on its implementation;

d) periodically report to the Director-General, advising on the operation of the Policy and related instruments, and the adequacy of the measures in place;

e) ensure alignment between the present Policy and existing FAO strategies, structures and mechanisms which have data protection implications, including by engaging in regular consultations with relevant internal bodies responsible for overseeing and supporting data related activities and initiatives.

43. The Committee shall meet at least two times a year, either virtually or in person. Upon agreement amongst the members of the Committee, it may take its decisions by correspondence.

44. Matters that are raised in the Data Coordination Group (DCG),[16] chaired by the Chief Economist, or by another internal body, which have data protection implications shall be referred to the Data Protection Oversight Committee for guidance.

Data Protection Unit

45. The Data Protection Unit shall:

a) provide secretariat support to the Data Protection Oversight Committee;

b) monitor compliance with this Policy and regularly report relating to compliance or the implementation of this Policy to the Data Protection Oversight Committee as well as any other data protection issues;

c) manage and evaluate requests by data providers;

d) provide advice to Heads of offices, Assistant Directors-General/Regional Representatives and to personnel on measures to ensure compliance with this Policy, including by providing guidance on the methodology for carrying out a data protection impact assessment, processing sensitive data that is of high risk, evaluate the validity of requests made by data providers, advice on data breaches, and development of data sharing arrangements;

e) receive annual reports from Heads of offices, Assistant Directors-General/Regional Representatives as appropriate, on the implementation of this Policy as concerns their units.

f) report and submit the reports referred to under par. 42 (b), provide information to and, as appropriate, seek guidance from the Data Protection Oversight Committee on the operationalization and implementation of this Policy.

Heads of offices, Assistant Directors-General/Regional Representatives,

46. Heads of offices, ADG/Regional Representatives, have the following responsibilities:

a) overseeing the processing of data under their area of responsibility;

b) acting as a focal point for data protection issues falling within their area of responsibility;

[16] The Data Coordination Group is responsible for endorsing and promulgating internal policies, processes and standards for data produced under FAO's mandate, providing oversight on data-related strategic priorities that will benefit the Organization and its stakeholders, and ensuring that their implementation is coherent with applicable data policies, principles and UN initiatives as well as FAO's overall programmatic priorities. The DCG will be chaired by the Chief Economist. Its members comprise senior FAO executives responsible for data-related policies and programmes.

c) as necessary, seeking the advice of the Data Protection Unit concerning queries with regard to the application and interpretation of this Policy;

d) establishing internal procedures within the unit to ensure that the processing of data is performed in accordance with this Policy;

e) monitoring data processing activities within the unit to ensure compliance with this Policy and identifying possible risks and mitigation measures;

f) assigning specific responsibilities within the unit at an individual level for the handling of data, taking into account the need for proper segregation of duties within the data lifecycle;

g) reporting annually on the implementation of the Policy and related instruments to the Data Protection Unit.

Personnel

47. All personnel are individually responsible for compliance with this Policy and related instruments. This means, *inter alia*, that personnel are required to:

a) determine the purposes and means of the processing of data in accordance with the present Policy;

b) implement appropriate technical and organizational measures, which may include the conclusion of appropriate contractual instruments, to ensure that the processing of data is performed in accordance with this Policy, and regularly review and update those measures where necessary;

c) maintain appropriate records of data processing operations, data sharing agreements, requests and complaints by data providers, data protection impact assessments, data breach notifications, requests by data providers and related matters;

d) inform their supervisors immediately in case of data breaches and cooperate in any investigation of a suspected data breach;

e) seek the advice of the Data Protection Unit concerning the application and interpretation of this Policy.

VIII. REVIEW AND AMENDMENT

48. This Policy will be reviewed by the Data Protection Oversight Committee twelve (12) months after its promulgation and adjusted, as needed. It will thereafter be reviewed, in consultation with FAO Member Nations, at least every two (2) years with a view to ensuring that it remains fit-for-purpose.

49. Amendments to this Policy shall become effective on the date of publication.

IX. EFFECTIVE DATE

50. This Administrative Circular has immediate effect and supersedes Administrative Circular No. 2013/23 Confidentiality Policy and Administrative Circular No. 2021/01 Personal Data Protection Principles, which are withdrawn.

Annex I

Definitions

Anonymized data means information which does not relate to an identified or identifiable natural person, or to personal data that has been rendered anonymous so that the data provider is not identifiable.

Consent means the freely given, specific, informed and unambiguous indication of the agreement by a data provider to the processing of their data, which may be implicit or, as far as sensitive data is concerned, explicit.

Data means any information suitable for processing that originates from FAO or that is disclosed to FAO by a data provider. Under this Policy, data includes non-personal data or personal data, contained in any form.

Data Breach means the accidental or unauthorized loss, destruction, alteration, access, acquisition, or other use for unauthorized purposes, of data, including sensitive data, which compromises the confidentiality, security, availability, or integrity of the data.

Data Lifecycle means all phases during the life of data, from planning, collection, processing, storage, and transfer, to destruction.

Data Provider means a legal person or individual that discloses data to FAO. Under this Policy, legal persons, including FAO Members, UN system organizations, intergovernmental organizations (IGOs), non-governmental organizations (NGOs), and private sector entities, may disclose personal data of an individual to FAO. In such a case, the personal data of such an individual will be afforded the protection provided under this Policy and, to that effect, will be considered a data provider.

Encryption is the process of converting data in order to make it unreadable without special knowledge such as a "key" or a password.

Non-Personal Data means any information of a financial, technical, or operational nature that does not relate to an identified or identifiable individual. Non-personal data includes, for example, financial reports, commercially sensitive data of a vendor, or data containing security sensitive information disclosed by Members.

Personal Data means any information relating to an identified or identifiable individual. For example, names, work and home addresses including email address, date of birth, job titles, etc.

Personnel as used in this Policy refers to staff members and to affiliates engaged by the Organization, including consultants, subscribers to Personal Services Agreements, National Project Personnel, Volunteers, Interns and all other individuals who are providing services to the Organization under a contractual arrangement.

Processing means any operation, or set of operations, automated or not, which is performed on data, including, but not limited to, the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer (whether in computerized, oral or written form), dissemination or otherwise making available of, correction, or destruction.

Pseudonymization means the processing of data so that it can no longer be attributed to a specific data provider without the use of additional information. Such additional information must be kept separately and is subject to technical measures to ensure that personal data cannot be attributed to an individual.

Sensitive Data means data classified by personnel as sensitive based on the likelihood and impact of potential risks that may materialize as a result of their inappropriate disclosure. This includes but is

not limited to personal data revealing racial or ethnic origin, political opinions, religious beliefs, as well as genetic or biometric data and health data of an individual which shall be considered by default as highly sensitive data. It also includes non-personal data that are commercially or economically sensitive in nature, related to national security, or other similarly sensitive information provided by FAO Members or other legal persons.

Third Party means any entity to whom data is transferred, other than FAO and the data provider.

Annex II

Examples on how to apply the Data Protection FIRST Principles

Principle	Example
Fairness	Within the context of a Beneficiary Grants project, FAO intends to use personal data from grant applications to send out survey requests. In line with the Fairness Principle, it would be recommendable to seek first the informed consent of data subjects for their personal data to be used for such a purpose. Following a natural disaster, communications and access to a Member Nation remain severely affected. Since it is not possible to determine what assistance would be required immediately or further down the line, FAO engages in a broad data collection exercise with the purpose of assessing the needs of the people affected. After the emergency has ended, FAO deletes the data that is not necessary to achieve the technical assistance identified. When preparing a funding proposal for a multilateral donor, FAO collects a wide range of data, including data received from project partners. In line with the fairness principle, the country office retains, following classification, the data only for a defined period. When it is not possible to determine how long data is to be retained, the office sets out an initial retention period, which is subject to periodic review. If the data have been shared with a Third Party, reasonable steps are taken to ensure that such Third Parties delete the data.
Integrity	FAO plans to implement a cash transfer project on the basis of beneficiary registration data that was collected 12 months prior to the start of the project. To ensure data accuracy, it must be verified, prior to implementation of the project, if beneficiary locations and household composition have changed during this period. Data accuracy checks should be conducted periodically until the end of the project.
Responsibility	A regional office processes data for various business activities such as project delivery, recruitment, contracting vendors and conducting workshops. To demonstrate compliance with the Policy, the office maintains up to date records for each processing activity, each identifying its purpose, the type of data used, recipient of data (if any), the time limits for keeping the data and the security measures.
Security	As part of the Sustainable Wildlife Management Programme (SWM), FAO has set up a protocol concerning research activities. In line with the principle of security, the protocol provides for the need to assign a unique *SubjectID* to individuals, ensuring data segregation – by only allowing access to data to primary investigators –, and ensuring encryption and protection with password of files that contain personal data.

	In the context of a contract for security alerts, whereby a FAO contractor sends FAO Staff alerts to warn them or keep them informed of situations that may represent a risk on their personal phone, the use of such data for marketing purposes by the contractor or sharing of that data with third parties is explicitly prohibited. In addition, prior to transferring data to the contractor, an assessment is made on the level of protection afforded by the contractor.
Transparency	A FAO country office engages in discussions with the host country with the aim of making the COVID-19 vaccine available to personnel and entitled dependents. In line with the transparency principle, by a specific questionnaire, personnel are informed of – and consent to – the disclosure of relevant personal data to the national healthcare authorities for the purpose of the administration of the COVID-19 vaccine. FAO receives research data from a consortium partner. FAO needs to inform the partner on the data that will be processed, how it will be processed, with whom it will be shared, and the envisaged time limit of processing. When handling a request for access from the partner, personnel shall ensure that it has obtained satisfactory proof of identity from the requestor and that no data relating to third parties is revealed.