SAVING LIVES
CHANGING LIVES

Internal Audit of WFP Cooperating Partners Digital and Data Processing Risks

Office of the Inspector General
Internal Audit Report AR/23/10

August 2023

WFP
World Food Programme

Table of Contents

I. Executive summary

Introduction and context

1. As part of its annual workplan, the Office of Internal Audit audited WFP cooperating partners' digital and data processing risks. The audit focused on the adequacy, efficiency and effectiveness of WFP governance, risk management and internal controls to mitigate cooperating partners' digital and data processing risks. The audit covered the period from 1 January 2021 to 31 March 2022. The Office of Internal Audit gathered evidence and completed the analysis of results on 30 September 2022.

2. WFP routinely relies on its cooperating partners' processes and technology to process and safeguard beneficiaries' personally identifiable information. In 2021, WFP contracted 977 national and international non-governmental organizations in 65 country offices, reaching 105 million people with activities that regularly involved processing beneficiary information.

3. WFP's cooperating partners process a large amount of personally identifiable information, including current and prospective beneficiaries' personal data. Protecting this information is a fundamental duty of care to those WFP serves. Therefore, it is incumbent on WFP to ensure beneficiaries' privacy rights and personal data are safeguarded and processed by its cooperating partners in a manner that does not compromise its confidentiality, availability and integrity. Breaches in privacy could have profound consequences for individual beneficiaries or beneficiary communities and impact WFP's mission objectives.

Audit conclusions and key results

4. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **major improvement needed**. The assessed governance arrangements, risk management and controls were generally established and functioning, but need major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified could negatively affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.

5. The data privacy, security practices and risks noted in this report impair WFP's ability to ensure that cooperating partners consistently carry out programme activities with a reasonable duty of care to safeguard beneficiaries' personal data and right to privacy.

6. It should be noted that the Principles on Personal Data Protection and Privacy were formally adopted by The United Nations High Level Committee on Management at its 36th Meeting on 11 October 2018. The Office of Internal Audit recognizes WFP's adoption of these principles and acknowledges management's reasonable expectations that these will gradually be embedded in the organization's policies and practices.

7. Despite WFP's efforts to improve the legal basis and cooperating partners' safeguards during data processing activities, the Office of Internal Audit observed that cooperating partners' data protection and privacy controls did not align with privacy information management system best practices. In the opinion of the Office of Internal Audit, beneficiary data processed by cooperating partners are at risk of privacy and information security breaches, and current practices only partially meet data subject privacy rights.

8. Many of the cooperating partners sampled lack information security and privacy policies, and few have designated staff with data protection roles. Weak practices were noted in data privacy areas, such as maintaining records of processing activities; processes to respond to data subject rights requests; methods to obtain and document informed consent; data retention policies; information classification; and incident handling procedures.

9. Regarding information security, the Office of Internal Audit observed weaknesses across a range of areas that make beneficiaries' personally identifiable information susceptible to information security breaches and to unauthorized access.

10. The processing of beneficiary data by cooperating partners did not follow coherent and consistent technology or process standards. For example, cooperating partners use a mixture of WFP's corporate solution and various local databases, spreadsheets, and paper records to process beneficiary data. The lack of uniform standards for data processing resulted in weak information security practices and a multiplicity of systems and tools, placing a heavy burden on WFP's capacity to govern the protection of beneficiaries' personal data.

11. Privacy impact assessments, used to detect data protection and privacy risks, were not consistently completed or used to detect and monitor cooperating partners' data processing and digital risks. Therefore, country offices, regional bureaux and headquarters units lacked the visibility needed to optimize cooperating partner risk management, capacity building and allocate monitoring resources. At the time of the audit, the Global Privacy Office was exploring new tools to facilitate the completion and use of privacy impact assessments.

12. WFP's ability to set expectations and enforce cooperating partners' compliance with data privacy conditions in field-level agreements was impaired by the absence of a specific corporate training programme for staff and partners. A digital solutions strategy and privacy information management system standards are needed to align cooperating partners' capabilities and practices to reasonable data privacy and security standards of practice. This report also highlights the importance of establishing a risk management framework, including metrics to monitor and manage cooperating partners' digital risks at all organizational levels beyond privacy impact assessments. Corporate due diligence and capacity and performance assessment tools for cooperating partners must be updated to incorporate data privacy and protection elements. Moreover, compliance reviews of cooperating partners need to include data privacy and protection objectives.

13. The Office of Internal Audit considers training and capacity building of WFP staff and cooperating partners as a vital element to achieving the necessary level of maturity on data protection and privacy; therefore, management should ensure that training and awareness programmes in this area are rolled out expeditiously.

14. The Office of Internal Audit notes the Executive Director's Decision Memorandum of April 2021,[1] reaffirming WFP's commitment to a centralized approach to beneficiary identity management (from here on referred to as 'identity management'), and appointment of the Programme and Policy Development Department to lead a cross-functional steering committee with delegated authority and clear accountability for strategic guidance on identity management.

15. The Office of Internal Audit commends the launch of the Global Privacy Office in May 2021 as a dedicated data privacy and protection advisory function, and the establishment of a governance structure for protecting personal data in October 2022 through the Executive Director's Memorandum OED2022/022,[2] which will set the foundations for further data privacy and protection progress.

Actions agreed

16. The audit report contains two high and three medium-priority observations. In consultation with some technical units, the Global Privacy Office will be the primary lead for implementing the agreed actions. Management has agreed to address the reported observations and work to implement the agreed actions by their respective due dates.

17. The Office of Internal Audit would like to thank managers and staff for their assistance and cooperation during the audit.

[1] Executive Director Decision Memorandum OED/3686 on Issues Requiring ED Guidance Related to Beneficiary Management at WFP.

[2] Executive Director's Memorandum OED2022/022 Establishing the roles of the Global Privacy Office and key governance bodies, including the Data Protection Supervisory Body, Data Protection and Privacy Committee, Data Protection Network and External Advisory Board.

II. Context and scope

Background

WFP policy objectives and commitments related to data protection and privacy

18. In 2016, WFP adopted a guide to personal data protection and privacy and defined personal identity information as any data that directly or indirectly identifies, or can be used to identify, an individual. These guidelines and principles align with the United Nations High-Level Committee on Management[3] framework for processing personal data, which indicates that "United Nations System Organizations should exercise caution when processing any data of vulnerable or marginalized individuals and groups of individuals, including children."

19. The High-Level Committee on Management personal data protection and privacy principles set out a basic framework for the processing of "personal data," which is defined as information relating to an identified or identifiable natural person ("data subject") by or on behalf of, the United Nations system organizations in conducting their mandated activities. These commitments extend to delegating processing activities to third parties, including WFP's cooperating partners (CPs).

20. WFP adopted five principles[4] that aim to safeguard beneficiaries' rights to have their privacy and personal data-related rights adequately protected. These rights include:

(i) lawful and fair processing;

(ii) specified and legitimate purpose, including data retention;

(iii) data quality (which includes data minimization and proportionality);

(iv) accountability; and

(v) data security.

21. Data protection and privacy principles have been adopted by design and default, embedding these in developing digital solutions and programme interventions that process personal data.

WFP cooperating partner data processing activities

22. Data processing activities conducted by CPs include collecting, storing, using, transferring and disposing of beneficiaries' personally identifiable data to fulfil contractual obligations in the execution of WFP programmes. The basis for determining those obligations is found in the field-level agreements signed by CPs with WFP and ancillary operational documents agreed upon with CPs for the execution of WFP-related programme activities. At the time of the audit, the Non-Governmental Organizations Partnerships Unit (NGO Partnership Unit) was piloting an enhanced version of the data protection conditions endorsed by WFP's Global Privacy Office (GPO).

23. The beneficiary data processing activities carried out by CPs vary depending on the programme intervention (e.g. general food distribution, nutrition, resilience, etc.) and delivery mechanisms (e.g. food, cash or vouchers). Data is processed in various ways, manually and automated, using digital and non-digital records and in WFP and non-WFP information systems. The beneficiary data processed is stored in multiple forms and media during programme implementation, including on-site, in cloud systems, and sometimes involves third-party processors.

[3] United Nations High-Level Committee on Management principles adopted in 2018: https://unsceb.org/high-level-committee-management-hlcm

[4] WFP Guide to Personal Data Protection and Privacy: https://docs.wfp.org/api/documents/

24. WFP enters partnerships with various international and national partners, including governments, to deliver programmes in line with its mandate. In 2021, WFP contracted 977 national and international NGOs in 65 country offices to process beneficiaries' personally identifiable information. WFP paid USD 668 million to CPs based on signed distribution agreements and reached 105 million beneficiaries across various programme interventions, including general food distribution, nutrition and resilience.

Roles and responsibilities

25. As a multifaceted objective, the responsibility for setting normative guidance and overseeing the use of digital technologies and data processing by CPs is shared by multiple stakeholders, including the GPO, the Cash Based Transfers Division (CBT Division), the NGO Partnerships Unit, the Legal Office and the Technology Division (TEC). Country offices and regional bureaux are responsible for assessing CPs' capacities and associated digital and data processing risks and monitoring and enforcing that beneficiaries' personally identifiable information is processed with a reasonable duty of care. Country offices that wish to deviate from corporately established identity management solutions for processing beneficiaries' personal data must follow guidance from the CBT Division and TEC.

26. The NGO Partnerships Unit plays a vital role by coordinating updates of the field-level agreement templates used when contracting CPs and ensuring that data protection conditions are incorporated, including annexes developed by subject matter experts. During the audit fieldwork, a new field-level agreement template was piloted in selected countries, with strengthened terms and conditions directly addressing data privacy and protection objectives.

27. TEC sets information technology (IT) standards, providing other units with expert support and advice on IT security, data classification, and other technical areas considered when third parties process data on behalf of WFP.

28. The CBT Division is the business owner of SCOPE[5] and is tasked with developing guidance on which systems to use to support identity management for cash, value voucher, in-kind, and commodity voucher operations. The CBT Division is tasked to develop guidance on identity management, including how much information to collect, how to process and protect the information of the people WFP assist, and to promote a consistent level of maturity globally for doing identity management[6].

29. Established in 2021, the GPO is responsible for setting WFP's overarching normative guidance on data privacy and protection. The GPO acts in an advisory role to other WFP functions and does not dictate operational procedures or monitor the execution of the effective implementation of policies or compliance with the data protection and privacy requirements in field-level agreements. These responsibilities are dispersed, without clear designation, between country offices, regional bureaux, and headquarters units.

30. It is important to note that WFP only recently formalized the governance structure for the protection of personal data through Executive Director's Memorandum OED2022/022, which established the roles of the GPO and key governance bodies, including the Data Protection Supervisory Body, the Data Protection and Privacy Committee, the Data Protection Network and the External Advisory Board. The final governance structures, reporting lines, and constituent members of these governance bodies were yet to be determined at the time of writing this report.

31. The Executive Director's Decision Memorandum of April 2021 reaffirms WFP's commitment to a centralized approach to identity management. The Memorandum appoints the Programme and Policy Development Department to lead a cross-functional steering committee with delegated authority and clear accountability for strategic guidance on identity management, including coordinating operational and policy decisions for digital assistance and setting principles and standards that country offices can follow.

[5] SCOPE is WFP's beneficiary information and transfers management platform.

[6] CBT Division Key Messages "What is Identity Management", March 2023.

International standards and frameworks on data protection and privacy

32. International standards and regulatory requirements that frame data protection and privacy vary across jurisdictions and do not bind WFP's activities and practices. The Office of Internal Audit considered these standards to assess whether WFP policies and practices align with internationally recognized best practices. The following standards set by the International Organization for Standardization (ISO) were used as the basis for the assessment:

(i) ISO/IEC 27701 is the international standard that serves as an extension to ISO 27001/ ISO 27002 on information security management systems. It provides guidelines for implementing, maintaining and continually improving privacy information management systems;

(ii) ISO/IEC 27001 is the international standard that details the requirements of an information security management system; and

(iii) ISO/IEC 27002 is the international standard that supports the implementation of information security management systems based on the requirements of ISO 27001.

33. These ISO standards are interpreted and used to determine reasonably expected data processing control objectives and to benchmark and assess CPs' policies, processes, systems, capabilities and tools when processing beneficiaries' personally identifiable information.

34. The Office of Internal Audit recognizes that WFP and its CPs do not strictly adhere to these ISO standards, nor is the organization or its CPs seeking to be certified. Therefore, these standards were used in the audit work as a reference point to objectively and rigorously assess data processing activities.

Objective and scope of the audit

35. The objective of the audit was to provide assurance on the adequacy, efficiency and effectiveness of WFP governance, risk management and the internal controls in place to mitigate CPs' digital and data processing risks. Such audits contribute to the Office of Internal Audit's annual and overall assurance statement to the Executive Director on governance, risk management and internal control processes. The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

36. The audit focused on information security, data protection, privacy, and accountability risks. It used ISO standards (see paragraph 32) to assess whether WFP policies and practices align with internationally recognized best practices.

37. The following five areas were included in the scope of the audit:

- Area 1: Governance and risk management
- Area 2: Programme management
- Area 3: Cooperating partners' management life cycle[7]
- Area 4: Cooperating partner management of beneficiary data life cycle[8]
- Area 5: Training and capacity building.

38. The audit scope covered the period from 1 January 2021 to 31 March 2022. Where necessary, transactions and events pertaining to other periods were reviewed. The audit fieldwork was conducted from 23 May to 30 September 2022.

[7] The CP management life cycle includes the following sub-process: selection process, due diligence, contracting and field-level agreements, monitoring and termination.

[8] The CP data management life cycle includes the following sub-processes: collection, storage, use, transfer and disposal.

39. The Office of Internal Audit conducted structured interviews with relevant stakeholders at global headquarters; sampled four regional bureaux; conducted survey meetings with the corporate data protection offices of two international NGOs to gather information; and carried out documentation reviews to evaluate the design and operational effectiveness of WFP information security, data protection, and privacy guidelines and policies. Nine[9] country offices were sampled (five through in-country field visits and four through remote reviews) as well as 16 CPs.

III. Results of the audit

Overview of conclusions

40. Table 1 outlines the extent to which audit work resulted in observations and agreed actions. These are classified according to the areas of coverage established for the audit (see paragraph 37) and are rated as medium or high priority; any observations that resulted in low-priority actions are not included in this report.

Table 1: Overview of areas, observations and priority of agreed actions	**Priority of issues/agreed actions**
Area 1: Governance and risk management	
Observation 1: Policies, accountabilities for data protection and use of digital tools	*High*
Area 2: Programme management	
Observation 2: Privacy impact assessments	*Medium*
Area 3: Cooperating partnership management life cycle	
Observation 3: Engagement and monitoring of cooperating partners	*Medium*
Area 4: Cooperating partner management of beneficiary data life cycle	
Observation 4: Information security and privacy controls by cooperating partners	*High*
Area 5: Training and capacity building	
Observation 5: Training and capacity building	*Medium*

41. The review of CP data processing activities linked to WFP programme activities will inform the actions WFP must take to strengthen its governance and risk management of CPs' privacy management information systems.

42. An overview of the actions to be tracked by the Office of Internal Audit for implementation and their due dates can be found in Annex A.

[9] Sampled country offices: Ecuador, Malawi, Myanmar, Nigeria, Pakistan, South Sudan, Sudan, Uganda and Yemen.

Area 1: Governance and risk management

43. In line with international data protection standards such as ISO 27701:2019 and with UN Personal Data Protection and Privacy Principles adopted by the United Nations High-Level Committee on Management, WFP has progressively introduced data protection and privacy policies and guidelines, including the WFP Master Data Governance Framework (May 2014), the WFP Corporate Information and IT Security Policy (May 2015), the WFP Guide to Personal Data Protection and Privacy (July 2016), the Protection and Accountability Policy (November 2020), the Cash Assurance Framework: Technical Note (October 2021), and the WFP Cash Assurance Framework (February 2022).

44. WFP established the GPO in May 2021 to strengthen WFP's technical know-how in data privacy. In October 2022, the governance structure for the protection of personal data was formalized by Executive Director's Memorandum OED2022/022 establishing the roles of the GPO and key governance bodies, including the Data Protection Supervisory Body, Data Protection and Privacy Committee, Data Protection Network and the External Advisory Board.

45. WFP's contractual relationship with CPs for assistance programmes is formalized through field-level agreements. These agreements include data protection conditions that govern the processing of beneficiary data needed to implement programme activities.

46. At the time of the issuance of this report, the NGO Partnerships Unit was rolling-out a revised version (2022.V02) of the data protection conditions included in field-level agreements in selected country offices.

Observation 1. Policies, accountabilities for data protection and use of digital tools

Accountabilities for data protection

47. While responsibilities for implementing the field-level agreements with CPs lie with country office functional units, the Office of Internal Audit noted that country offices need guidance and clear accountabilities to effectively implement and enforce the data protection conditions in the agreements.

48. The review of the data protection and privacy controls implemented by the sampled CPs revealed significant gaps in data standards when compared to best practices for data privacy and the data protection requirements included in the field-level agreements. These gaps are described in observation 4.

49. The NGO Partnerships Unit is responsible for issuing and administering corporate support to country offices for field-level agreement templates. Although monitoring CP compliance with these obligations is an inherent task for country offices, it remains unclear which second-line actors should be monitoring the effective fulfilment of these obligations.

50. Executive Director Decision Memorandum 2981 signed 6 July 2020 identifies the Programme Humanitarian and Development Division as the master data owner of beneficiary information, with the CBT Division being responsible for identity management. Despite this, the designation as data owner of beneficiary data has yet to lead to specific accountabilities for monitoring the implementation of data protection conditions at the CP level.

Governance of cooperating partner digital technologies for processing beneficiary data

51. The CBT Division is responsible for developing guidance on identity access management, including how much information to collect, how to process and protect the information of the people WFP assists, and to promote a consistent level of maturity globally. The Framework articulates the standards and principles of identity management specific to cash and voucher operations. At the time of the issuance of this report, the CBT Division was in the process of expanding the framework beyond cash and voucher operations.

52. The CBT Division is also tasked with developing guidance on which systems to use to support identity access management for all assistance modalities, including a menu of corporately endorsed systems that meet WFP technology and programme standards. Country offices are expected to contact the CBT Division and TEC when deviating from approved digital solutions, including for systems that process beneficiaries' personally identifiable information.

53. Processing of beneficiary data at the CP level is performed without following specific technology or process standards. Some CPs use WFP's corporate solution, SCOPE, for identity management, while others rely on their solutions or spreadsheets and, in some cases, use re-purposed WFP monitoring systems. In a few instances, beneficiary data was processed relying mainly on paper documentation.

54. This lack of CP-directed standards resulted in widespread weak information security practices, including sharing unencrypted beneficiary data via email and unsecure storage of beneficiary data on personal devices and the cloud. The absence of standards and multiplicity of CP systems and tools places a heavy burden on WFP's capacity to govern the protection of personal data.

55. In some cases, CPs adapted the tools used to conduct surveys for beneficiary data processing. These processes and systems had not been assessed to determine their adequacy in relation to privacy and information security.

Underlying causes: Undefined responsibility for enforcing data protection conditions in field-level agreements; need to update applicable policies and guidelines for data protection; a centralised approach and standards for identity management that is in development but not yet available.

Agreed Actions [High priority]

The Global Privacy Office, together with the Programme and Policy Development Department, will develop policies and guidelines for the implementation and enforcement of data privacy and protection conditions of field-level agreements with cooperating partners.

Timeline for implementation

30 June 2024

Area 2: Programme management

56. Privacy impact assessments are described in WFP's Guide to Personal Data Protection and Privacy[10] as a project-based management tool in which risks to privacy are identified and assessed. These assessments should be carried out during programme design to help guide decisions regarding risk avoidance and mitigation strategies. The Office of Internal Audit reviewed the privacy impact assessments that the sampled country offices had conducted; the tools used to carry out these assessments; follow-up on the assessments' risk mitigating recommendations and associated accountability mechanisms.

Observation 2. Privacy impact assessments

57. Only four of the nine country offices sampled had carried out privacy impact assessments, identifying relevant data privacy and protection risks and recommending mitigation actions extending to CPs' data processing activities in programme implementation.

58. From the sample of 16 CPs, only 26 percent (mainly international NGOs) had performed privacy impact assessments on WFP-related programmes. The results of these assessments were not shared with WFP, highlighting missed opportunities for WFP to avoid potential duplication of efforts in risk-assessing data privacy and protection practices.

59. Gaps in the completion and use of privacy impact assessments included:

- **Inconsistencies**: Privacy impact assessment exercises were not standardized, were inconsistent and non-comparable, limiting their utility in managing risks. The information from these assessments stayed at the country level, restricting the ability of regional bureaux and headquarters to monitor and follow up on country office and CP data privacy risk management actions.
- **Privacy impact assessment drivers:** The decision to conduct a privacy impact assessment was driven by resource availability (budgets and skilled staff) and did not always consider the complexity of data processing activities. There was no systematic process or ownership to enforce the completion of the assessments.
- **Risk management:** The risk and mitigation recommendations identified in privacy impact assessments were not integrated and monitored in country office risk management practices (i.e. country office or partnership units' risk registers). Implementation of the risk mitigation recommendations identified in privacy impact assessments was not followed up at country, regional, or headquarters levels.

60. The Office of Internal Audit acknowledges that at the time of finalizing this report, the GPO is in the process of launching technology tools to streamline privacy impact assessment exercises and improve the visibility and management of privacy risk.

Underlying causes: Lack of updated guidelines for country offices in conducting privacy impact assessments; limited capacity at the country office level to conduct and follow up on the implementation of privacy impact assessment recommendations; lack of integration of the privacy impact assessment exercise with corporate risk management frameworks; and absence of standardized framework agreements for partnerships with government partners.

[10] Published in June 2016.

Agreed Actions [Medium priority]

The Global Privacy Office will:

(i) Provide updated standardized privacy impact assessment tools and guidelines to country offices, including technology platforms to gather assessment information and track recommended actions.

(ii) In consultation with the Risk Management Division and Technology Division, provide strategic guidance for establishing a risk management framework, tools, and metrics to effectively monitor and manage cooperating partners' privacy and digital risks by units at headquarters, regional and country levels.

Timeline for implementation

31 March 2024

Area 3: Cooperating partnership management life cycle

61. The Office of Internal Audit interviewed functional heads from selected headquarters divisions, regional bureaux, and country offices to assess the processes, tools, and procedures for due diligence, performance assessment, and monitoring of contracted CPs, focusing on data processing activities. The Office of Internal Audit reviewed CPs' implementation of the data privacy and protection clauses in field-level agreements, training, and capacity building.

62. At the time of the issuance of this report, the NGO Partnerships Unit was rolling out a revised version of the field-level agreement, including new data protection conditions to clarify CP obligations. This revised version was developed by the GPO and TEC's Information Security Branch.

Observation 3. Engagement and monitoring of cooperating partners

Corporate due diligence, capacity, and performance assessment tools

63. None of the due diligence reports, capacity assessments, and performance management tools in the country offices examined referred to CPs' data protection and privacy capabilities.

64. There was no regular monitoring or checks to ensure CPs complied with the data privacy and protection standards and conditions in field-level agreements. In addition, the risk and compliance and programme functions did not have data privacy and protection risk indicators or minimum monitoring requirements to assess CPs' digital and data processing risks. These are needed to raise management's awareness of instances of CPs' non-compliance with agreed-upon data privacy contractual obligations.

Monitoring of data protection conditions in field-level agreements

65. Three of the nine country offices sampled introduced updated data protection conditions through new field-level agreements during the first quarter of 2022. However, this was not accompanied by an assessment of the CPs' data protection practices or actions governing their implementation. Interviews with country office partnership teams show low awareness of the new field-level agreement data privacy conditions and minimal awareness of how these should be evaluated and monitored.

Plan of operations

66. The country office "plan of operations" annex to field-level agreements sets specific activity-level focus, objectives, and output expectations for CPs. The Office of Internal Audit found no reference to data privacy and protection considerations in these plans, including references to beneficiary data flow, roles and responsibilities, and descriptions of the minimum standards needed to safeguard beneficiaries' personally identifiable information. The plans did not leverage existing corporate tools to map CPs' processing activities.

Underlying causes: Evolution of data privacy policies and tools; slow build-up of corporate data privacy and protection capabilities; and staff and CPs' limited awareness of protection and privacy conditions.

Agreed Actions [Medium priority]

1. The Global Privacy Office, in consultation with and Technology Division, will provide support and advice to the Programme and Policy Development Department on the data protection and privacy capabilities to be considered during due diligence and performance assessments of cooperating partners.
2. The Global Privacy Office, in consultation with the Risk Management Division and the Programme and Policy Development Department, will expand the scope of current cooperating partner management and compliance reviews to include data privacy and protection objectives.

Timeline for implementation

31 March 2024

Area 4: Cooperating partner management of beneficiary data life cycle

67. In reviewing CPs' processing activities related to beneficiaries' personally identifiable information, the Office of Internal Audit tested the presence, design, and operating effectiveness of key internal control objectives for privacy information management systems, referencing internationally accepted standards. These tests spanned the entire beneficiary data life cycle, including collection, storage, use, transfer, and disposal of beneficiaries' personally identifiable information.

Observation 4. Information security and privacy controls by cooperating partners

68. In testing CP data processing activities, the Office of Internal Audit observed significant deviations from best practice standards for privacy information systems, information security, and required obligations under field-level agreements. While all the CPs tested presented internal control weaknesses, international NGOs were better positioned to meet WFP's expectations and align with data privacy principles and objectives.

Policies, roles, and responsibilities

69. Forty percent of the 16 CPs tested did not have information security and privacy policies. Further, 80 percent of the CPs tested did not have information security and privacy roles, such as designated data protection personnel. Over 40 percent of CPs had yet to undertake data privacy and awareness campaigns or education.

Data privacy

70. Work by the Office of Internal Audit detected several weak practices in data privacy, including:

- With one exception, **records of processing activities** were not maintained by the CPs tested. These records gather information about data processing, including the processing activities performed; a description of categories of data subjects and personally identifiable information processed; and a general description of the technical and organizational security measures. Maintaining records of processing activities is a requirement of a privacy framework and a foundational element of a privacy programme.
- **Data subject rights** had been defined by 2 of the 16 CPs audited. Most CPs had not established procedures or implemented mechanisms to handle requests from individuals wishing to exercise their privacy rights, including access, correction, deletion, or any other rights regarding the personal data held in the CP's custody.
- **Informed consent** – approximately 55 percent of the audited CPs did not have a comprehensive procedure to clearly and transparently inform subjects about the processing of their data, and none maintained evidence that this action had been carried out.
- **Data retention** policies and practices were not established in over 50 percent of the CPs audited, including documented procedures to delete beneficiary data from IT systems or destroy documentation as soon as the personally identifiable information was no longer necessary for the identified purpose. Further, 80 percent of the CPs tested still needed to establish an **information classification scheme**.
- **Data breach** policies and procedures were absent in half of the CPs tested, including strategies to handle and notify data subjects of incidents that may affect their personally identifiable information. Several CPs reported cases of lost or stolen equipment during the audit period. These were treated as IT asset losses and security incidents without considering the potential impact on beneficiaries' data privacy. Incidents were not reported to WFP and were handled through national authorities.

Information security

71. While testing CP data processing activities, the Office of Internal Audit noted numerous information security weaknesses that put beneficiaries' personally identifiable information at risk and raised technology risks that could impair the continuous delivery of assistance to beneficiaries. These include:

- **IT asset management:** Inventory or documentation regarding IT assets and cloud services hosting beneficiaries' personally identifiable information were not maintained in 90 percent of cases. Over 50 percent of the CPs did not have procedures to dispose of or re-assign personal computers and electronic devices, ensuring that personally identifiable information was removed or securely overwritten.
- **Data encryption and transfer:** Encryption technologies to protect beneficiaries' personally identifiable information data was not used in 66 percent of cases. Beneficiary data was mainly transferred without a secure file transfer mechanism or encryption.
- **Network and device security:** Tools to protect the CPs' network and end-user devices, such as anti-virus tools, were absent in 40 percent of cases.
- **User access controls:** A documented user access control policy serving as the basis for controlled access to beneficiaries' personally identifiable information was absent in over 50 percent of cases. Mobile devices capturing and storing beneficiaries' personally identifiable information were often not considered within user access or security policies.
- **Network management:** Network management was not documented in 56 percent of cases, and many CPs operated without a designated network manager.
- **Physical security:** Physical security in CPs' premises, and access to devices and records containing beneficiaries' personally identifiable information, was deficient in 40 percent of cases.
- **Business continuity management:** Most (82 percent) of the CPs examined did not have documented business continuity or disaster recovery plans. Upon further enquiry, the Office of Internal Audit observed that 67 percent of these CPs did not regularly back up data following a formal backup policy. Only a few had tested the backups to corroborate that the data could be retrieved.

72. The data privacy and security risks in this report significantly impair WFP's ability to ensure that its CPs carry out programme activities with the duty of care needed to reasonably safeguard beneficiaries' right to privacy.

Underlying causes: No minimum standards in place for CP privacy and information security practices; CP underinvestment and lack of skills at the CP level; and lack of enforcement by WFP of existing data protection of personal data clauses.

Agreed Actions [High priority]

The Programme and Policy Development Department, in consultation with the Global Privacy Office, Technology Division, the Identity Management Steering Committee, and the Data Protection and Privacy Committee as appropriate, will define roles and responsibilities for addressing the data privacy and information security gaps noted in this report.

Timeline for implementation

30 June 2024

Area 5: Training and capacity building

73. WFP implements a variety of programme activities that process beneficiaries' personally identifiable information. WFP works with various national and international NGOs with different degrees of capacity to understand and establish privacy information management systems. Therefore, it is incumbent on WFP to understand the capabilities of each CP to fulfil their contractual obligations regarding data privacy and establish support mechanisms and tools to close any capacity gaps that a CP may have related to data privacy and protection.

74. The Office of Internal Audit reviewed existing corporate processes, tools, and procedures for evaluating CPs' capacity related to data privacy and protection and the training and capacity-building strategies and activities provided to CPs by country office partnership teams.

Observation 5. Training and capacity building

75. While robust, WFP's CP induction programmes focus on programme data requirements and the technical aspects of using WFP tools to collect beneficiary data, with little consideration of data protection. These programmes did not raise awareness of data protection and privacy principles, standards, and the controls expected across the beneficiary data life cycle as stipulated in field-level agreements. Information security expectations of CPs' were also not raised in the training and induction programmes examined during the audit, nor were practical guidelines delivered for CPs to follow.

76. The absence of a specific corporate training programme on data protection and privacy, coupled with the limited resources at headquarters and regional bureaux to support country offices, hinders the capacity and capability of WFP staff to set expectations and enforce CPs' compliance with the data privacy conditions introduced in field-level agreements.

77. Beyond WFP-mandated training, the Office of Internal Audit noted that some international NGOs have mandatory training designed to raise their staff's awareness of information security, and digital tools are used to track staff participation. These types of training and awareness-raising exercises were not prevalent in local CPs.

Underlying causes: Unclear roles, responsibilities, and accountabilities for training and capacity building of WFP and CP staff; current data protection and privacy training included in CP induction programme not comprehensive; and lack of data protection and privacy training tools accessible to WFP and CP staff.

Agreed Actions [Medium priority]

The Programme and Policy Development Department, in consultation with the Global Privacy Office, the Identity Management Steering Committee and the Data Protection and Privacy Committee will:

(i) Assign roles, responsibilities, and accountabilities for the capacity building and training of cooperating partners on data protection and privacy.

(ii) Roll out updated capacity-building and awareness-raising programs to cooperating partners on personal data protection and information security.

Timeline for implementation

30 June 2024

Annex A – Agreed action plan

The following table shows the categorization, ownership, and due date agreed with the auditee for all the audit observations raised during the audit. This data is used for the macro analysis of audit findings and monitoring the implementation of agreed actions.

#	Observation title	Process Area	Owner	Priority	Timeline for implementation
1	Policies, accountabilities for data protection and use of digital tools	Area 1: Governance and risk management	GPO	**High**	30 June 2024
2	Privacy impact assessments	Area 2: Programme management	GPO	**Medium**	31 March 2024
3	Engagement and monitoring of cooperating partners	Area 3: Cooperating partners management life cycle	GPO	**Medium**	31 March 2024
4	Information security and privacy controls by cooperating partners	Area 4: Cooperating partner management of beneficiary data life cycle	PD	**High**	30 June 2024
5	Training and capacity building	Area 5: Training and capacity building	PD	**Medium**	30 June 2024

Annex B – Definitions of audit terms: ratings & priority

1 Rating system

The internal audit services of UNDP, UNFPA, UNOPS and WFP adopted harmonized audit rating definitions, as described below:

Table B.1: Rating system

Rating	Definition
Effective / satisfactory	The assessed governance arrangements, risk management and controls were adequately established and functioning well, to provide reasonable assurance that issues identified by the audit were unlikely to affect the achievement of the objectives of the audited entity/area.
Some improvement needed	The assessed governance arrangements, risk management and controls were generally established and functioning well but needed improvement to provide reasonable assurance that the objective of the audited entity/area should be achieved. Issue(s) identified by the audit were unlikely to significantly affect the achievement of the objectives of the audited entity/area. Management action is recommended to ensure that identified risks are adequately mitigated.
Major improvement needed	The assessed governance arrangements, risk management and controls were generally established and functioning, but need major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could negatively affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.
Ineffective / unsatisfactory	The assessed governance arrangements, risk management and controls were not adequately established and not functioning well to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area. Urgent management action is required to ensure that the identified risks are adequately mitigated.

2 Priority of agreed actions

Audit observations are categorized according to the priority of agreed actions, which serve as a guide to management in addressing the issues in a timely manner. The following categories of priorities are used:

Table B.2: Priority of agreed actions

High	Prompt action is required to ensure that WFP is not exposed to high/pervasive risks; failure to take action could result in critical or major consequences for the organization or for the audited entity.
Medium	Action is required to ensure that WFP is not exposed to significant risks; failure to take action could result in adverse consequences for the audited entity.
Low	Action is recommended and should result in more effective governance arrangements, risk management or controls, including better value for money.

Low priority recommendations, if any, are dealt with by the audit team directly with management. Therefore, low priority actions are not included in this report.

Typically audit observations can be viewed on two levels: (1) observations that are specific to an office, unit or division; and (2) observations that may relate to a broader policy, process or corporate decision and may have a broad impact.[11]

[11] An audit observation of high risk to the audited entity may be of low risk to WFP as a whole; conversely, an observation of critical importance to WFP may have a low impact on a specific entity, but have a high impact globally.

3 Monitoring the implementation of agreed actions

The Office of Internal Audit tracks all medium and high-risk observations. Implementation of agreed actions is verified through the Office of Internal Audit's system for the monitoring of the implementation of agreed actions. The purpose of this monitoring system is to ensure management actions are effectively implemented within the agreed timeframe to manage and mitigate the associated risks identified, thereby contributing to the improvement of WFP's operations.

Office of Internal Audit monitors agreed on actions from the date of the issuance of the report with regular reporting to senior management, the Independent Oversight Advisory Committee, and the Executive Board. Should action not be initiated within a reasonable timeframe, and in line with the due date as indicated by Management, the Office of Internal Audit will issue a memorandum to management informing them of the unmitigated risk due to the absence of management action after review. The overdue management action will then be closed in the audit database and such closure confirmed to the entity in charge of the oversight.

When using this option, the Office of Internal Audit continues to ensure that the office in charge of the supervision of the unit who owns the actions is informed. Transparency on accepting the risk is essential, and the Risk Management Division is copied on such communication, with the right to comment and escalate should they consider the risk accepted is outside acceptable corporate levels. Office of Internal Audit informs senior management, the Audit Committee and the Executive Board of actions closed without mitigating the risk on a regular basis.

Annex C – Acronyms

CP	Cooperating Partner
CBT	Cash Based Transfers
GPO	Global Privacy Office
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
NGO	Non-Governmental Organization
PRO	Programme Humanitarian and Development Division
SCOPE	WFP's beneficiary information and transfers management platform
TEC	Technology Division
UNDP	United Nations Development Programme
UNFPA	United Nations Population Fund
UNOPS	United Nations Office for Project Services
USD	United States Dollar
WFP	World Food Programme