International Organization for Migration (IOM)
The UN Migration Agency

EXECUTIVE SUMMARY

INTERNAL AUDIT REPORT

Migrants Personal Data Protection and Security

3P201907

September - March 2020

Issued by the Office of the Inspector General

Report on the Audit of Migrants Personal Data Protection and Security
Executive Summary
Audit File No. 3P201907

The IOM Office of the Inspector General (OIG) conducted an internal audit of the process for Migrants Personal Data Protection and Security from 18 September to 2 October 2019 at IOM Headquarters and field visits in the following country offices: 30 November to 12 December 2019 in South Sudan, 20 to 31 January 2020 in Tanzania, and 9 to 12 March 2020 in Greece.

The internal audit aimed to assess the adequacy and effectiveness of IOM's policies, procedures, systems, and internal controls around migrants' personal data protection and security, as well as its relevance with external requirements/expectations; and to ascertain IOM's compliance and controls' effectiveness for the data protection policies on processing and securing migrants' personal data. Selected samples from the following areas were reviewed:

a. Data Protection Framework
b. Risk Management
c. Oversight and Monitoring
d. Training
e. Compliance

Because of the concept of selective testing of data and inherent limitation of the internal audit work, there is no guarantee that all matters of significance to IOM will be discovered by the internal audit. It is the responsibility of the management of the units involved to establish and implement internal control systems to assure the achievement of IOM's objectives in operational effectiveness and efficiency, reliable financial reporting and compliance with relevant laws, regulations and policies. It is also the responsibility of the management of the units involved to determine whether the areas the internal audit covered, and the extent of verification or other checking included are adequate for their respective purposes. Had additional procedures been performed, other matters might have come to internal audit attention that would have been reported.

The internal audit was conducted in accordance with the Charter of the Office of the Inspector General and in general conformance with the *International Standards for the Professional Practice of Internal Auditing.*

Overall audit rating

OIG assessed the process for Migrants Personal Data Protection and Security as **partially effective**, which means that *"while the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. Or, some of the controls do not seem correctly designed in that they do not treat root causes, and those that are correctly designed are operating effectively."*

The rating was based on weaknesses noted in the following areas:

1. Data Protection framework
2. Data Protection principles
3. General Data Protection Regulations
4. Risk management
5. Monitoring and enforcement
6. Training on data protection

7. Data Sharing with third parties
8. Policy on retention and destruction of personal data
9. Processing of migrants' personal data

Key recommendations: Total = 12; High Priority = 9; Medium Priority = 3

Recommendations made during the internal audit fieldwork and in the report aim to equip the departmental managers and staff to review, evaluate and improve their own internal control and risk management systems over Migrants Personal Data Protection and Security.

High Priority Recommendations

For the high priority recommendations, prompt action is required to ensure that IOM will not be adversely affected in its ability to achieve its strategic and operational objectives.

There are 9 high priority recommendations, consisting of: 3 recommendations each in Data Protection Framework, and Compliance, and 1 recommendation each in Risk Management, Oversight and Monitoring, and Training.

- Refine the existing data governance framework to ensure the effective implementation of the data protection and privacy programme targeting migrants' personal data.
- Prioritize the review of Data Protection Principles to ensure that data protection policies and procedures are updated, disseminated, and well understood.
- The Institutional Law and Programme Support Division along with other United Nations System Organizations should continue the high-level consultations with European Commission to alleviate the challenges and difficulties in dealing with third parties that are obliged to comply with General Data Protection Regulation.
- Establish a data privacy management framework.
- Monitoring and oversight functions should be formally established with clear assignment of roles and responsibilities in the update of IOM Data Protection Principles.
- Devise a training plan and identify training focal points that could assist in the delivery of a face-to-face training on data protection.
- Establish clear policies, mandatory minimum procedures, appropriate controls, and risk mitigating measures encompassing all types of data sharing arrangements.
- Establish a comprehensive, clear, and harmonized policies and procedures on retention and destruction of records containing migrants' personal data.
- IOM's Data Protection Policies and other relevant security policies should specify clear instructions on mandatory minimum-security measures in handling different types of migrants' personal data.
- IOM systems that are considered high risk should undergo a comprehensive and specific data privacy assessment.

There remains 3 Medium priority recommendations consisting of: 2 recommendations in Compliance, and 1 recommendation in Oversight and Monitoring, which need to be addressed by the units involved within one year to ensure that such weaknesses in controls will not moderately affect the Country Office's ability to achieve its entity or process objectives.

There was no Low priority recommendation.

Management comments and action plans

All 12 recommendations were accepted. Management of the units involved is in the process of implementation. Comments and/or additional information provided have been incorporated in the report, where appropriate.

This report is intended solely for information and should not be used for any other purpose.

International Organization for Migration
Office of the Inspector General

I. About the Migrants Personal Data Protection and Security

The management for Migrants Personal Data Protection and Security is under the oversight of Institutional Law and Programme Support Division - Office of Legal Affairs. The audit covered the review of transactions from January 2018 to June 2019.

II. Scope of the Audit

1. Objective of the Audit

The internal audit was conducted in accordance with the Charter of the Office of the Inspector General and in general conformance with the *International Standards for the Professional Practice of Internal Auditing.* The focus of the audit was the adequacy and effectiveness of IOM's policies, procedures, systems, and internal controls around migrants' personal data protection and security, as well as its relevance with external requirements/expectations; and to ascertain IOM's compliance and controls' effectiveness for the data protection policies on processing and securing migrants' personal data.

2. Scope and Methodology

In compliance with Internal Audit standards, the audit assessed the adequacy and effectiveness of IOM's policies, procedures, systems, and internal controls around migrants' personal data protection and security, as well as its relevance with external requirements/expectations; and to ascertain IOM's compliance and controls' effectiveness for the data protection policies on processing and securing migrants' personal data.

The audit was intended to cover policy, practice, and the information technology components of the migrant personal data protection in IOM. However, due to IA's limitation of scope, observations and recommendations related to information technology applications were based on the general understanding demonstrated by IOM staff in the sampled country offices and other units during the fieldwork. Technical related information technology security measures relevant to safeguarding migrants' personal data were also not assessed from an expert's point of view.

Recommendations for improvements that were made during the internal audit fieldwork and in this report aim to equip the relevant departments and staff to review, evaluate and improve their own processes, internal control, and risk management systems.

III. Audit Conclusions

1. Overall Audit Rating

OIG assessed the management for Migrants Personal Data Protection and Security as **partially effective**, which means that *"while the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. Or,*

some of the controls do not seem correctly designed in that they do not treat root causes, and those that are correctly designed are operating effectively."

IV. Key Findings and High Priority Recommendations

1. Data Protection Framework
   There is no data protection framework available. In addition, there are no resources that support the central governing body and clear roles and responsibilities within the different levels of IOM operations. In addition, there is limited resources that handle data protection matters.

   High Priority Recommendation:

   - Refine the existing Data governance framework to ensure the effective implementation of the data protection and privacy programme targeting migrants' personal data.

2. Data Protection Principles
   IOM Data Protection Principles are outdated and needs to be more aligned with international data protection regulations and adapt to the continuous modernization in information and communication technology.

   High Priority Recommendation:

   - Prioritize the review of Data Protection Principles to ensure that data protection policies and procedures are updated, disseminated, and well understood.

3. General Data Protection Regulations
   According to the European Commission, General Data Protection Regulations does not apply to the UN System Organizations. Difficulties were encountered in dealing with third parties including donors, as they are not fully aware of the exemption resulting to extended negotiations and nearly loss of funding.

   High Priority Recommendation:

   - The Institutional Law and Programme Support Division along with other United Nations System Organizations should continue the high-level consultations with European Commission to alleviate the challenges and difficulties in dealing with third parties that are obliged to comply with General Data Protection Regulations.

4. Risk Management
   The wide range of migrants' personal data handled makes IOM susceptible to privacy risk, which if not mitigated will negatively impact the organization's reputation and might negatively impact on the safety and security of migrants.

   High Priority Recommendation:

   - Establish a data privacy management framework.

5. Monitoring and Enforcement
   Compliance and Internal Remedies is one of the IOM Data Protection Principles, however, the role of monitoring and enforcing compliance with the data protection programme was not formally established due to absence of a clear set of responsibilities.

   High Priority Recommendation:
   - Monitoring and oversight functions should be formally established with clear assignment of roles and responsibilities in the update of IOM Data Protection Principles.

6. Training on Data Protection
   Training on data protection is not mandatory, as such, training has not been formally cascaded to all country offices mainly due to limited resources both manpower and budget wise.

   High Priority Recommendation:

   - Devise a training plan and identify training focal points that could assist in the delivery of a face-to-face training on data protection.

7. Data sharing with third parties
   The current Data Protection Principles focus on transfers of personal data to third parties. However, there is no detailed guidance on receiving personal data by third parties.

   High Priority Recommendation:

   - Establish clear policies, mandatory minimum procedures, appropriate controls, and risk mitigating measures encompassing all types of data sharing arrangements.

8. Policy on Retention and Destruction of Personal data
   Existing policies incorporates data retention, however, there are no specific policies that define the retention period, criteria, and method of disposal, and required documentation.

   High Priority Recommendation:

   - Establish a comprehensive, clear, and harmonized policies and procedures on retention and destruction of records containing migrants' personal data.

9. Processing Migrants' personal data
   Existing policies and procedures and practices undertaken revealed gaps in safeguarding the confidentiality, integrity, and availability of personal data.

   High Priority Recommendations:

   - IOM's Data Protection Policies and other relevant security policies should specify clear instructions on mandatory minimum-security measures in handling different types of migrants' personal data.
   - IOM systems that are considered high risk should undergo a comprehensive and specific data privacy assessment.

Management agreed with the recommendations and is implementing them.

ANNEXES

Definitions

The overall adequacy of the internal controls, governance and management processes, based on the number of audit findings and their risk levels:

Descriptor	Guide
Fully effective	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, address the root causes and Management believes that they are effective and reliable at all times.
Substantially effective	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness or Management has doubts about operational effectiveness and reliability.
Partially effective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. Or, some of the controls do not seem correctly designed in that they do not treat root causes, those that are correctly designed are operating effectively.
Largely ineffective	Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively.
None or totally ineffective	Virtually no credible controls. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness.

Audit Recommendations – Priorities

The following internal audit rating based on **IOM Risk Management** framework has been slightly changed to crystalize the prioritization of internal audit findings according to their relative significance and impact to the process:

Rating	Definition	Suggested action	Suggested timeframe
Very High	Issue represents a control weakness which could cause ***critical*** disruption of the process or ***critical*** adverse effect on the ability to achieve entity or process objectives.	Where control effectiveness is not as high as 'fully effective', take action to reduce residual risk to 'high' or below.	Should be addressed in the short term, normally within 1 month.
High	Issue represents a control weakness which could have ***major*** adverse effect on the ability to achieve entity or process objectives.	Plan to deal with in keeping with the annual plan.	Should be addressed in the medium term, normally within 3 months.
Medium	Issue represents a control weakness which could have ***moderate*** adverse effect on the ability to achieve entity or process objectives.	Plan in keeping with all other priorities.	Should be addressed normally within 1 year.
Low	Issue represents a minor control weakness, with ***minimal*** but reportable impact on the ability to achieve entity or process objective.	Attend to when there is an opportunity to.	Discussed directly with management and actions to be initiated as part of management's ongoing control.