

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

OFFICE OF INTERNAL OVERSIGHT SERVICES · BUREAU DES SERVICES DE CONTRÔLE INTERNE
INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE

TO: Mr. Robert Benson, Director

DATE: 21 December 2009

A: Ethics Office

REFERENCE: IAD: 09- **03228**

FROM: Fatoumata Ndiaye, Acting Director
Internal Audit Division, OIOS



SUBJECT: **Assignment No. AT2008/510/01 – Horizontal audit of data privacy in the United Nations Secretariat**
OBJET:

The Ethics Office should define a standard privacy notice and implement stricter controls for the transmission of information with third parties, and the security of data stored on mobile devices.

1. I am pleased to present the report on the above-mentioned audit which was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
2. While cross-cutting issues related to data privacy in the UN Secretariat have been documented in a separate report, this memorandum addresses issues specific to the Ethics Office.
3. Based on your comments, we are pleased to inform you that we will close recommendation 3 in the OIOS recommendations database as indicated in Annex 1. In order for us to close the remaining recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
4. Your response indicated that you did not accept recommendation 4. In OIOS' opinion however, this recommendation seeks to address a significant risk area. We are therefore reiterating it and requesting that you reconsider your initial response based on the additional information provided in the report.
5. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendation 1 and 3), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

EXECUTIVE SUMMARY

Horizontal audit of data privacy in the United Nations Secretariat

OIOS conducted an audit of data privacy across the United Nations Secretariat. The overall objective of the audit was to determine whether the Secretariat has adequate controls in place to protect the confidentiality and integrity of sensitive information related to employees, representatives of Member States, and other individuals. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

The cross-cutting issues identified during the course of the audit have been documented in a separate audit report. This report addresses the risks and controls specific to the Ethics Office (EO).

The Ethics Office performs several activities that require collecting, processing, and storing personal identifiable data. Considering the sensitivity of data collected, processed and stored by the Ethics Office, OIOS recommended that the Office:

- a) Implement a more secure way of data exchange with third parties, using encryption mechanisms to protect the integrity and confidentiality of the data transmitted by email;
- b) Review past cases where conflicts of interest were confirmed, and identify what data fields were used to reach those conclusions. If, as a result of this review, there are certain data fields that have never been used to confirm the existence of conflict of interest, the Ethics Office should recommend the removal of those fields from the standard form;
- c) Store data collected through the "Protection Against Retaliation Programme" only on encrypted mobile computing devices (laptops or flash drive);
- d) Develop a standard notice procedure, in collaboration with the Office of Legal Affairs, to provide staff involved in alleged cases of retaliation with information about the collection, use, disclosure, and disposal of information gathered during the review; and
- e) Develop a retention schedule for the cases of retaliation in collaboration with the Office of Legal Affairs and the United Nations Archives and Records Management Section.

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of data privacy at the United Nations Secretariat. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
2. Data privacy refers to the right of individuals to control the collection and use of personal information about themselves. The Black's Law Dictionary defines it as "a private person's right to choose to determine whether, how, and to what extent information about oneself is communicated to others". It has not been formally defined by the United Nations Secretariat.
3. Comments made by the Ethics Office are shown in *italics*.

II. AUDIT OBJECTIVES

4. The main objectives of the audit were to assess whether:
 - (a) A governance system is in place to manage privacy of data;
 - (b) The Secretariat has defined what data should be considered sensitive, with particular reference to privacy of data, per ST/SGB/2007/6 on Information sensitivity, classification, and handling; and
 - (c) Adequate controls are in place for the protection of data privacy.

III. AUDIT SCOPE AND METHODOLOGY

5. The audit covered the current policies, procedures, working practices and systems in the Ethics Office.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Financial disclosure programme

Inadequate controls for the transmission of data to third parties

6. The Ethics Office supports the Financial Disclosure Programme of the Secretariat. This programme includes a database containing sensitive data related to approximately 7,000 senior level staff members of the United Nations, such as: assets, liabilities, spouse information, and board memberships. The Ethics Office periodically requests updates from each Department about the names of in-scope staff members. These names are then provided to the Office of Information and Communications Technology (OICT), for their subsequent upload into a database maintained by Price Waterhouse Coopers (PWC). Staff members submit their documentation to the Ethics Office via diplomatic pouch, and the Ethics Office then submits hard copies to PwC via registered mail. In some cases, however,

data is also collected by the Ethics Office and it sent to PwC via unencrypted email messages.

7. PwC administers the database containing data and files for each staff member involved in the Financial Disclosure Programme, and analyzes the submissions for discrepancies. PwC in turn submits to the Ethics Office, via electronic mail, unprotected compressed files containing the report of their analysis.

Recommendation 1

(1) The Ethics Office should implement a more secure way of data exchange with Price Waterhouse Coopers, using encryption mechanisms to protect the integrity and confidentiality of the data transmitted by email.

8. *The Ethics Office accepted recommendation 1 and stated that they requested the ICT Quality Assurance and Risk Management Section (QARMS) of OICT to perform a comprehensive risk assessment of the Ethics Office information systems and data. This exercise was initiated in August 2007 and the final report was received by the Ethics Office in November 2008. The report included a risk treatment plan and 31 recommendations, five of which relate directly to the Financial Disclosure Programme. The Ethics Office confirmed that is committed to and is presently in the process of implementing all of the recommendations of the report to ensure the integrity and confidentiality of all the data handled by the Ethics Office. Recommendation 1 remains open pending submission to OIOS of evidence documenting the implementation of secure mechanisms for data exchange with Price Waterhouse Coopers (PWC).*

Collection of personal financial data

9. The audit revealed a common concern among several staff outside the Ethics Office about the extent of the information required within the Financial Disclosure Programme, and whether all the data requested were actually needed and used to reach reasonable conclusions about the existence of conflicts of interest. In this regard, an analysis of the informational value of the data gathered throughout the years would help the Ethics Office to identify those data elements that are needed for an efficient and effective implementation of the programme.

Recommendation 2

(2) The Ethics Office should conduct a review of the data gathered in the context of the Financial Disclosure Programme. The review should consider past cases where conflicts of interest were confirmed, identify what data fields were used to reach those conclusions, and adjust the data collection procedures accordingly.

10. *The Ethics Office accepted recommendation 2 and stated that the information disclosed on a confidential basis by eligible staff members within the context of the Financial Disclosure Programme(FDP) is reviewed to ensure that potential conflicts of interest arising from staff members' financial holdings, private affiliations or outside activities can be identified, and advice provided as to how best to manage any potential*

conflicts of interests in the best interests of the United Nations. The information is also reviewed for its completeness and is maintained in strict confidence throughout the process, unless otherwise agreed to by the concerned staff members. Following the completion of each filing cycle, aggregate data are analyzed, while maintaining the confidentiality of the data and concerned staff members, in order to understand common issues and trends, and draw comparisons and lessons for the future. Adjustments, including those in relation to the analytical framework, data requirements, collection procedures and technological improvements are regularly reviewed. These are ongoing features of the FDP. Recommendation 2 remains open pending submission to OIOS of evidence documenting the analysis conducted on the aggregate data at the end of the last filing cycle.

B. Protection against retaliation programme

Inadequate procedures and controls to ensure secure collection, transmission, and storage of data

11. The Ethics Office administers a process designed to protect whistleblowers when reporting cases of retaliation. About 60 cases were handled in 2006, and 52 in 2007. 67% of staff initiated the process via e-mail, and then produced, in person, a “Protection Against Retaliation Form” (PAR Form), along with additional supporting documentation. The information collected through the PAR Forms is subsequently stored in flash drives, and a Master Database developed on Microsoft Access.

12. OIOS noted that from a privacy perspective, the current process presents the following risks:

- a. Sensitive e-mails are received and sent using unencrypted e-mail;
- b. Sensitive data is stored on unencrypted flash drives;
- c. In general, individuals involved in cases of alleged retaliations are not informed about the procedures followed by the Ethics Office for the collection, use, disclosure, and disposal of data reviewed; and
- d. The Office does not dispose files where the allegations were unfounded, and does not have a policy for disposing closed cases that have reached a certain age limit.

Recommendation 3

(3) The Ethics Office should store data collected through the “Protection Against Retaliation Programme” only on encrypted mobile computing devices (laptops or flash drive).

13. *The Ethics Office accepted recommendation 3 and stated that this recommendation has been implemented since March 2009, following the QARMS report mentioned in response to recommendation 1 above. Secure flash drives, as approved by QARMS, were purchased and are in use. Based on the actions taken by the Ethics Office in coordination with OICT, recommendation 3 has been closed.*

Recommendation 4

(4) The Ethics Office, in collaboration with the Office of Legal Affairs, should develop a standard notice procedure to provide staff members involved in suspected case of retaliation with information about the collection, use, disclosure, and disposal of information gathered during the review.

14. *The Ethics Office did not accept recommendation 4, stating that the implementation of the recommendation goes beyond the purview of the mandated responsibilities of the Ethics Office. In the context of the implementation of the protection against retaliation policy that is contained in ST/SGB/2005/21, the mandate of the Ethics Office is to receive complaints of retaliation and to conduct a preliminary review to determine whether a prima facie case of retaliation exists. If such a determination is made, the case is referred to OIOS for investigation in order to establish retaliation. The Ethics Office does not receive any reports of misconduct other than complaints of retaliation and it does not conduct investigations against anyone suspected of misconduct. As per Section 5.2 of the SGB, the Office maintains a confidential record of all complaints received, including all information gathered during the review. Information received is not disclosed to any third parties. OIOS is unable to accept the assertions made by the Ethics Office and reiterates its recommendation. The Ethics Office, in addition to preserving the confidentiality of all complaints and information gathered during its review, should also ensure that all parties involved in its review are informed about the collection, use, disclosure, and disposal of information provided. Therefore, recommendation 4 remains open pending submission to OIOS of evidence documenting the coordinated efforts between the Ethics Office and the Office of Legal Affairs for the development of a standard notice procedure. This notice should provide staff members involved in suspected case of retaliation with information about the collection, use, disclosure, and disposal of information gathered during the review.*

Recommendation 5

(5) The Ethics Office, in collaboration with the Office of Legal Affairs and the United Nations Archives and Records Management Section, should develop a retention schedule for the cases brought to its attention.

15. *The Ethics Office accepted recommendation 5 and stated that the Office has implemented the recommendation made, in so far as developing a retention schedule for all files and case materials maintained in confidence in the Ethics Office. Following the QARMS report mentioned above in response to recommendation 1, the Ethics Office has initiated a dialogue with the Archives and Records Management Section and is currently working with this office to establish a retention schedule for documents safeguarded by the Ethics Office. The retention schedule is expected to be finalized in Summer 2009. Recommendation 5 remains open pending submission to OIOS of evidence documenting the retention schedule developed by the Ethics Office in collaboration with the Archives and Records Management Section.*

V. ACKNOWLEDGEMENT

16. We wish to express our appreciation to the Management and staff of the Ethics Office for the assistance and cooperation extended to the auditors during this assignment.

cc: Ms. Angela Kane, Under-Secretary-General, Department of Management
Ms. Patricia O'Brien, Under-Secretary-General, Office of Legal Affairs
Mr. Choi Soon-hong, Assistant Secretary General, Chief Information Technology Officer
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwanye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG, OIOS
Ms. William Petersen, Chief, New York Audit Service, OIOS

CONTACT INFORMATION:

ACTING DIRECTOR:

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,
e-mail: ndiaye@un.org

ACTING DEPUTY DIRECTOR:

Gurpur Kumar: Tel: +212.963.5920, Fax: +1.212.963.3388
e-mail: kumarg@un.org

CHIEF, NYHQ AUDIT SERVICE:

William Petersen: Tel: +1.212.963.3705, Fax: +1.212.963.3388,
e-mail: petersenw@un.org

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date ²
1	The Ethics Office should implement a more secure way of data exchange with Price Waterhouse Coopers, using encryption mechanisms to protect the integrity and confidentiality of the data transmitted by email.	Information Resources	High	O	Submit to OIOS evidence documenting the implementation of secure mechanisms for data exchange with Price Waterhouse Coopers	Not provided
2	The Ethics Office should conduct a review of the data gathered in the context of the Financial Disclosure Programme. The review should consider past cases where conflicts of interest were confirmed, identify what data fields were used to reach those conclusions, and adjust the data collection procedures accordingly.	Information Resources	Medium	O	Submit to OIOS evidence documenting the analysis conducted on the aggregate data at the end of the last filing cycle.	Not provided
3	The Ethics Office should store data collected through the "Protection Against Retaliation Programme" only on encrypted mobile computing devices (laptops or flash drive).	Information Resources	High	C	Action completed.	Implemented
4	The Ethics Office, in collaboration with the Office of Legal Affairs, should develop a standard notice procedure to provide staff members involved in suspected case of retaliation with information about the collection, use, disclosure, and disposal of information gathered during the review.	Governance	Medium	O	Submit to OIOS a standard notice describing the collection, use, disclosure, and disposal of information gathered by the Ethics Office during the review of alleged cases of retaliations.	Not provided
5	The Ethics Office, in collaboration with the Office of Legal Affairs and the United Nations Archives and Records Management Section, should develop a retention schedule for the cases brought to its attention.	Information Resources	Medium	O	Submit OIOS evidence documenting the retention scheduled developed by the Ethics Office in collaboration with the Archives and Records Management Section.	Not provided

-
1. C = closed, O = open
 2. Date provided by the Ethics Office in response to recommendations.