



## INTERNAL AUDIT DIVISION

# AUDIT REPORT

---

Horizontal audit of data privacy in the  
United Nations Secretariat and  
peacekeeping missions

The Secretariat is yet to establish internal  
controls to manage data privacy and ensure the  
protection of sensitive data

30 December 2009  
Assignment No. AT2008/510/01

---

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. Vijay Nambiar, Chef de Cabinet  
A: Executive Office of the Secretary-General

DATE: 30 December 2009

Mr. Kiyotaka Akasaka, Under-Secretary-General  
Department of Public Information

Ms. Angela Kane, Under-Secretary-General  
Department of Management

Mr. Choi Soon-hong,  
Assistant Secretary-General and  
Chief Information Technology Officer

REFERENCE: IAD: 09-

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



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

1. I am pleased to present the report on the above-mentioned audit.
2. In order for us to close the audit 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.
3. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 1, 2, 3, 18, 27, 30, and 32), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Ms. Patricia O'Brien, Under-Secretary-General, OLA  
Ms. Susana Malcorra, Under-Secretary-General, DFS  
Mr. Alain Le Roy, Under-Secretary-General, DPKO  
Mr. Shaaban Muhammad Shaaban, Under-Secretary-General, DGACM  
Mr. Gregory Starr, Under-Secretary-General, DSS  
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

---

## INTERNAL AUDIT DIVISION

---

### FUNCTION

*“The Office shall, in accordance with the relevant provisions of the Financial Regulations and Rules of the United Nations examine, review and appraise the use of financial resources of the United Nations in order to guarantee the implementation of programmes and legislative mandates, ascertain compliance of programme managers with the financial and administrative regulations and rules, as well as with the approved recommendations of external oversight bodies, undertake management audits, reviews and surveys to improve the structure of the Organization and its responsiveness to the requirements of programmes and legislative mandates, and monitor the effectiveness of the systems of internal control of the Organization” (General Assembly Resolution 48/218 B).*

---

### CONTACT INFORMATION

**ACTING DIRECTOR:**

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,  
e-mail: [ndiaye@un.org](mailto:ndiaye@un.org)

**ACTING DEPUTY DIRECTOR:**

Gurpur Kumar: Tel: +1.212.963.5920, Fax: +1.212.963.3388,  
e-mail: [kumarg@un.org](mailto:kumarg@un.org)

---

## EXECUTIVE SUMMARY

### Horizontal audit of data privacy in the United Nations Secretariat and peacekeeping missions

OIOS conducted an audit of data privacy across the United Nations Secretariat and peacekeeping missions. The overall objective of the audit was to assess whether the Secretariat has adequate controls in place to protect the confidentiality and integrity of sensitive information related to staff, 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 United Nations Secretariat has not established sufficient controls to ensure the privacy of personal data. In addition, since no data classification scheme has been implemented, the Organization was unable to consistently determine the controls to be put in place to protect sensitive information. These conditions expose the Secretariat to the risks of breach of confidentiality, and failure to protect the privacy of personal data.

The audit highlighted several control weaknesses, as summarized below:

- (a) Insufficient formalization of accountability and policy guidance for data privacy;
- (b) Lack of defined data classification for privacy management;
- (c) Lack of knowledge and training initiatives for data privacy;
- (d) Lack of procedures to obtain consent of data subjects (employees, representatives of member states, and other individuals) before data collection;
- (e) Collection of unnecessary personal identifiable data;
- (f) Lack of procedures for destroying personal identifiable data that is no longer needed;
- (g) Ad-hoc and inconsistent approach to providing staff access to their own personal identifiable data;
- (h) Lack of comprehensive policy and adequate process for identifying and correcting data inaccuracies that could potentially harm individuals;
- (i) Inadequate controls and procedures for secure e-mail communication and electronic recordkeeping; and
- (j) Absence of a central point of contact for privacy-related issues.

# TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1-3
II. AUDIT OBJECTIVES	4
III. AUDIT SCOPE AND METHODOLOGY	5-7
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Governance of data privacy	8-16
B. Data privacy notification	17-28
C. Informed consent of data privacy	29-33
D. Collection of personal data	34-37
E. Use and retention of personal data	38-42
F. Access to personal data	43-49
G. Accuracy of personal data	50-53
H. Security of personal data	54-85
I. Disclosure of personal data to third parties	86-94
J. Monitoring and enforcement of privacy policies	95-103
V. ACKNOWLEDGEMENT	104
ANNEX 1 – Status of Audit Recommendations	

---

## I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of data privacy in the United Nations Secretariat and peacekeeping missions. 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". Data privacy has not been formally defined by the Secretariat.
3. Comments made by the Executive Office of the Secretary-General (EOSG), Office of Information and Communications Technology (OICT), Department of Public Information (DPI) and Department of Field Support (DFS) 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, as per the Secretary-General's Bulletin 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 following Offices and Departments of the Secretariat and peacekeeping missions:

- Executive Office of the Secretary-General (EOSG)
  - Ethics Office
  - Department of Field Support (DFS)
  - Department of General Assembly and Conference Management (DGACM)
  - Department of Management (DM)
  - Department of Public Information (DPI)
  - Department of Peacekeeping Operations (DPKO)
  - Department for Safety and Security (DSS)
  - Office of Information and Communications Technology (OICT)
  - Office of Legal Affairs (OLA)
  - United Nations Mission in Sudan (UNMIS)
-

---

6. The audit focused on the main process components of the data privacy programme, as stipulated in the United Nations guidelines for the regulation of computerized personal data (General Assembly resolution 45/95), and the Generally Accepted Privacy Principles (GAPP) developed by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). These are:

- (a) Management;
- (b) Notice;
- (c) Choice and consent;
- (d) Collection;
- (e) Use and retention;
- (f) Access;
- (g) Disclosure;
- (h) Security; and
- (i) Monitoring and enforcement.

7. Interviews were held with key officers with responsibilities for data privacy. Documentation was obtained and reviewed to ascertain the governance structure, management, and security environment. Tests were conducted to confirm the adequacy of controls and to identify threats, risks and vulnerabilities that may affect the privacy of data.

## IV. AUDIT FINDINGS AND RECOMMENDATIONS

### A. Governance of data privacy

The Secretariat does not have formally defined responsibilities, accountabilities, and policies for data privacy

8. The Secretary-General has not assigned data privacy responsibilities to a dedicated committee, department or an individual staff member. This void was particularly evident within the United Nations Secretariat's public internet presence. Except for a partial subset of internet websites directly managed by DPI, the authority to approve the public release of the many United Nations Secretariat entities' websites has not been formally clarified. These websites can capture and share sensitive information in the public domain – including potentially private data – in an open and insecure manner. Such data may include, for example, personal identifiable information of staff, vendors and others (names, index numbers, email addresses, telephone numbers, etc). There were no Secretariat-wide privacy standards for use by departments and offices to develop their own privacy requirements and processes. The Medical Services Division (MSD) of the Office of Human Resources Management (OHRM) requires that all new staff read and sign a five-page document entitled "Undertaking to Protect the Confidentiality of Medical Information", detailing the privacy standards and procedures of the Division. The Field Personnel Division of DFS has recently disseminated a detailed five-page document on data

---

protection to its 35 field desk officers. The Department of Safety and Security (DSS) has developed a draft Standard Operating Procedure for information sharing and handling. DPKO has developed Standard Operating Procedures. While these documents should be considered models for other units within the United Nations Secretariat, there is a risk that the Organization as a whole does not process private data in a consistent manner. In addition, multiple departmental initiatives with no centralized policy tend to be not sufficiently efficient and effective.

### **Recommendations 1 and 2**

#### **The Secretary-General should:**

- (1) Assign to a new or existing Secretariat unit the responsibility to develop and manage a comprehensive data privacy programme for the Secretariat; and**
- (2) Establish a Data Privacy Steering Committee comprising representatives of Departments and Offices with sufficient authority to establish privacy requirements and provide guidance for implementing related internal controls.**

#### **Recommendation 3**

- (3) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Office of Legal Affairs, develops a Secretariat-wide data privacy policy.**

9. *EOSG accepted recommendation 1 and agreed that a governance system needed to be established to manage privacy of data in the Secretariat EOSG advised that OICT will be assigned to undertake the responsibility to manage a data privacy programme for the United Nations Secretariat. Further, the Office of the Deputy Secretary-General (ODSG) held consultations with OICT, who agreed to undertake this task. OICT, however, informed ODSG that the responsibility to develop and manage a comprehensive data privacy programme for the Secretariat was a significant, long-term effort that will require the allocation of additional resources by the General Assembly. OICT added that unless additional funding was provided, it would be impossible to make progress on this matter. Recommendation 1 remains open pending receipt of documentation showing the allocation of responsibility to develop and manage a comprehensive data privacy programme for the United Nations Secretariat to OICT.*

10. *EOSG did not provide a specific response to recommendation 2 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy. Recommendation 2 remains open pending the establishment of a Data Privacy Steering Committee comprising of representatives of Departments and Offices.*

---

11. *EOSG accepted recommendation 3 and stated that it supported the recommendation that the Secretary-General should develop a comprehensive data privacy policy to address issues related to: data classification schemes; collection, use, retention, disclosure, access and security of personal data; mechanisms to report abuse and violation of data privacy of staff; and provision of privacy notices on United Nations public websites.* Recommendation 3 remains open pending the development and dissemination of a Secretariat-wide data privacy policy.

#### Lack of data classification for privacy management

12. According to ST/SGB/2007/6 on information sensitivity, classification and handling, “information deemed sensitive shall include documents whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights or invade his or her privacy”. The implementation of these provisions requires the identification of what types of data fall within the definition of privacy, as indicated in ST/SGB/2007/6. Since the Organization has not yet identified these data types, there is a risk that different offices of the United Nations Secretariat will have different interpretations of data classification requirements, or use different classifications altogether. A divergence in data classification requirements and their implementation could render data privacy protections ineffective.

13. In addition, the non implementation of the data classification scheme established in ST/SGB/2007/6 prevented the Organization from identifying, in a consistent manner, the controls to implement in order to protect sensitive information. The United Nations Secretariat was unable to determine: (a) its exposure to the risks associated with breaches of data confidentiality; and (b) the adequate allocation of its human, financial, and technical resources to data protection.

#### **Recommendation 4**

**(4) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy identifies all data classification schemes in use within the United Nations Secretariat and proposes their replacement with a common, detailed classification scheme based on the general categories listed in ST/SGB/2007/6.**

14. *EOSG accepted recommendation 4 and stated that it supported the recommendation that the Secretary-General should develop a comprehensive data privacy policy to address issues related to data classification schemes; collection, use, retention, disclosure, access and security of personal data; mechanisms to report abuse and violation of data privacy of staff; and provision of privacy notices on United Nations public websites.* Recommendation 4 remains open pending the identification of all data classification schemes in use within the Secretariat and the development of a common classification scheme based on ST/SGB/2007/6.

---

Lack of knowledge and training initiatives for data privacy

15. The Secretariat does not have specific training modules on data privacy, nor is the topic included in the orientation programme for newly recruited staff. Some departments have included references to some aspects of data privacy in their internal training activities. For example, DSS conducts periodic training for its staff, posts security awareness posters in its New York office, and makes a poster in multiple languages available on its intranet site. However, while these ad-hoc initiatives address the operational needs of specific departments, the absence of a Secretariat-wide approach limits the ability of the Organization to prevent and mitigate data privacy risks.

**Recommendation 5**

**(5) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with Department of Management, undertakes activities to sensitize and train staff in United Nations data privacy requirements.**

16. *EOSG did not provide a specific response to recommendation 5 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy.* Recommendation 5 remains open pending the undertaking of activities to sensitize and train staff on United Nations data privacy requirements.

**B. Data privacy notification**

Individuals are not notified about why their personal data is collected, and how it is used, secured, shared, and disposed of

17. Individuals who are the subject of their personal data are referred to as “Data Subjects”. Providing “Privacy Notices” to data subjects about the specific purposes of data collection is considered a foundational data privacy principle.

18. A privacy notice should allow data subjects to know: (a) what are the principal purposes for which the information is intended to be used; and (b) the routine uses that may be made of their personal information. Without purpose specification, many other privacy principles cannot be fully manifested.

19. The practices of the United Nations Secretariat included many instances where departments and offices do not provide privacy notices to data subjects upon collecting their “personal identifiable information”. For example, the Medical Services Division, OHRM, did not provide privacy notices to its users. Such notices are a common practice in the health care sector. Also, the Ethics Office did not notify staff members who had been the subject of ethics inquiries. One exception to these common practices is that OHRM, in accordance with the applicable administrative instructions, notifies a staff member when adverse material is placed on their official status file.

---

20. In addition, websites operated by the United Nations Secretariat that collect personal identifiable information, including credit card information, had a mixed record on providing privacy notices. Examples of this variety were found in the following cases, where no details were provided about the use, retention, and disposal of personal identifiable data:

(a) The website of the United Nations Bookshop (<https://unp.un.org>), administered by DPI. Considering the commercial nature of this web site and its large public audience, the site should be completed with a standard privacy notice regarding the purpose and use of the data collected through the “sign-in” process and purchasing transactions;

(b) The United Nations Procurement Division’s Global Marketplace, which captures personal identifiable information from vendors;

(c) The United Nations Global Teaching and Learning Project’s “Cyberschoolbus”, used by school teachers and students, collecting and storing their e-mail addresses, and

(d) The online process for media accreditation available at “[www.un.org/media/accreditation/form/index.html#](http://www.un.org/media/accreditation/form/index.html#)”, that requires its users to input several personal identifiable data items, such as name, telephone numbers, citizenship, date of birth, place and country of birth, home address, hair colour, eye colour, height, and weight.

25. The lack of complete privacy notifications prevent data subjects (staff, contractors, delegates, external users, etc.) from understanding the level of data protection afforded to them by the United Nations Secretariat. This condition weakens their level of confidence in the information systems and related processes of the Organization.

### **Recommendations 6 to 8**

**The Executive Office of the Secretary-General should:**

**(6) Ensure that the unit charged with the new responsibilities for data privacy, in coordination with heads of Departments and Offices, defines a standard “Privacy Notice”, indicating the terms of reference for the collection, use, security, sharing, and disposing of personal identifiable data within the Organization;**

**(7) Ensure that the unit charged with the new responsibilities for data privacy, in coordination with heads of Departments and Offices, develops procedures to catalog all forms used to collect personal identifiable data in the United Nations, whether manually or electronically generated. Each form should be complemented by a “Privacy**

---

**Notice”, indicating the terms of reference for the collection, use, security, sharing, and disposing of personal identifiable data within the Organization; and**

**(8) Ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Department of Public Information, the Office of Legal Affairs, and the Office of Information and Communications Technology, conducts a review of all United Nations public web sites and ensures that a privacy notice is posted on each such site.**

#### **Recommendation 9**

**(9) The Department of Public Information should ensure that the online media accreditation site contains a privacy notice regarding the purpose and use of the data collected through that site.**

26. *EOSG accepted recommendation 6 and stated that it supports the recommendation that the Secretary-General should develop a comprehensive data privacy policy to address issues related to data classification schemes; collection, use, retention, disclosure, access and security of personal data; mechanisms to report abuse and violation of data privacy of staff; and provision of privacy notices on UN public website.* Recommendation 6 remains open pending the formal promulgation of a standard “Privacy Notice”, indicating the terms of reference for the collection, use, security, sharing, and disposing of personal identifiable data within the Organization.

27. *EOSG did not provide a specific response to recommendations 7 and 8 but accepted the summary findings of the draft audit report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy. EOSG supports the recommendation that the Secretary-General should develop a comprehensive data privacy policy to address issues related to data classification schemes; collection, use, retention, disclosure, access and security of personal data; mechanisms to report abuse and violation of data privacy of staff; and provision of privacy notices on UN public website.* Recommendation 7 remains open pending the development of procedures to catalog all forms used to collect personal identifiable data at the United Nations Secretariat, whether manually or electronically generated. Recommendation 8 remains open pending the review of all United Nations Secretariat public websites and the posting of a privacy notice on each such site.

28. *DPI accepted recommendation 9 and stated that preliminary work had begun to implement it.* Recommendation 9 remains open pending the posting of a privacy notice on DPI’s online media accreditation site regarding the purpose and use of the data collected.

---

## C. Informed consent of data subject

### Departments and offices do not seek or collect the consent of data subjects

29. Data subjects should provide their informed consent for having their personal data collected and used. Such consent, which may be explicit or implicit, relies on the timely provision of privacy notices.

30. The consent of data subjects is especially relevant if personal data is used for purposes other than those for which it was initially collected (“secondary purposes”). This can happen if personal data is used in studies, research, and statistics, or if data is shared with non-United Nations entities.

31. The results of OIOS’ review indicated that departments and offices of the Secretariat do not seek or collect the consent of data subjects. However, it was also confirmed that there were no instances of incorrect secondary uses, or external sharing of personal information, for which data subjects would expect their consent to be sought. As one example, the Medical Services Division, OHRM, does not share personal identifiable data with anyone without the consent of the data subject and OLA’s direction.

32. The absence of systematic controls and processes for acquiring consent from data subject exposes the Secretariat to the risk of using sensitive data and information for purposes that have not been explicitly accepted and authorized.

### **Recommendation 10**

**(10) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Office of Legal Affairs, conducts an analysis to determine those instances where the Secretariat should capture and record the consent of its data subjects, and direct the relevant offices to do so.**

33. *EOSG did not provide a specific response to recommendation 10 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy. EOSG supports the recommendation that the Secretary-General should develop a comprehensive data privacy policy to address issues related to data classification schemes; collection, use, retention, disclosure, access and security of personal data; mechanisms to report abuse and violation of data privacy of staff; and provision of privacy notices on UN public website. Recommendation 10 remains open pending issuance of appropriate directions to relevant departments and offices regarding the recording of consent of their data subjects.*

---

## D. Collection of personal data

### Collection of unnecessary personal data

34. Collecting personal data should be limited to what is strictly necessary, in order to reduce the risk of improperly using personal information. A critical component for complying with all other data privacy principles is managing an inventory of the ways in which personal identifiable information is collected, stored, shared, and disposed of.

35. The Secretariat collected personal identifiable data it deemed necessary for its functions. However, in some cases, offices adopted the approach of collecting at once all of the information they might possibly need, rather than in stages, as needs evolved. For example:

(a) Medical Services Division, OHRM: An “Entry Medical Examination” form, which contains four pages of detailed, sensitive health information, has been administered for the past sixty years. The "Periodic Medical Examination" form likewise is a four-page form of sensitive data. The doctors require all this information in order to form a full picture of a data subject’s health profile. However, Medical Services Division acknowledged that some of the information currently collected through these forms could be revised and requested, if needed, at a later stage of analysis.

(b) OHRM: The recruitment process requires that candidates interested in applying for employment opportunities at the United Nations Secretariat complete and submit a Personal History (“P.11”) form. This form includes much data that would only be relevant and necessary at the final stage of the appointment process, in the event the candidate is hired (i.e. dependant children, spouse). The same observation also applies to the recruitment of external consultants, who are asked to complete and submit the same Personal History form (P.11), required for the recruitment of regular staff members.

(c) Ethics Office: In the Financial Disclosure Programme administered by the Ethics Office, approximately 3,000 United Nations staff members who satisfy the Programme eligibility criteria, involved in monetary transactions and decision making, are required to complete a thorough disclosure of their personal and family income, assets, and investments. Indeed, several interviewees in different offices of the Secretariat, when asked to name what concerned them most about privacy in the United Nations Secretariat, mentioned the Financial Disclosure Programme.

36. Collecting unnecessary personal data increases the risks of confidentiality breaches, unauthorized access, and misuse of information. Consequently, this situation would force the Organization to allocate additional resources and controls to manage and mitigate these risks.

---

## Recommendation 11

**(11) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with heads of Departments and Offices, defines a process and criteria to identify the specific needs for personal identifiable data collected through forms and databases, in order to avoid the collection of unnecessary personal data.**

37. *EOSG did not provide a specific response to recommendation 11 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy. EOSG supports the recommendation that the Secretary-General should develop a comprehensive data privacy policy to address issues related to data classification schemes; collection, use, retention, disclosure, access and security of personal data; mechanisms to report abuse and violation of data privacy of staff; and provision of privacy notices on UN public website. Recommendation 11 remains open pending the formal promulgation of procedures and criteria to identify the specific needs of the United Nations departments and offices for personal identifiable data, to be collected through forms and databases, and to avoid collecting unnecessary personal data.*

## E. Use and retention of personal data

### Procedures for the destruction of personal identifiable data that is no longer needed are still under development

38. The use of personal information should be limited to the purpose identified in the notice provided to individuals, and for which they have provided implicit or explicit consent.

39. The sample of activities reviewed during the audit indicated that in general, departments and offices used personal identifiable information they needed only for the purposes of implementing their respective mandates. However, the process for destruction of personal identifiable information that is no longer needed was still under development. An initiative was launched by the Archives and Records Management Section (ARMS) to define and improve consistency of archiving records that contains personal data.

40. Inadequate controls and processes for the disposition of personal data could result in data being retained indefinitely. This condition would increase the risk of using sensitive information inconsistently with its intended purpose, potentially in ways that could endanger the safety and security of individuals.

## Recommendation 12

**(12) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Archives and Records**

---

**Management Section, includes in its guidelines for records retention schedules, instructions for identifying and marking records containing private data that are no longer needed, which should be disposed of.**

41. *EOSG did not provide a specific response to recommendation 12 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy. Recommendation 12 remains open pending receipt of instructions for identifying and marking records containing private data that are no longer needed, and their disposal.*

42. *DM also commented on recommendation 12 stating that the suggestion that ARMS and/or the newly created unit charged with the responsibilities for data privacy include markers in records retention schedules indicating records containing private data is impractical. Responsibility for identifying sensitive content in substantive records lies within the purview of the creating office. Each UN department and office should have a comprehensive records security plan that would identify records that contain private and sensitive information, assign appropriate protection and access levels for such information, and link to its disaster mitigation/vital records programmes. OIOS clarifies that recommendation 12 indicates that instructions should be given to department and offices for marking records. OIOS agrees with DM's comments and the principle established in ST/SGB/2007/6, assigning the responsibility for identifying sensitive content in substantive records to the creating offices. However, in view of the non-implementation of ST/SGB/2007/6 after more than two years of its issuance, OIOS maintains that the newly created unit responsible for data privacy, in coordination with ARMS, should issue instructions to departments and offices for marking records containing private and sensitive information.*

## F. Access to personal data

### Ad-hoc and inconsistent approach to providing staff access to their information

43. Access to personal data should be limited to properly authorized and authenticated staff members. These could include the data subjects themselves, and/or officers conducting data processing activities during the performance of their duties.

44. The Secretariat takes an ad-hoc and inconsistent approach to providing staff access to their own information. Official status files of staff are kept with OHRM, which allows staff to review their individual file once every year. In addition, however, many (but not all) staff members can access their information stored in the main human resources information system (the Integrated Management Information System, IMIS), through the United Nations internal Web Integrated Reporting portal "WIRE".

45. Other United Nations Secretariat entities have access to staff personal information. These include, for example, personnel of Executive Offices of the departments/offices where staff have worked in the past, and the Medical

---

Services Division, OHRM. With regard to the practices followed by Executive Offices, the sample reviewed during the audit indicated that at least in one case, a staff member was not allowed to access an unofficial personal file kept in the department and was instead referred to the main OHRM file.

46. The Medical Services Division referred data access requests to OLA, and when directed by OLA to grant a request, redacted doctors' handwritten notes from the disclosure.

47. Another entity, the Ethics Office, indicated that in order to ensure the confidentiality of its processes, it never granted data access to any subject of an ethics review.

48. Inconsistent processes and control weaknesses in securing access to personal data expose the United Nations Secretariat to the risks of weakened reliance and loss of control on the part of the data subjects on the information systems and processes of the Organization.

### **Recommendation 13**

**(13) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Department of Management and the Office of Legal Affairs, develops norms and conditions regulating staff members' access to their own data, stored in the various files databases and archives of the Organization.**

49. *EOSG did not provide a specific response to recommendation 13 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy. Recommendation 13 remains open pending promulgation of consistent procedures for regulating staff members' access to their own personal data.*

### **G. Accuracy of personal data**

The Secretariat does not have a comprehensive policy or process for identifying and correcting data inaccuracies that could harm individuals

50. Controls and processes should be in place to ensure that personal data is accurate and complete.

51. This area is partially regulated in the Secretariat by the provisions established in ST/AI/292 "Filing of adverse material in personnel records", and ST/AI/354 "Request for rectification of date of birth or of other personal data". These provisions, however, do not automatically extend to the numerous repositories of personal data that have been developed through the years, such as IMIS, Galaxy, Financial Disclosure, and the Medical Database. Many of these

---

repositories contain personal data needed in case of emergency situations (home address, emergency contacts, etc.).

52. The accuracy of personal data is critically important to prevent the risks associated with decisions made on the basis of inaccurate data. The absence of clear terms of reference regulating the process for identifying and correcting inaccurate personal data constitute a serious deficiency that could impact on the safety or welfare of individuals.

#### **Recommendation 14**

**(14) The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in collaboration with the Office of Legal Affairs, defines the Secretariat's standards, responsibilities, and procedures for the correction and revision of personal data.**

53. *EOSG did not provide a specific response to recommendation 14 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy.* Recommendation 14 remains open pending documentation of standards, responsibilities and procedures for the correction and revision of personal data.

## H. Security of personal data

### Lack of ICT security policies and guidelines

54. Information security, particularly the assurance of data confidentiality, is necessary to assure privacy of personal data.

55. From a privacy perspective, the most relevant policies regulating the security of data in the Secretariat are as follows:

(a) ST/SGB/2004/15 – “Use of information and communication technology resources and data”, defining the terms of reference for the use and monitoring of information technology and related resources and data;

(b) ST/SGB/2007/5 – “Record-keeping and the management of United Nations archives”, defining the terms of reference for records, archives, electronic records, and access of staff members to non-current records;

(c) ST/SGB/2007/6 – “Information sensitivity, classification and handling”, defining the terms of reference for the classification and secure handling of confidential information entrusted to or originating from the United Nations; and

---

(d) In DFS, a series of policies and procedures being developed by the Information and Communication Technology Division, in accordance with the international standard for information security management (ISO 27001). Many of these policies address security controls relevant to data privacy.

56. The Secretariat needs to consolidate in one policy the security requirements for information and communications technologies to ensure clear terms of reference for both system-wide and Department-specific applications.

### **Recommendation 15**

**(15) The Office of Information and Communications Technology should develop a Secretariat information security policy and guidelines in accordance with established security international standards and best practices.**

57. *OICT accepted recommendation 15 and stated that the ICT strategy (A/62/793 and Corr. 1) had been endorsed by the General Assembly in December 2008 and OICT was established in February 2009. As part of the implementation of the ICT strategy, a new governance structure is in the process of being established. The Secretariat information security policy will be developed in coordination with all relevant departments and offices. The implementation of this recommendation is thus dependent on the adoption of the new ICT governance model and the active participation of all the major stakeholders. However, OICT estimates that the Secretariat information security policy can be developed by mid-2010.* Recommendation 16 remains open pending receipt of an information security policy and guidelines.

### Inadequate controls and procedures for secure communications and electronic recordkeeping

58. The local and metropolitan area networks (LAN and MAN) supporting the core electronic repositories of the Organization are managed by OICT (formerly Information Technology Services Division, ITSD) at Headquarters, New York. LAN and MAN have been certified in 2006 to be in compliance with the international standard for information security management system ISO 27001. Since then, two yearly sustaining audit verifications have confirmed that the security system maintained its compliance with the requirements of the standard.

59. The electronic repositories and applications containing – or potentially to contain - most of the personal information pertaining to staff members and other individuals (consultants, contractors, etc.), include: (a) IMIS; (b) Financial Disclosure Programme database; (c) Galaxy system; (d) Medical Services database; (e) Document workflow applications (i.e. MARS used in DFS); and (f) Electronic messaging system (E-mail).

60. IMIS is used for human resources management, payroll, finance and accounting, requisition and funds control, budget execution and travel

---

management. The system contains personal information pertaining to all staff of the Organization, including consultants and contractors.

61. The Financial Disclosure Programme database contains the personal financial data of approximately 3,000 senior staff members, including staff involved in monetary transactions and decision making. Staff members included in these two categories are required to complete a full disclosure of their family income, assets, and investments. The database is administered, supported, and maintained by Price Waterhouse Coopers, and is physically hosted at their data centre located in Virginia.

62. The Galaxy system, used for recruiting purposes, stores approximately 1.2 million Personal History Profiles (PHPs). The system is hosted by OICT, managed by the Information and Communication Technology Division (ICTD) in DFS, and outsourced to the United Nations International Computing Centre (UNICC) for call centre and database support. The main risks to the confidentiality of this system pertain to the storage of new PHPs outside of the firewall of the United Nations Secretariat, which is a substandard security practice.

63. The Medical Services database “EarthMed”, an electronic medical records and occupational health information management system is used by approximately 50 users. In this regard, OIOS noted that:

(a) Access control policy or guidelines for the use of this application have not been developed to ensure that data and information are accessed only by those staff members that have the right and need to know; and

(b) A security risk assessment of the “EarthMed” database had never been conducted.

64. A workflow and document tracking system application (“MARS”) is used by DFS. The audit review highlighted instances where confidential code cables were stored in the application as attachments, defeating the confidential nature of the code cables.

65. The electronic messaging system (E-mail) of the Secretariat is based in the Lotus Notes environment, and is managed by OICT. OIOS noted that while the UN email system was never intended to be used as a “secure” communication system, it is indeed widely used across the Secretariat to transmit sensitive information in an un-protected manner (i.e. without encryption), including personal identifiable data. In this regard, it is important to refer the relevant requirement issued by the Secretary-General in ST/SGB/2007/5, Section 6.2, as follows:

“E-mail has become an important business and communication tool in the United Nations and many of the e-mail messages created and received by the Organization constitute records because they provide evidence of and information about its business transactions. Departments and offices shall ensure that e-mail records are identified,

---

managed and stored in accordance with the requirements for record-keeping set forth in the present bulletin. Departments and offices shall be required to develop and disseminate guidelines, in keeping with business process and practice, to prescribe appropriate use of e-mail systems as a means of official communication.”

66. The processes and controls in place for the management and use of the email system at the Secretariat are not adequate to address and support: (a) the increased need for security required by the extensive use of the system; and (b) the requirement established by the Secretary-General to ensure that the e-mail system is used as a means of official communication.

67. The extensive list of applications storing and processing personal data, the wide allocation of responsibilities for the administration and support of the various applications, and the absence of a comprehensive ICT assessment over the security of these applications expose the Organization to risks to the security and confidentiality of data.

#### **Recommendations 16 to 19**

**The Office of Information and Communications Technology should:**

**(16) Conduct a comprehensive ICT security assessment of all applications in use at the Secretariat that process and store personal data;**

**(17) Ensure that granular and unalterable “audit event logging controls” are enabled in all applications processing and storing personal data, both at the level of each application and supporting operating system;**

**(18) Develop policies and procedures to ensure periodic review and follow-up of the information contained in the audit trails generated by the applications processing and storing personal data, and their supporting operating systems; and**

**(19) Conduct a comprehensive review of the E-mail infrastructure (hardware and software), and its supporting processes and controls, with the purpose of upgrading the security of the system to meet the increased demand of the offices and the requirements established in ST/SGB/2007/5, Section 6.2.**

#### **Recommendation 20**

**(20) The Medical Services Division should conduct a review of the procedures for the use of the medical database**

---

**and develop an access control policy defining user profiles and rights.**

68. *OICT accepted recommendation 16 and stated that it supports the rationale of the recommendation but at present is not in a position to implement such a comprehensive assessment. Many applications that process and store personal data are operated by other departments and offices, and are not known to OICT. OICT would therefore rely on the unit charged with the responsibility for data privacy to create a prioritized inventory of all such applications and to initiate an ICT security assessment. In addition, unless additional resources are made available, OICT can only provide a general methodology for and limited assistance with these ICT security assessments. In OIOS' opinion, OICT is the custodian of the data and should drive an ICT security assessment initiative of all applications in the Secretariat in this capacity, in collaboration with all departments and offices. Recommendation 16 remains open pending an ICT security assessment of applications within the UN secretariat.*

69. *OICT accepted recommendation 17 and stated that it appreciates the rationale for this recommendation but foresees significant operational difficulties for its implementation. In addition, due to the fragmented nature of responsibility over these applications (see above), it may not be technically feasible to implement such controls on all applications, particularly in the case of legacy systems. As part of the individual ICT security assessment the feasibility of such controls will need to be evaluated and suitable measures will be identified where possible. OICT will also ensure that this recommendation is implemented in all new systems that process and store personal data most importantly the new Enterprise Resource Planning (ERP) and Enterprise Content Management (ECM) systems. OIOS acknowledges that this recommendation may not be applicable to all legacy systems. However, where possible, OICT needs to undertake an assessment of existing applications to determine whether the audit event logging controls are implementable. Therefore, recommendation 17 remains open pending an assessment of existing applications and the implementation of audit event logging controls within the Secretariat's applications.*

70. *OICT accepted recommendation 18 and stated that it will ensure that the audit trails are reviewed periodically for all systems on which such granular auditing is possible. However, the review and follow-up on a large volume of audit information requires additional resources which have to be included in the cost and support model for each system. Recommendation 18 remains open pending documentation of policies and procedures to ensure periodic review and follow-up of the information contained in the audit trails generated by the applications processing and storing personal data, and their supporting operating systems.*

71. *OICT accepted recommendation 19 and stated that the estimated target date for implementation of the recommendation is December 2010 on the basis of current work priorities and resource availability. Recommendation 19 remains open pending the comprehensive review of the email infrastructure (hardware and software), and its supporting processes and controls, with the purpose of*

---

upgrading the security of the system to meet the increased demand of the offices and the requirements established in ST/SGB/2007/5, Section 6.2.

72. *DM accepted recommendation 20 and stated that from the Medical Services Division's point of view, the audit observations are reasonable. The Division has an access control policy, based on roles and responsibilities of medical staff that access the system. This policy is currently not a written one, but a practical one (with roles defined within the system according to job requirements, and access to users granted according to those roles). Medical Services Division intends to include the access control policy in the system manual which is currently at a draft stage. Recommendation 20 remains open pending formalization of the access control policy and system manual by the Medical Services Division.*

Handling, custody, and sharing of personal identifiable data and documentation (i.e. national passports, Laissez-Passer, and visa request forms)

73. The procedures followed for the issuance and renewal of visas and official travel documentation (i.e. Laissez-Passer) requires that the Travel and Transportation Section (TTS) in DM collect and share personal identifiable data (PID) and documents (i.e. national passport, visa request forms) of staff members and their dependants. OIOS noted that the handling of these documents during the processing period exposes personal information to potential risks of loss of confidentiality. This condition was particular evident in the modalities adopted for storing the documentation (i.e. national passports, Laissez-Passer, visa request forms) in easily accessible file cabinets within TTS premises.

**Recommendation 21**

**(21) The Travel and Transportation Section should develop internal procedures and guidelines for handling personal documentation, including requirements to ensure that all documents containing personal identifiable data (i.e. national passports, Laissez-Passer, and completed visa requests forms) are stored in safe-locked containers.**

74. *DM accepted recommendation 21 and stated that TTS has standard operating procedures for handling Laissez-Passer documents, including the proper storage of these documents. TTS acknowledges the value of this recommendation and will formalize these guidelines into a documented standard procedure for all passport and visa processes. Recommendation 21 remains open pending documentation and implementation of standard operating procedures for handling personal documentation in a secure manner.*

Online payments

75. The procedures adopted by the United Nations Postal Administration (UNPA) for the sale of philatelic products include online payment processes. For this function, OIOS noted that UNPA had a dedicated stand-alone desktop computer, connected through a modem, located in a shared office space within its

---

premises in the basement of the Secretariat building. The security of the online payment process has never been subject to any assessment or validation.

76. The DPI Visitors' Section operates a desk that accepts credit card payments for tours, and then prints out receipts containing full names and credit card numbers, in contravention of the data security standard issued by the Payment Card Industry (PCI), requiring that primary account numbers (PANs) are masked when displaying/printing cardholder data.

#### **Recommendation 22**

**(22) The United Nations Postal Administration, in coordination with the Office of Information and Communications Technology, should ensure that its online credit card payment procedures are in compliance with the security standard of the Payment Card Industry.**

#### **Recommendation 23**

**(23) The Department of Public Information should ensure that its credit card payment procedures are in compliance with the security standard of the Payment Card Industry.**

77. *DM accepted recommendation 22 and stated that UNPA operates its credit card payment system in line with the requirements set by the payment system provider. UNPA strictly adheres to the requirements set by the company. The system operated on a stand-alone computer with limited access by a total of 3 specifically authorized staff members. Furthermore, the system is disconnected from the modem at the end of every working day and the modem is stored in separately in a secured, locked location. In order to comply with OIOS recommendation, UNPA will request OICT to conduct a separate assessment of the data security of the system.*

78. *OICT accepted recommendation 22 and stated that it will provide the necessary technical support on request of UNPA. Recommendation 22 remains open pending documentation and implementation of procedures for the online credit card payment system, in compliance with the security standards of the Payment Card Industry.*

79. *DPI responded to recommendation 23 but did not indicate whether it accepted the recommendation. DPI stated that the Visitors' Services Cluster credit card processor "WebAuthorize" scrambles the account numbers of all credit card transactions, thus ensuring security of visitors' account information. At the time of audit, OIOS did not find evidence that DPI's online credit card payment system complied with the security standards of the Payment Card Industry. Therefore, recommendation 23 remains open pending receipt of evidence that the DPI credit card payment system complies with the security standards of the Payment Card Industry.*

---

Case management database of the Administrative Law Unit/OHRM

80. The Administrative Law Unit maintains a database of cases and processes, containing personal identifiable data, on a database application developed with Microsoft Access. OIOS noted that this database had no password protection, and did not appear to be covered by adequate security controls.

81. OIOS has already made in this report a recommendation to OICT to conduct a comprehensive ICT security assessment of all applications and databases containing personal identifiable data. Therefore, no additional recommendation is made to the Administrative Law Unit concerning the security of its database.

Inadequate controls over the nature of data and information posted on i-Seek

82. The internal web site “i-Seek” was defined as “The UN worldwide intranet...that...connects staff members at all major duty stations and peacekeeping missions. With the aim to improving usability and accessibility, as well as its use as the primary vehicle of internal communications.....”. The Outreach Division of DPI is mandated to manage overall content on i-Seek, and produces content that supports the overall internal communications strategy on the basis of defined objectives, guiding principles, and posting procedures. However, OIOS found that no process was established to verify and validate the nature of data and information published on i-Seek to safeguard their confidentiality and security. Indeed, in one case, the Organization inadvertently posted names and index numbers of staff members that had participated in a Staff Union petition.

**Recommendation 24**

**(24) The Department of Public Information should assign clear responsibilities and develop procedures for the prior verification and validation of the nature of data and information to be posted on i-Seek.**

83. *DPI responded to recommendation 24 but did not indicate whether it accepted the recommendation. DPI stated that the recommendation should not be limited to DPI because the Department was not responsible for all content posted on i-Seek - just DPI pages and the start page. Other departments and offices are responsible for their own pages. OICT should provide DPI with tools to be able to verify and validate information posted on i-Seek. At this time, DPI is not able to identify who posts announcements. In OIOS’ opinion, DPI and OICT should take the lead and document procedures to ensure prior verification and validation of data that gets posted on i-Seek. Therefore, recommendation 24 remains open pending documentation of procedures for prior verification and validation of data before being posted on i-Seek.*

---

Security controls of web sites and mailing lists linked to the main UN Internet domain [www.un.org](http://www.un.org)

84. OIOS' review of the main public web site ([www.un.org](http://www.un.org)) of the United Nations Secretariat indicated the following control weaknesses that could expose the Organization to risks to security and confidentiality of data and information:

(a) The main public web site “[www.un.org](http://www.un.org)” is directly linked to over 200 accounts posting data in the UN site (using the insecure File Transferring Protocol). Only 20 of these external web sites are directly managed by DPI. This condition exposed the UN to the risk of inadvertently posting confidential data and information that have not been verified and confirmed;

(b) There were no documented policies for managing, updating, monitoring, and securing mailing lists. This condition exposed the UN to the risk of distributing confidential data and information through un-monitored mailing lists;

(c) A privacy disclaimer is posted only on the main web page and is not consistently presented in other pages/levels of the site; and

(d) There were no procedures to control and coordinate the registration of Internet domains outside the main [www.un.org](http://www.un.org) domain (e.g. UNPA/DESA; UNIFEM; Cyber school bus; United Nations News.com). This condition exposed the UN to the risk of inconsistent implementation of security controls and presentation requirements.

**Recommendation 25**

**(25) The Department of Public Information, in collaboration with the Office of Information and Communications Technology, should ensure that adequate procedures and controls are implemented to verify and confirm the security of all UN web sites and mailing lists directly linked to the main UN domain.**

85. *DPI accepted recommendation 25 and stated that adequate procedures and controls were already being implemented. OICT also accepted recommendation 25 and stated that it will provide the necessary technical support on request of the DPI. Recommendation 25 remains open pending evidence of procedures and controls implemented to verify and confirm the security of UN websites and mailing lists.*

**I. Disclosure of personal data to third parties**

86. Controls pertaining to the sharing of personal data are essential to minimize the risk of a security breach, particularly when data is disclosed to organizations outside the United Nations system. These controls include two

---

practices: limiting what is disclosed, and assuring the security of non-United Nations entities authorized to access United Nations data.

87. The Secretariat does not have a policy and procedures for assuring the security of non-United Nations entities accessing, receiving, or hosting personal data of United Nations staff. Data disclosures with third parties are taking place. For example, OHRM distributes to Member States a directory of United Nations staff for the purposes of supporting Member States' oversight needs regarding proper representation among United Nations staff. Most critically, the United Nations has outsourced the maintenance of the system containing perhaps its largest store of its personal data – DFS's Nucleus, which contains over 1 million records – to a company based in Guatemala City that has never undergone a site assessment. On a positive note, the Ethics Office has enlisted the help of OICT to conduct a security assessment of the processes implemented in support of the Price Waterhouse Coopers' Financial Disclosure Programme database, hosted in Virginia.

88. Other examples of risks pertaining to the disclosure of personal data with third parties included:

(a) The frequent requests made to the Medical Services Division to release medical information of staff members. The Division has been following the practice of seeking on a case-by-case basis the authorization of OLA in response to each request; and

(b) Two Units of DFS (Conduct and Discipline Unit, and MOU & Claims Management Section) did not have criteria and procedures to support and guide their staff when sharing sensitive information.

89. The lack of adequate controls in this area exposes the Secretariat to the risks of personal data being shared with third parties that have substandard security practices, and consequently, to breaches of data confidentiality.

#### **Recommendations 26 to 29**

**The Executive Office of the Secretary-General should ensure that:**

**(26) The unit charged with the new responsibilities for data privacy, in coordination with the Office of Legal Affairs, defines a policy for regulating the modalities for sharing with, or granting access to, non-United Nations entities personal data related to United Nations staff members;**

**(27) The unit charged with the new responsibilities for data privacy documents standard requirements and procedures for assuring the security of third-party data processors;**

---

**(28) The unit charged with the new responsibilities for data privacy, in coordination with the Medical Services Division and the Office of Legal Affairs, develops standard procedures to address the requests for release of medical information pertaining to staff members; and**

**(29) The unit charged with the new responsibilities for data privacy, in coordination with the Department of Field Support and the Office of Legal Affairs, develops a procedure for sharing sensitive information about the cases handled by the Conduct and Discipline Unit and the MOU & Claims Management Section.**

90. *EOSG did not provide specific responses to recommendations 26, 27, 28 and 29 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy.*

91. Recommendation 26 remains open pending documentation of a policy for regulating the modalities for sharing or granting non-United Nations entities access to personal data related to United Nations staff members.

92. Recommendation 27 remains open pending documentation of standard requirements and procedures for assuring the security of third-party data processors.

93. Recommendation 28 remains open pending the development of standard procedures to address the requests for release of medical information pertaining to staff members.

94. Recommendation 29 remains open pending documentation of a procedure for sharing sensitive information about the cases handled by the Conduct and Discipline Unit and the MOU & Claims Management Section.

## J. Monitoring and enforcement of privacy policies

### Absence of a central point of contact for privacy-related issues

95. The discipline of monitoring and enforcing privacy policies ensures that policies are taken seriously, policy gaps are steadily reduced, and privacy complaints are resolved. A robust enforcement programme is essential for effecting a widespread cultural change on data privacy.

96. The United Nations Secretariat has not yet conducted a comprehensive assessment of all of its privacy practices, nor has it adopted an annual or biannual commitment to renew such an assessment. Indeed, this audit is a first attempt at assessing the privacy practices of the Secretariat in handling personal data.

97. The Secretariat does not maintain or publicize a central phone number, e-mail address, or postal address for data subjects to contact with privacy-related

---

questions and concerns or for United Nations staff to report suspected privacy breaches. The Secretariat also does not appear to have a documented process for responding to such inquiries and reports.

98. The Secretariat does not enforce a “clean desk” policy - that is, requiring staff to lock away sensitive documents when their desk is unattended - in a consistent manner. Only in one case – DPI Sales and Marketing – did OIOS find that such a policy was enforced.

99. There does not appear to be any documented guidance within the Secretariat on what is an appropriate sanction for staff violations of privacy.

100. Inadequate monitoring procedures expose the Secretariat to the risk of privacy breaches and exposures going undetected, with consequent loss of confidentiality and damage to the reputation of the Organization.

### **Recommendations 30 to 32**

**The Executive Office of the Secretary-General should ensure that:**

**(30) The unit charged with the new responsibilities for data privacy, in coordination with the Office of Information and Communications Technology and the Office of Legal Affairs, defines a central point of contact for privacy inquiries and reports, documents a response process, and trains relevant personnel on the process;**

**(31) The unit charged with the new responsibilities for data privacy develops a policy defining requirements for the safekeeping of sensitive documents; and**

**(32) The unit charged with the new responsibilities for data privacy, in coordination with the Office of Legal Affairs, documents and disseminates guidelines on which types of privacy abuses and violations would be subject to the UN’s standard disciplinary process.**

101. *EOSG did not provide specific responses to recommendations 30, 31 and 32 but accepted the summary findings in the report, stating that the United Nations needs a better system of control to ensure adequate management and protection of data privacy. OICT also accepted recommendation 30 and stated that it will provide the necessary technical support on request of EOSG.* Recommendation 30 remains open pending identification of a central point of contact for privacy inquiries and reports; the documentation of a response process; and the training of relevant personnel on the process.

102. Recommendation 31 remains open pending the development of a policy defining requirements for the safekeeping of sensitive documents.

---

103. Recommendation 32 remains open pending the documentation and dissemination of guidelines on which types of privacy abuses and violations would be subject to the United Nations' standard disciplinary process.

## V. ACKNOWLEDGEMENT

104. We wish to express our appreciation to the Management and staff of all Departments and Offices involved in the audit for the assistance and cooperation extended to the auditors during this assignment.

## STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
1.	The Secretary-General should assign to a new or existing Secretariat unit the responsibility to develop and manage a comprehensive data privacy programme for the Secretariat.	Governance	High	O	Provide formal evidence documenting the allocation of responsibility to develop and manage a comprehensive data privacy programme for the United Nations Secretariat to OICT.	Not provided
2.	The Secretary-General should Establish a Data Privacy Steering Committee comprising representatives of Departments and Offices with sufficient authority to establish privacy requirements and provide guidance for implementing related internal controls.	Governance	High	O	Provide formal evidence documenting the establishment of a Data Privacy Steering Committee comprising representatives of Departments and Offices.	Not provided
3.	The Executive Office of the Secretary-General should ensure that the Organizational unit charged with the new responsibilities for data privacy identify all data classification schemes in use within the United Nations Secretariat and propose their replacement with a common, detailed classification scheme based on the general categories listed in ST/SGB/2007/6.	Governance	High	O	Provide formal evidence documenting the development and dissemination of a Secretariat-wide data privacy policy.	Not provided
4.	The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy identifies all data classification schemes in use within the United Nations Secretariat and proposes their replacement with a common, detailed classification scheme based on the general categories	Compliance	Medium	O	Provide formal evidence documenting the identification of all data classification schemes in use within the Secretariat and the development of a common classification scheme based on ST/SGB/2007/6.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	listed in ST/SGB/2007/6.					
5.	The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with Department of Management, undertakes activities to sensitize and train staff in United Nations data privacy requirements.	Human Resources	Medium	○	Provide formal evidence documenting the development of activities to sensitize and train staff on United Nations Secretariat's data privacy requirements.	Not provided
6.	The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with heads of Departments and Offices, define a standard "Privacy Notice", indicating the terms of reference for the collection, use, security, sharing, and disposing of personal identifiable data within the Organization.	Governance	Medium	○	Provide formal evidence documenting the promulgation of a standard "Privacy Notice", indicating the terms of reference for the collection, use, security, sharing, and disposing of personal identifiable data within the Organization.	Not provided
7.	The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with heads of Departments and Offices, develops procedures to catalog all forms used to collect personal identifiable data in the United Nations, whether manually or electronically generated. Each form should be complemented by a "Privacy Notice", indicating the terms of reference for the collection, use, security, sharing, and disposing of personal identifiable data within the Organization.	Governance	Medium	○	Provide formal evidence documenting the development of procedures to catalog all forms used to collect personal identifiable data at the United Nations Secretariat, whether manually or electronically generated	Not provided
8.	The Executive Office of the Secretary-General should ensure that the unit charged	Information Resources	Medium	○	Provide formal evidence documenting the review of all United Nations Secretariat	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	with the new responsibilities for data privacy, in coordination with the Department of Public Information, the Office of Legal Affairs, and the Office of Information and Communications Technology, conducts a review of all United Nations public web sites and ensures that a privacy notice is posted on each such site.				public websites and the posting of a privacy notice on each such site.	
9.	The Department of Public Information should ensure that the online media accreditation site contains a privacy notice regarding the purpose and use of the data collected through that site.	Information Resources	Medium	○	Provide formal evidence documenting the posting of a privacy notice on the online media accreditation site regarding the purpose and use of the data collected.	Not provided
10.	The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Office of Legal Affairs, conducts an analysis to determine those instances where the Secretariat should capture and record the consent of its data subjects, and direct the relevant offices to do so.	Information Resources	Medium	○	Issuance of appropriate directions to relevant offices regarding recording of consent of their data subjects.	Not provided
11.	The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with heads of Departments and Offices, defines a process and criteria to identify the specific needs for personal identifiable data collected through forms and databases to avoid the collection of unnecessary personal data.	Information Resources	Medium	○	Provide formal evidence documenting the promulgation of procedures and criteria to identify the specific needs of the United Nations department and offices for personal identifiable data, to be collected through forms and databases, and to avoid collecting unnecessary personal data.	Not provided
12.	The Executive Office of the Secretary-	Information	Medium	○	Provide formal evidence documenting the	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Archives and Records Management Section, includes in its guidelines for records retention schedules, instructions for identifying and marking records containing private data that are no longer needed, which should be disposed of.	Resources			promulgation of instructions for identifying and marking records containing private data that are no longer needed and that should be disposed of.	
13.	The Executive Office of the Secretary-General should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Department of Management and the Office of Legal Affairs, develops norms and conditions regulating staff members' access to their own data, stored in the various files databases and archives of the Organization.	Governance	Medium	O	Provide formal evidence documenting the promulgation of consistent procedures for regulating staff members' access to their own personal data.	Not provided
14.	The Executive Office of the Secretary General should ensure that the unit charged with the new responsibilities for data privacy, in collaboration with the Office of Legal Affairs, defines the Secretariat's standards, responsibilities, and procedures for the correction and revision of personal data.	Governance	Medium	O	Provide formal evidence documenting standards, responsibilities and procedures for the correction and revision of personal data.	Not provided
15.	The Office of Information and Communications Technology should develop a Secretariat information security policy and guidelines in accordance with established security international standards and best practices.	Governance	Medium	O	Provide formal evidence documenting an information security policy and guidelines.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
16.	The Office of Information and Communications Technology should conduct a comprehensive ICT security assessment of all applications in use at the Secretariat that process and store personal data.	Information Resources	Medium	O	Provide formal evidence documenting the ICT security assessment of applications within the United Nations Secretariat.	Not provided
17.	The Office of Information and Communications Technology should ensure that granular and unalterable “audit event logging controls” are enabled in all applications processing and storing personal data, both at the level of each application and supporting operating system.	Information Resources	Medium	O	Provide formal evidence documenting the assessment of existing applications and the implementation of audit event logging controls within the United Nations Secretariat applications.	Not provided
18.	The Office of Information and Communications Technology should develop policies and procedures to ensure periodic review and follow-up of the information contained in the audit trails generated by the applications processing and storing personal data, and their supporting operating systems.	Information Resources	High	O	Provide formal evidence documenting policies and procedures to ensure periodic review and follow-up of the information contained in the audit trails generated by the applications processing and storing personal data, and their supporting operating systems.	Not provided
19.	The Office of Information and Communications Technology should conduct a comprehensive review of the E-mail infrastructure (hardware and software), and its supporting processes and controls, with the purpose of upgrading the security of the system to meet the increased demand of the offices and the requirements established in ST/SGB/2007/5, Section 6.2.	Information Resources	Medium	O	Provide formal evidence documenting a comprehensive review of the e-mail infrastructure (hardware and software), and its supporting processes and controls, with the purpose of upgrading the security of the system to meet the increased demand of the offices and the requirements established in ST/SGB/2007/5, Section 6.2.	Not provided
20.	The Medical Services Division should conduct a review of the procedures for the	Information Resources	Medium	O	Provide formal evidence documenting formalization of the access control policy	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	use of the medical database and develop an access control policy defining user profiles and rights.				and system manual of the Medical Services Division.	
21.	The Travel and Transportation Section should develop internal procedures and guidelines for handling personal documentation, including requirements to ensure that all documents containing personal identifiable data (i.e. national passports, Laissez-Passer, and completed visa requests forms) are stored in safe-locked containers.	Governance	Medium	○	Provide formal evidence documenting the standard operating procedures for handling personal documentation in a secure manner.	31 December 2009
22.	The United Nations Postal Administration, in coordination with the Office of Information and Communications Technology, should ensure that its online credit card payment procedures are in compliance with the security standard of the Payment Card Industry.	Compliance	Medium	○	Provide formal evidence documenting the implementation of procedures for the online credit card payment system in compliance with the security standards of the Payment Card Industry.	31 December 2009
23.	The Department of Public Information should ensure that its credit card payment procedures are in compliance with the security standard of the Payment Card Industry.	Compliance	Medium	○	Provide formal evidence demonstrating that the DPI credit card payment system complies with the security standards of the payment card industry.	Not provided
24.	The Department of Public Information should assign clear responsibilities and develop procedures for the prior verification and validation of the nature of data and information to be posted on i-Seek.	Governance	Medium	○	Provide formal evidence documenting the implementation of procedures for the prior verification and validation of data before being posted on iSeek.	Not provided
25.	The Department of Public Information, in collaboration with the Office of Information and Communications	Governance	Medium	○	Provide formal evidence documenting the implementation of procedures and controls to verify and confirm the security of UN	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	Technology, should ensure that adequate procedures and controls are implemented to verify and confirm the security of all UN web sites and mailing lists directly linked to the main UN domain.				websites and mailing lists.	
26.	The EOSG should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Office of Legal Affairs, defines a policy for regulating the modalities for sharing with, or granting access to, non-United Nations entities personal data related to United Nations staff members;	Governance	Medium	○	Provide a formal policy for regulating the modalities for sharing or granting non-United Nations entities access to personal data related to United Nations staff members	Not provided
27.	The EOSG should ensure that the unit charged with the new responsibilities for data privacy documents standard requirements and procedures for assuring the security of third-party data processors.	Governance	High	○	Provide formal evidence documenting standard requirements and procedures for assuring the security of third-party data processors.	Not provided
28.	The EOSG should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Medical Services Division and the Office of Legal Affairs, develops standard procedures to address the requests for release of medical information pertaining to staff member.	Governance	Medium	○	Provide formal evidence documenting the development of standard procedures to address the requests for release of medical information pertaining to staff members.	Not provided
29.	The EOSG should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Department of Field Support and the Office of Legal Affairs, develops a procedure for sharing sensitive information about the cases handled by the Conduct and	Governance	Medium	○	Provide formal evidence documenting a procedure for sharing sensitive information about the cases handled by the Conduct and Discipline Unit and the MOU & Claims Management Section.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	Discipline Unit and the MOU & Claims Management Section.					
30.	The EOSG should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Office of Information and Communications Technology and the Office of Legal Affairs, defines a central point of contact for privacy inquiries and reports, documents a response process, and trains relevant personnel on the process.	Governance	High	O	Provide formal evidence documenting the identification of a central point of contact for privacy inquiries and reports; the documentation of a response process; and the training of relevant personnel on the process.	Not provided
31.	The EOSG should ensure that the unit charged with the new responsibilities for data privacy develops a policy defining requirements for the safekeeping of sensitive documents.	Governance	Medium	O	Provide formal evidence documenting the development of a policy defining requirements for the safekeeping of sensitive documents.	Not provided
32.	The EOSG should ensure that the unit charged with the new responsibilities for data privacy, in coordination with the Office of Legal Affairs, documents and disseminates guidelines on which types of privacy abuses and violations would be subject to the United Nations standard disciplinary process.	Governance	High	O	Provide formal evidence of the documentation and dissemination of guidelines on which types of privacy abuses and violations would be subject to the United Nations' standard disciplinary process.	Not provided

1. C = closed, O = open

2. Date provided by EOSG, OICT, DPI and DFS in response to recommendations.