Treasury Board of Canada
Secretariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Privacy Impact Assessment Summary for PeopleSoft Human Resources Management System

Published: 2010-00-07

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board, 2010

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT43-188/2010E-PDF
ISBN: 978-0-660-25546-0

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Sommaire de l’évaluation des facteurs relatifs à la vie privée du
Système de gestion des ressources humaines PeopleSoft

1. Purpose

This document facilitates the review of the Privacy Impact Assessment (PIA) prepared on the PeopleSoft Human Resources Management System (HRMS) as Operated by Treasury Board Secretariat, supporting human resources in the Central Agency Cluster (CAC) departments. It provides context, highlighting key points that show how privacy considerations have been factored into the design, development and implementation of the PeopleSoft HRMS. It then reviews the three privacy risk areas, the recommendations to address them, and outlines steps being taken to implement them.

This PIA focuses on the assessment of personal information collected, used, disclosed and retained in the CAC PeopleSoft system. It does not encompass HR-related information that exists outside of the system, nor does it depict information within the system that is not considered 'personal' as per the *Privacy Act*.

2. Description – PeopleSoft Human Resources Management System

The scope of this PIA is limited to PeopleSoft v8.9 as implemented by the Treasury Board Secretariat for the CAC. PeopleSoft is installed in a Protected B enclave at the Treasury Board Secretariat (TBS) and serves users at Treasury Board Secretariat (TBS), Department of Finance (FIN), Canada School of the Public Service (CSPS) and Privy Council Office (PCO). The GC HRMS 'vanilla' version has been installed, with minimal customizations. At the present time only certain modules are being used: Position Management; Workforce Administration; Base Benefits; Labour Administration, Enterprise Learning (2 pages), Employee Self Service. In addition, there are four custom modules: Security; Pay Card; Records Management; and, Benefit Information.

The Corporate Services Sector is responsible for the day-to-day operation, security and maintenance of the PeopleSoft system. The Corporate Services Sector, which had been a shared service between TBS and FIN, has been split into separate Corporate Services branches for TBS and FIN. The responsibility for supporting PeopleSoft for the Central Agency Cluster will reside in the TBS Corporate Services Sector. Within Corporate Services Sector the Human Resources Information Management (HRIM) Unit is responsible for the day-to-day functional side of the business and the Information Technology Division (ITD) of the Information Management and Technology Directorate is responsible for technical services and technical support.

This instance of PeopleSoft has a self-service module (LSS) that provides leave, benefit, employment and personal information. It should be noted that there has been a conscious effort over the last several years by the CAC to remove customizations and return to the Core GC "vanilla" version of PeopleSoft.

At the present time there are approximately 5,400 self-service accounts administered in CAC PeopleSoft for the partner organizations. In addition historical records are maintained for approximately 21,000 people.

3. Why the PIA was Necessary

This PIA is part of a process to incorporate privacy requirements into the development of systems being deployed in the Government of Canada. CAC has been using PeopleSoft since 1994 and upgraded to version 8.9 in December 2008. Because there is no PIA on file for PeopleSoft and because v.8.9 has some different functionality, TBS decided to conduct a PIA at this time. This PIA is based on current information and reflects the situation as of June 2009.

The implementation of the upgrade to PeopleSoft v8.9 did not require that any new information be collected and captured by any new Personal Information Banks (PIBS).

4. PIA Objectives

- To assess whether privacy considerations have been adequately factored into the development and delivery of this human resources management system.
- To resolve any privacy issues that may be of potential public concern (i.e. employees and individuals performing services for the departments).

5. PIA Findings

One privacy risk considered high and two risks considered moderate in severity were identified. Recommendations and initiatives that are either planned or underway to address these risks are highlighted in the final section of this summary document.

6. Current PeopleSoft Data Holdings

This PIA involved an analysis of the flow of personal information as defined in the *Privacy Act*. It identified that current personal information held in PeopleSoft falls into four Clusters: Person; Employment Equity; Grievance; and, Identification and Building Pass Cards. Transfers in or out of the Protected B enclave and network are done only through the secured FTP process. The analysis is summarized in the following table:

Description of Personal Information Cluster	Collected by	Type of Format (e.g. paper, electronic)	Used by	Purpose of Collection	Disclosed to	Storage or Retention site
"Person" Cluster. Personal fields are: Name, EmplID, PRI, First Official Language, Linguistic Status, home address,	Collected by HR staff or manager and passed to HR staff who enters it into PeopleSoft.	Paper	HR: staffing, labour relations, compensation. HR compensation are the ones who would modify any personal information. Security staff	HR administration.	CHRO (TBS) for PCIS purposes in accordance with *Public Service Employment Act*.	PeopleSoft database

telephone number.						
Employment equity Cluster. Personal fields are: Disability code, Visible minority code, Aboriginal code	One person (the ‘Monitoring Officer’) is designated to receive the Questionnaire from each employee.	Employee fills in a paper questionnaire. Monitoring officer enters into PeopleSoft	HR Planning.	HR for policy and planning purposes and for statistical purposes to fulfill the government’s employment equity program. (*Public Service Labour Relations Act, formerly Public Service Staff Relations Act*)	CHRO (TBS)	PeopleSoft database
Grievances Cluster Personal fields are: Description: (of grievance) Grievance Step: Resolution Comments: (of grievance)	HR Labour Relations	Data entered into PeopleSoft varies from only the aggregate data about the grievance to details on the grievance and settlement, from paper documents.	HR Labour Relations staff.	To administer the grievance process.	Not disclosed	PeopleSoft database
Identification and Building Pass Cards Additional fields are: Name, EmplID, RCMP print checks, CSIS Assessments, Credit checks	Security Services	Data entered by Security Services staff from paper documents	Security Services	To administer security for TBS, FIN, CSPS	Not disclosed	PeopleSoft database.

7. Use of Personal Information

The PIA looked at whether PeopleSoft information would be used in a manner consistent with the *Privacy Act*. Information will be used internally for administration and management of personnel. These uses are consistent with the purpose for which employee information was originally collected.

8. Accuracy of Personal Information

PeopleSoft records data collected from human resources records and information. Through self-service all employees of CAC (c. 5,400) have access to view their own personal information, leave balances, job records, etc. Self-Service permits employees to modify certain personal information such as address, phone number. For other information employees can contact an HR professional to identify errors or omissions and will see changes, if and when made, through self-service.

9. Access to Information through PeopleSoft

The PeopleSoft 8.9 application operates on Role Based Access Controls (RBAC). Roles are created based on a "need to know", "right to know" basis and are updateable only by the 4 ITD staff. Each role contains permissions (rights) to access information specific to the job function being performed. Roles are granted by the HRIM Help Desk's Security Administrators.

The Security Administrators on the Help Desk team in HRIM receive PeopleSoft access request forms from users in the client departments. These forms are signed by the user's supervisor and indicate the access roles the individual is to be given. Various audit reports are available for the HRIM security administrator to confirm the movement of individuals, either within HR or to outside HR. Notification to the HRIM Security Administrator of a change or termination of the role of a PeopleSoft user is the manager's responsibility. No data is purged from the data base. Access accounts are removed within 7 days after an employee is terminated in the system. Personal and job information remains in the system.

10. Training, Communications and Information for PeopleSoft Users

Since information will be directly accessible to users through PeopleSoft, they will need guidance on their responsibilities to use and protect employee information under the *Privacy Act*. This will be accomplished through:

- Including information about the *Privacy Act* on the PeopleSoft sign-in page and in training materials.
- Requiring individuals to whom the tool is deployed to accept their responsibilities in accordance with the *Privacy Act*.
- Advising end users of the consequences of non-compliance.

11. Security Management

System security was considered satisfactory based on the Threat and Risk Assessment that was previously conducted. All users have the necessary clearance to access Protected B information.

12. Risk Summary

This PIA identifies three areas of risk with respect to privacy requirements for the PeopleSoft v8.9 Human Resources Management System. One is assessed as a high-level risk and two as medium-level risks. These risks are impacted by the structure of the Central Agency Cluster and the associated split in departmental responsibilities, and the mandate to work with the GC "vanilla" version of PeopleSoft. A further risk is associated with the recent split of the Department of Finance Corporate Services Branch, moving responsibility and accountability for operating the PeopleSoft system to Treasury Board Secretariat. These areas of risk along with mitigation recommendations are:

1. **Authorization of PeopleSoft users (high-level risk)**
    - Implementing a program for control of users such that a single point of contact in each partner organization is named for authorizing and removing users
    - Human Resources Information Management (HRIM) security administrators regularly utilizing audit reports to ensure appropriate role based access
    - Providing employees with ATIP training on handling of personal information.
2. **Accountability and performance measurement (medium-level risk)**

    TBS HR to:

    - Ensure that the accountability of the program custodian of personal information has been documented. This accountability could be documented, for example, in TBS HR policy and procedures manuals. The reference to the custodian should be by title rather than name.
    - Develop and document performance requirements for the custodian of personal information.
    - Arrange for audits of compliance with privacy requirements with TBS's Audit and Evaluation Branch. These should take place every two years, or as required if there is a breach of privacy requirements.
3. **Procedures and documentation (medium-level risk)**

    CAC HR to:

    - Review person-to-person procedures and electronic processes for the collection of personal information and ensure that the documentation of the purpose and authority for the collection of personal information, and consent, are consistent across all collection processes.

    Present participants, their designates, or replacements to:

    - Continue to participate in discussions between GC HRMS users and the Office of the Chief Human Resources Officer (TBS) regarding the retention and disposition of personal information with a view to reaching an early resolution to this issue.

An additional point for consideration and follow-up was identified:

Openness

- Treasury Board policy requires that, at a minimum, a summary of the PIA be made available to the public, preferably on the Department's website.
- The full PIA will be shared with the CAC partner organizations and with the PeopleSoft Cluster members through the Program Centre once the document is finalized.