Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Canada

Serving GOVERNMENT, serving CANADIANS.

Final Report

Audit of Selected PSPC Programs' Management of Personal Information

Office of the Chief Audit Executive

Table of Contents

Introduction 1
Focus of the audit 2
Statement of conformance 2
Observations 3
Internal controls were in place in selected sectors for the collection, use, disclosure, retention, safeguard, and disposal of personal information. 3
Awareness of the definition of personal information could be improved. 3
Guidelines on updating privacy impact assessments need to be implemented. 3
Guidelines on retention and disposal of personal information could be strengthened. 4
Monitoring and reporting on the effectiveness of privacy management could be strengthened 4
Conclusion 4
About the audit 5

Introduction

1. This engagement was included in the Public Services and Procurement Canada (PSPC) 2018 to 2023 Risk-Based Audit and Evaluation Plan.

2. PSPC collects and manages the personal information of individuals as part of its mandate to support other federal institutions, and as the Receiver General of Canada. Within PSPC, sectors that manage programs or activities involving the management of personal information are responsible for establishing effective controls over the collection, use, disclosure, retention, safeguarding and disposal of personal information. These sectors must therefore develop and implement effective management practices in the handling of such information.

3. The protection and handling of personal information at PSPC is governed by the Privacy Act, the associated Privacy Regulations, and Treasury Board Secretariat policies, directives, and guidelines.

4. Under the Privacy Act, personal information is defined as "information about an identifiable individual that is recorded in any form". Examples include information relating to an individual's name, address, race, education, national or ethnic origin, religion, age, marital status, criminal, financial or employment history, or a personal identification number (such as Social Insurance Number). The Privacy Act also provides individuals (such as Canadian citizens and permanent residents) with a right to access and correct personal information about themselves that is under the control of a government institution. The Privacy Act requires that federal institutions limit their collection of personal information to what directly relates to the program or activity of the institution.

5. Prior to the collection of personal information, a Privacy Impact Assessment should be completed. A Privacy Impact Assessment is a tool used to evaluate potential privacy risks for new or substantially modified programs or activities involving personal information. It is also required that assessments be revisited and updated regularly.

6. In accordance with section 10 of the Privacy Act, all personal information under the control of PSPC that is used for an administrative purpose, or that is retrievable by name or personal identifier has to be described in personal information banks. The inventory of PSPC's personal information banks and sectors managing/using the personal information is available on the PSPC Info Source on the internet. Info Source is a series of publications that provides information about the Government of Canada's functions, programs, activities and information holdings that are subject to both Access to information and Privacy Acts. The primary purpose of Info Source is to assist individuals by providing relevant information so they can exercise their rights under the Access to Information Act and the Privacy Act. The Info Source for PSPC indicates that the department has 26 institution-specific personal information banks, excluding those associated with internal services.

7. PSPC's personal information banks are related to activities such as: pay and pension administration; document imaging services for Old Age Security and Canada Pension Plan; Receiver General's deposits and payments; controlled goods registry and

industrial security clearances; supplier registration and integrity assessment program; seized property management program; and shared travel services program.

8. The Treasury Board Secretariat Directive on Privacy Practices requires federal institutions to develop retention and disposal schedules to manage their records. These schedules establish how long records will be kept before they are destroyed or transferred to the control of Library and Archives Canada.

Focus of the audit

9. The objective of this audit was to assess whether effective internal controls are in place in selected sectors of PSPC for the collection, use, disclosure, retention, safeguarding and disposal of personal information in accordance with the requirements of the Privacy Act, the Privacy Regulations, and the related Treasury Board, and departmental policies and directives.

10. The scope of the audit focused on internal controls relevant to the collection, use, disclosure, retention, safeguarding and disposal of personal information in selected PSPC sectors. The audit assessed the processes that have been implemented by PSPC from the review of the privacy management framework in June 2015 to October 2018. The audit focused on the privacy practices of the following sectors/branches:

    - Departmental Oversight Branch: 1) The Industrial Security Sector which collects and uses personal information to provide personnel screening services for individuals and industry contractor personnel working and applying to work with government institutions. 2) The Integrity Regime Renewal Sector, which uses personal information to assess supplier ineligibility to a government of Canada contract, lease, or tenant occupancy agreement, based on convictions or charges for certain offences.

    - Receiver General and Pensions Branch: 1) The Pension Sector and 2) the Government of Canada Pension Centre which collect and use a significant amount of personal information to administer the pension for the Public Service of Canada.

    - Acquisitions Program: The Services and Technology Acquisition Management Sector, Procurement Branch, is the centre of excellence for service procurements. The sector manages, on behalf of a wide range of federal organizations, the procurement processes for services.

11. More information on the audit objective, scope, approach and criteria can be found in the section "About the audit" at the end of the report.

Statement of conformance

12. The audit conforms with the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program.

13. Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the findings and conclusions in this report, and to

provide an audit level of assurance. The findings and conclusions are based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed with management. The findings and conclusions are only applicable to the entities examined and for the scope and time period covered by the audit.

Observations

14. Audit observations develop through a process of comparing criteria (the correct state) with condition (the current state). The following observations may note satisfactory performance, where the condition meets the criteria, or they may note areas for improvement, where there was a difference between the condition and the criteria.

Internal controls were in place in selected sectors for the collection, use, disclosure, retention, safeguard, and disposal of personal information.

15. Overall, we found that effective internal controls were in place for the collection, use, disclosure, retention, safeguard and disposal of personal information for the sectors reviewed.

16. More specifically, we found PSPC sectors identified the purpose for the collection, use, and disclosure of personal information, and provided notice of these purposes to the individuals. We also found personal information was limited to the information necessary and was used for the purpose it was collected. Further, we found controls were in place to ensure the accuracy of the personal information, and to protect the information from unauthorized use.

Awareness of the definition of personal information could be improved.

17. We noted the majority of employees had a good understanding of the definition of personal information, the purpose for which it was collected, and how it should be used. They were also knowledgeable about proper disclosure, safeguarding, and retention and disposal of the personal information.

18. However, it was observed that not all those managing personal information were aware the information they managed met the definition of personal information under the Act.

19. It should be noted nonetheless, the information was protected in a manner that respects the requirements for personal information.

Guidelines on updating privacy impact assessments need to be implemented.

20. Guidelines for privacy impact assessments are consistent for all programs. Departmental guidance is maintained by the Access to Information and Privacy Directorate. Although selected programs completed a privacy impact assessment for their respective programs, we noted several privacy impact assessments have not been updated in the past 10 years.

21. Although guidance for the initial assessment exists, we did not find any departmental guidelines or procedures for the periodic review and update of the assessments. It is our understanding the Access to Information and Privacy Directorate is developing procedures for updating assessments, and will be implemented in Fall 2019.

Guidelines on retention and disposal of personal information could be strengthened.

22. Retention and disposal guidelines and standards are unique to the individual personal information bank and reflect the nature of the information contained therein. We found that retention and disposal guidelines and standards existed for some PSPC personal information banks, although for other personal information banks, retention and disposal standards remained under development.

23. Further, it was observed in some areas that information was retained beyond standard retention periods.

24. It should be noted nonetheless, the information retained beyond standard retention periods remained protected in a manner that respected the requirements for personal information.

Monitoring and reporting on the effectiveness of privacy management could be strengthened

25. The Access to Information and Privacy Directorate has developed a protocol for the regular tracking and reporting of privacy breaches. While regular tracking and reporting on privacy breaches was done, we found that there was no formal mechanism in place to monitor and report on the effectiveness of privacy management.

26. We were informed the Access to Information and Privacy Directorate is considering guidelines on monitoring and reporting on the effectiveness of privacy management as part of the update of the department's privacy management framework. This framework is to be implemented in Fall 2019.

Conclusion

27. Overall, we found that effective internal controls were in place for the collection, use, disclosure, retention, safeguard and disposal of personal information for the sectors reviewed. Several administrative observations were noted.

28. There were no recommendations stemming from this audit.

About the audit

Authority
This engagement was included in the Public Services and Procurement Canada (PSPC) 2018 to 2023 Risk-Based Audit and Evaluation Plan.

Objective
The objective of this internal audit was to assess whether effective internal controls are in place in selected sectors of PSPC for the collection, use, disclosure, retention, safeguarding and disposal of personal information in accordance with the requirements of the Privacy Act, the Privacy Regulations, and the related Treasury Board, and departmental policies and directives.

Scope and approach
This audit covered the period from June 2015 to October 2018. The audit focused on internal controls relevant to the collection, use, disclosure, retention, safeguarding and disposal of personal information in selected PSPC sectors.

This audit was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Prior to the development of the terms of reference, a preliminary survey phase was conducted to gain familiarity with the subject area. This consisted of interviews with key departmental personnel involved in the management of personal information, and a review of relevant policies, processes and documentation. A risk assessment was conducted to assist the auditors in determining the audit objective and scope.

During the examination phase, in-depth interviews was conducted with key departmental personnel along with documentation review and file testing. At the end of the examination phase, the audited organization was requested to provide validation of the findings.

During the reporting phase, the audit team documented the audit findings, and conclusions. The audited organizations were provided with the audit findings, and conclusions, and were requested to review and provide comments. Comments were assessed and incorporated as relevant.

Criteria
Audit criteria were derived from the results of the detailed risk assessment, and risk areas with risk levels of medium and above. The audit criteria were developed based on the Privacy Act, and the related Treasury Board Secretariat policies and directives. The following criteria were used for the audit:

1. Personal information has been collected, used and disclosed in accordance with the identified purpose.
   - **1.1.** Selected PSPC sectors identify the purposes for the collection, use or disclosure of personal information, and provide notice of these purposes to individuals.
   - **1.2.** Collection of personal information is limited to the information necessary by the selected sectors to manage their programs.

1.3. Personal information is used for the purpose it was collected.

2. Appropriate retention and disposal schedules are in place and operating as intended.
3. Controls are in place to ensure accuracy of personal information during the period of retention.
4. Controls are in place and working effectively to safeguard personal information in paper and electronic format against unauthorized use.
5. Controls are in place to monitor and report on the effectiveness of privacy management (including controls in place for tracking and reporting on privacy breaches).

Audit work completed

Audit fieldwork for this audit was substantially completed on February 8, 2019.

Audit team

The audit was conducted by members of the Office of the Chief Audit Executive overseen by the Director of Procurement Audit, and under the overall direction of the Chief Audit Executive.

The audit was reviewed by the quality assessment function of the Office of the Chief Audit Executive.