Employment and Social Development Canada
Emploi et Développement social Canada

Unclassified

Internal Audit Services Branch

Audit of Personal Information Management for Policy Analysis, Research and Evaluation

March 2015

SP-1102-05-15E

Canada

You can download this publication by going online: publicentre.esdc.gc.ca This document is available on demand in multiple formats by contacting 1 800 O-Canada (1-800-622-6232), teletypewriter (TTY), 1-800-926-9105.

© Her Majesty the Queen in right of Canada, 2015

droitdauteur.copyright@HRSDC-RHDCC.gc.ca

PDF
Cat. No.: Em20-32/2015E-PDF
ISBN: 978-0-660-02268-0

Table of Contents

Executive Summary

Policy Analysis, Research and Evaluation (PARE) projects submissions to the Privacy and Information Security Committee (PISC) must comply with the *Privacy Act,* the *Department of Employment and Social Development Act* and the Treasury Board Secretariat (TBS) Policy on Privacy Protection[1] to approve and control the use of privileged personal information for PARE purposes. Submissions have to indicate the purpose of the PARE project, and identify data elements to be collected, accessed, disclosed, or linked as well as the users of the information. The submission, put forward by the Director General responsible for a PARE project, describes the proposed activity requiring databank connection and/or use of unmasked personal identifiers with a rationale on how the activity satisfies PARE objectives. After a PISC submission is approved by the Deputy Minister (DM), it is the responsibility of the PARE project authority to adhere to the conditions outlined in the approved submission.

Audit Objective

The objective of this audit was to determine whether policy analysts, researchers and evaluators (project authority) for PARE activities adhere to the conditions on handling, disclosing and destroying personal information, which are documented in the approved submissions.

Summary of Key Findings

- All PARE submissions to PISC identified the requirements and legislative authority for the collection and use of personal information and/or the connection of databanks.
- All PARE submissions to PISC were approved. However they were not always approved by the authority identified in the documented Databank Review Working Group (DRWG) and PISC Terms of Reference.
- Current PARE project authorities could not be easily identified when the original project authority is no longer employed by Employment and Social Development Canada (ESDC).
- There are currently no formal guidelines for the production and release of PARE data.

Audit Conclusion

The process in place for approving PARE submissions is thorough. The process, when it is followed, ensures that personal information collected and used for PARE projects is protected and properly destroyed at the end of each project. Project authorities however, do not always adhere to the conditions set out in the approved submissions.

[1] Section 6.2.15 of the TBS Policy on Privacy Protection - Establishing a privacy protocol within the government institution for the collection, use or disclosure of personal information for non-administrative purposes, including research, statistical, audit and evaluation purposes.

Recommendations

The Senior Assistant Deputy Minister of Strategic and Service Policy (SSP) Branch, in consultation with the appropriate departmental officials, should ensure that:

- All PARE submissions include a clause to inform the DRWG of cancelled projects, changes to the project authority, and confirmation when the project is completed and data destroyed.
- Departmental guidelines for managing data and databank connections in the context of PARE activities are established and communicated to all branches and regions.

1.0 Background

1.1 Context

ESDC maintains personal information about individuals which is collected and used in support of specific programs and activities in compliance with the *Privacy Act*, the *Department of Employment and Social Development Act* and the TBS Policy on Privacy Protection. Information used for PARE activities is subject to a process that masks personal identifying information before it is analyzed. This process is done to prevent the identification of individuals when undertaking approved PARE activities.

Recognizing the privacy issues relating to the use of information maintained about individuals, ESDC has implemented a strict governance approach for all PARE activities involving the connection of separate databanks and/or the use of unmasked personal identifiers.

In year 2000, the former Databank Review Committee (DRC) was established to review all PARE projects that required the connection of separate databanks and/or use of unmasked personal identifiers, and to make recommendations for such projects to the DM of the former Human Resources Development Canada. Since 2000, various changes have occurred in the process.

As a result of the creation of the PISC, the DRC was replaced by the DRWG established in June 2010 as a sub-committee of PISC to ensure that privacy is incorporated in the design and conduct of departmental PARE activities (see definitions below)[2]. The DRWG brings forward PARE submissions to PISC for consideration and recommendation for approval by the DM. The Director-level DRWG reports to the PISC and oversees the application of privacy policy and the use of personal information for PARE purposes[3]. Prior to establishing the DRWG, a similar function was performed by an informal group referred to as the Databank Review Committee Extended Secretariat. This group had similar membership as the DRWG and derived its mandate from the Governance Protocol for Conducting Policy Analysis, Research, and Evaluation Activities. Since the establishment of the DRWG and the PISC, this Protocol has not been updated and is no longer on the Department's Intranet site. A new Departmental Policy on Privacy came into effect on April 1st, 2014[4].

Submissions to PISC must comply with the requirements of the *Privacy Act*, departmental legislation and the Departmental Policy on Privacy Management. They have to indicate the purpose of the PARE project, and identify data elements to be collected, accessed, disclosed, or linked as well as the users of the information. The submission, put forward by the Director General responsible for a PARE project, describes the proposed activity requiring databank connection and/or use of unmasked personal identifiers with a rationale on how the activity satisfies PARE objectives. After a PISC submission is approved by the DM, it is the responsibility of the PARE project authority to adhere to the conditions outlined in the approved submission.

The information that is used for PARE purposes shall not be used for any administrative purpose as defined in section 3 of the *Privacy Act*. The *Privacy Act* and the *Department of Employment and Social Development Act* mandate a separate regime[5] to approve and control the use of privileged personal information for PARE purposes.

---

[2] Source: Governance Protocol for Conducting Policy Analysis, Research, and Evaluation Activities

[3] http://www.esdc.gc.ca/eng/transparency/ati/reports/annual_privacy/2011_2012/index.shtml

[4] This policy replaced the Human Resources and Skills Development Privacy Policy.

[5] Section 39 of the *Department of Employment and Social Development Act*

Each proposed PARE project must be evaluated to ensure that access to privileged personal information is required, the use of the data is permitted and that the conditions of use are set out in a submission.

Definitions of PARE

Policy Analysis	Research	Evaluation
Policy analysis is the detailed examination of the various elements that make up the policy development process from identification of the issue, defining the issue in practical terms (and in its constituent parts), identifying and assessing alternative solutions and selecting the best one.	Research is the attempt by careful scientific or technical inquiry, experimentation, study, observation, analysis, and recording to discover new facts, knowledge and information in order to develop new interpretations of facts, knowledge or information; or to discover new means of applying existing knowledge.	Evaluation, which includes monitoring and reporting activities, is the disciplined or planned, comprehensive assessment that provides information on: relevant and objective information on a policy's or program's overall effectiveness, efficiency, results, and impacts against its objectives; the continued relevance of policies and programs; and opportunities using alternative and more cost-effective policy instruments or program delivery mechanisms to achieve the objectives.

1.2 Audit Objective

The objective of this engagement was to determine whether policy analysts, researchers and evaluators (project authority) for PARE activities adhere to the conditions on handling, disclosing and destroying personal information, which are documented in the approved submissions.

1.3 Scope

The audit focused on PARE projects undertaken since 2008 in order to include full life cycle projects. A judgmental sample of 13 PARE projects was selected from the departmental inventory prepared by the DRWG in July 2014, which at the time, contained 100 projects. PARE projects selected for file review were located in six branches – Learning, Skills and Employment, Income Security and Social Development, Citizen Service, Labour and SSP - the Branch formerly known as Strategic Policy and Research. The sample included current (ongoing) projects, completed full life cycle projects, and projects with contractors/sub-contractors. The audit was performed at National Headquarters.

The audit excluded process activities supporting project approval. These activities include the reviews performed by the DRWG and PISC as well as secretarial services provided throughout the approval process.

1.4 Methodology

The audit was conducted using a number of methodologies including:

- Documentation review of applicable legislation, policies, directives and processes surrounding PARE projects that require the connection of databanks and/or use of unmasked personal identifiers.

- Interviews with project authorities and with the Data Management Directorate (DMD) in the SSP Branch.
- Review of guidelines and existing controls to ensure that employees and third parties are aware of their roles and responsibilities and to confirm that the information is used for its intended purpose.
- File review of a sample of PARE projects.

2.0 Audit Findings

2.1 Changes to Approved PARE Projects Need to be Communicated

All PARE submissions to PISC identified the requirements and legislative authority for the collection and use of personal information and/or the connection of databanks.

Approval of Submissions

According to the Governance Protocol for Conducting Policy Analysis, Research, and Evaluation Activities, as well as the DRWG and PISC Terms of Reference, PARE activities requiring the use of unmasked personal identifiers and/or the linkage of two or more internal or external databanks are to be approved by the DM following the review and recommendation by PISC.

The review of the sample of submissions indicated that 3 out of 13 (or 23%) submissions were approved by the Senior Associate Deputy Minister (SADM) of ESDC and Chief Operating Officer (COO) for Service Canada. A further review of the total number of approved submissions indicated that submissions channeled through the DRC were all approved by the DM; while 62% of submissions channeled through the DRWG to PISC were approved by the SADM of ESDC and COO for Service Canada. The audit team was unable to find any documentation supporting the change to the approval process. Through additional inquiries, the audit team was informed by departmental officials that a decision was made to have the SADM of ESDC and COO for Service Canada approve the submissions. During the review of PARE files, the auditors found that approval has since been reverted to the DM for the latest submissions.

Updates to PARE Projects

The DRWG, as specified in its Terms of Reference, reviews amendments to previously approved projects and receives periodic updates from project authorities. Major amendments such as requests for additional databank linkages are reviewed by the DRWG and forwarded to the DM for approval. Minor and clerical amendments such as increasing the sample size, extending the project end date, or minor writing errors are approved by the DRWG chair. Project authorities may be required to give updates on their project and present to PISC if necessary.

During the file review, the audit team found it challenging to identify the current project authority for 8 of the 13 (or 62%) submissions selected for review as they had left ESDC. In addition, the audit team was informed that one of the 13 projects was cancelled as members on the project had left the Department. We were also informed that the project never started; however, we were unable to confirm whether information had been collected, stored or destroyed prior to the cancellation of the project.

Recommendation

The Senior Assistant Deputy Minister of SSP Branch, in consultation with the appropriate departmental officials, should ensure that all PARE submissions include a clause to inform the DRWG of cancelled projects, changes to the project authority, and confirmation when the project is completed and data destroyed.

Management Response

Management agrees with the recommendation. The DRWG Secretariat, Evaluation Directorate drafted a clause to be included in all PARE submissions that will be submitted to the DRWG in April 2015 for review and approval. The clause will require the project authorities to inform the DRWG Secretariat on cancellations, changes to the project authority, as well as a confirmation when the project is complete and the subsequent date of when data is scheduled for destruction. Following DRWG approval, PISC will be informed of the changes to the PARE Submissions. Actions are expected to be completed by April 2015.

2.2 Guidance for Managing PARE Data and Databank Connections Needs to be Established

Access to Personal Information

Projects in our sample for which databank connections were provided by DMD on behalf of Skills and Employment, Citizen Service and SSP branches had a signed Access to Personal Information (API) on file.

Interviews with DMD indicated that access to personal information is provided only after authorization by the Senior Assistant Deputy Minister of SSP through the signing of a completed API form. This form must be completed by ESDC officials seeking to access data containing personal information held in SSP Branch for PARE activities. Access to data files is granted under the general supervision of DMD. This procedure only exists at DMD.

The audit team believes this is a good practice and constitutes an added control to ensure that only authorized staff can access personal information for the purposes of PARE.

Our sample also included PARE projects from the Learning Branch for which databank connections were not provided by DMD, but by the Learning Branch data analyst. Interviews with the data analyst indicated that access to data is restricted to authorized staff only and that electronic data files are stored on a restricted folder in the Common Drive.

Managing Data and Databank Connections

The Governance Protocol for Conducting Policy Analysis, Research, and Evaluation Activities had assigned the responsibility for linking databanks and masking personal identifiers to DMD for SSP and other branches and regions where required. The same Protocol also stated that other branches and regions, however, had the authority to perform data linkages and mask personal identifiers for PARE activities when authorized and in accordance with the principles outlined in the Guidelines for Managing Data and Databank Connections for Policy Analysis, Research, and Evaluation Activities[6].

DMD has established a Data Access, Integration and Development Project Checklist, a tool that is currently used by its analysts for each PARE project to confirm that proper processes have been performed for the production and release of PARE data set extracts from the Statistical Analysis System - Data Integration Server (SAS-DIS).

However, since the Protocol has not been updated and is no longer available, and in the absence of guidelines for managing data and databank connections for PARE activities in the newly implemented Departmental Policy on Privacy Management, branches and regions do not currently have any guidelines to follow when performing data linkages and masking personal identifiers for PARE activities.

Storage of Personal Information

Masked personal information is stored by DMD on SAS-DIS, a dedicated server. For each project, an extract is run and the data moved to the required location by DMD analysts. The SAS-DIS can only be accessed by six analysts as well as a certain number of Shared Services Canada maintenance employees. DMD analysts are required to complete API annually which allows them overall access to the databanks.

SAS-DIS does not have a built-in "auditing of access" feature. Monitoring is performed and controlled at the Operating System and Metadata Server level. However, DMD is looking into acquiring and implementing new features to create access reports which can include flagging irregular access to the server such as access outside of working hours.

Project authorities and members of the PARE projects safeguard masked personal information either on the C drive under the individual user's restricted folder, the U drive restricted to the Branch or Directorate, on a stand-alone server, on Compact Disk or an encrypted key held in a secured cabinet with a combination lock.

With respect to PARE projects conducted by consultants, the audit team found that contracts had clauses for the protection of personal information including privacy breaches while in storage with the consultants. Although a good practice, the auditors were unable to confirm whether data containing personal information was appropriately handled and stored when under custody with the consultants.

[6] The guidelines are appended to the Governance Protocol for Conducting Policy Analysis, Research, and Evaluation Activities.

Disclosing Personal Information

Interviews with DMD as well as the network visual verification of PARE project files, when applicable, indicated that personal information was only released to project authorities after the approval of the PARE submission by the DM (or the SADM of ESDC and COO for Service Canada) and the signing of the API when required. However, the auditors found two projects which involved consultants where contracts were awarded prior to the approval of the PARE submission, and for one of them, data files were requested from the program areas and received at DMD prior to the approval of the PARE submission. Furthermore, some of the data files were provided to the project authority prior to the approval of the submission by the DM.

Destroying Personal Information

The date for destroying information created as a result of PARE projects is set by the project authority. Information is to be destroyed in accordance with the appropriate Records Disposition Authority. 10 out of the 13 sampled project data files are still active and they are not due for destruction yet. For one of them, the audit team found that the date for destroying data files has not been set.

In our sample, there were three project data files due for destruction. The audit team was unable to confirm destruction due to lack of historical information on two projects. For the third project, the audit team found that the project authority had not destroyed the project data files at the time of the audit.

According to the terms and conditions of contracts, data used by consultants should be disposed of at the completion of the contract with a written confirmation to the project authority. For 6 out of the 8 projects with consultants, the audit team was unable to find the written confirmation that was supposed to be received.

Recommendation

The Senior Assistant Deputy Minister of SSP Branch, in consultation with the appropriate departmental officials, should ensure that departmental guidelines for managing data and databank connections in the context of PARE activities are established and communicated to all branches and regions.

Management Response

Management agrees with the recommendation. The process of updating the departmental guidelines has been initiated by the DRWG Secretariat, Evaluation Directorate. The DRWG has been engaged regarding the audit recommendations, and the current version of the "Guidelines for Managing Data and Databank Connections for Policy Analysis, Research, and Evaluation Activities" was circulated to all members. A work plan to update and disseminate the guidelines is being developed by the DRWG Secretariat for discussion with the DRWG in April 2015. After PISC approval, the departmental guidelines will be communicated to all branches and regions. Actions are expected to be completed by April 2016.

3.0 Conclusion

The process in place for approving PARE submissions is thorough. The process, when it is followed, ensures that personal information collected and used for PARE projects is protected and properly destroyed at the end of each project. Project authorities however, do not always adhere to conditions set out in the approved submissions.

4.0 Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only to the 13 PARE projects reviewed. The evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing*.

Appendix A: Audit Criteria Assessment

Audit Criterion	Rating
It is expected that the Department:	
Is managing personal information in accordance with the conditions set out in the approved submission during the life cycle of the project.	◎

✪ = Best practice
● = Sufficiently controlled, low risk exposure
◎ = Controlled, but should be strengthened, medium risk exposure
○ = Missing key controls, high risk exposure

Appendix B: Glossary

API	Access to Personal Information
COO	Chief Operating Officer
DM	Deputy Minister
DMD	Data Management Directorate
DRC	Data Review Committee
DRWG	Databank Review Working Group
ESDC	Employment and Social Development Canada
PARE	Policy Analysis, Research and Evaluation
PISC	Privacy and Information Security Committee
SADM	Senior Associate Deputy Minister
SAS-DIS	Statistical Analysis System – Data Integration Server
SSP	Strategic and Service Policy
TBS	Treasury Board Secretariat