Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Privacy Impact Assessment for Government of Canada Relocation Support Services

Published: 2016

© His Majesty the King in Right of Canada,
represented by the President of the Treasury Board 2016,

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

Catalogue Number:

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 : Résumé de l’évaluation des facteurs relatifs à la vie privée pour les Services de soutien à la réinstallation du gouvernement du Canada

Privacy Impact Assessment for Government of Canada Relocation Support Services

Introduction

The Privacy Impact Assessment (PIA (Privacy Impact Assessment)) for Government of Canada Relocation Support Services (GCRSS (Government of Canada Relocation Support Services Program)) outlines the measures that the Government of Canada has in place to maintain the privacy of employees' personal information when they use GCRSS. The PIA also assesses the privacy implications of using an external service provider to manage GCRSS on behalf of the Government of Canada.

Background

GCRSS is a program that helps Government of Canada employees with their move to new work locations when such a move is necessary for the government's operational requirements.

In early 2016, a new procurement process was initiated for an external service provider to manage all activities related to relocating federal government employees. The contract was awarded in July 2016. Under the contract, the provider is responsible for the following:

- collecting personal information from employees
- billing departments for administration fees
- providing advances to employees
- refunding receipts
- preparing financial reports
- recovering overpayments
- preparing financial reports to departments and agencies

All GCRSS relocation activities are managed through the Information Management Expenditure Tracking System (IMETS (Information management expenditures tracking system)), which is a secure electronic system.

PIA requirements

Under the Treasury Board's Directive on Privacy Impact Assessment, institutions must undertake PIAs for programs and activities in the following circumstances:

- when personal information is used for or is intended to be used as part of a decision-making process that directly affects an individual
- upon substantial modifications to programs or activities where personal information is used or intended to be used for an administrative purpose
- when contracting out or transferring a program or activities to another level of government or the private sector results in substantial modifications to the program or activities

Why this PIA was undertaken

With the award of a new contract for administrating GCRSS, a PIA was recommended to be conducted to determine privacy risks and risk mitigation strategies for the contractor's collection, use and disclosure of personal information. Although substantial modifications have not been made to GCRSS, the recommendation to conduct a PIA was made because a thorough privacy assessment of the program had never been undertaken.

The PIA involves analyzing privacy compliance based on the collection, use and disclosure of personal information, as well as the processing of personal information between departments and the contractor. A review of the Request for Proposal (RFP), the Statement of Requirements (SOR) and the contractual provisions for the procurement process were included in the review of the PIA in order to identify risks and propose mitigation strategies.

An implementation period of six months started on the date of contract award and will be completed on the anticipated service effective date (SED (Service Effective Date)). During this period, the contractor must ensure that the specific requirements of the RFP, SOR and contractual provisions are met. These requirements include but are not limited to the following:

- collecting, using and safeguarding data, including personal information
- requirements for administrative, physical and technical security that must be in place prior to the SED

Any risks identified through the PIA process should be mitigated, or be in the process of mitigation, prior to the SED.

Objectives of the PIA

The PIA's overall objective is to assess, reduce and mitigate potential risks associated with collecting and using personal information in the administration of GCRSS. A thorough analysis of all personal information elements was completed to ensure that only individuals who can access and use GCRSS data have a need to know such data.

PIA findings and summary of action plan

The PIA provides an informed assessment of the privacy risks associated with the collection, use and disclosure of personal information in relation to GCRSS. It also provides recommendations to mitigate identified privacy risks to an acceptable level. The recommendations are as follows:

- modify the contractor's current Acknowledgment and Consent to Collect Information form and include a verbal script for collecting personal information by telephone
- modify the Government of Canada's Personal Information Bank TBS (Treasury Board Secretariat) PCE 792, which is specific to federal institutions
- ensure that guidelines for retaining personal information that is collected, used or disclosed are provided to the contractor prior to the SED to ensure proper handling and disposition of personal information as retention periods expire, or work that involves personal information is completed, or the contract is complete or terminated
- complete a Threat and Risk Assessment (TRA) on IMETS prior to the SED, as set out in contract requirements. Any residual risks to personal information identified in the TRA should be made known and accepted by the Treasury Board of Canada Secretariat executive or senior official

responsible for the program or activity and the head or delegated authority for the Privacy Act, and further updated in the PIA
- implement privacy and security training and awareness for the contractor to ensure that all contractor personnel who have access to personal information in GCRSS are fully aware of their obligations with respect to collecting, using, disclosing, retaining and disposing of such information
- implement privacy and security training and awareness at departments that use GCRSS to ensure that all staff that handle personal information are fully aware of their obligations with respect to collecting, using, disclosing, retaining and disposing of personal information in relation to the GCRSS

Once privacy risks have been fully mitigated, GCRSS will likely present minimal risk to the privacy of individuals who use the service.

Date modified: 2016-12-29