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

Privacy Impact Assessment Summary for Access to Information and Privacy (ATIP) Online Request Service Project

Published: 2018

© His Majesty the King in Right of Canada,
represented by the President of the Treasury Board 2018,

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 le projet de service de demande d'accès à l'information et de protection des renseignements personnels (AIPRP) en ligne

Privacy Impact Assessment Summary for Access to Information and Privacy (ATIP) Online Request Service Project

On this page

- Introduction
- Description
- Why the Privacy Impact Assessment was necessary
- Privacy Impact Assessment Objectives
- Privacy Impact Assessment Findings, Risk Summary and Action Plan

Introduction

The proposed change to the Access to Information Program and the Privacy Request Program for which this Privacy Impact Assessment (PIA) is undertaken is to provide a new online service delivery channel by means of a central website. The ATIP Online Request Service, to be administered and operated by the Open Government division within the Treasury Board of Canada Secretariat (TBS), will allow the public to submit access to information requests under the *Access to Information Act* and personal information requests under the *Privacy Act* and pay applicable fees to 260+

Government of Canada institutions subject to the Acts. The central website will eventually replace the existing ATIP Online pilot operated by Immigration, Refugees and Citizenship Canada (IRCC).

The existing ATIP Online pilot has been in operation by IRCC since 2013. It currently serves 33 federal institutions and is the intake channel for approximately 57% of all ATIP requests received by all government institutions.

Description

The ATIP Online Request Service (AORS) is intended to provide a secure online channel to allow the public to submit access to information (ATI) requests under the *Access to Information Act* (ATIA) and Personal Information (PI) requests under the *Privacy Act* (PA). This website will enable a faster and simpler request process, thereby encouraging a shift from paper to electronic forms. The website will eventually be accessible by 260+ Government of Canada (GC) institutions subject to the Access to Information and Privacy Acts, to receive requests. Applicable fees will be submitted through a third-party payment-processing service provider (Moneris) in a secure manner and subsequently sent to Treasury Board of Canada Secretariat. TBS will then remit the payment to the Receiver General. However, this fee payment mechanism cannot currently be used by Crown corporations, which make up a sizeable portion of the 265 or so GC institutions subject to the Acts; a mechanism enabling fees to be paid through the AORS for requests to Crown Corporations will be established at a later date.

Why the Privacy Impact Assessment was

necessary

A PIA checklist was conducted in relation to the ATIP Central Website with a recommendation to conduct a core PIA. Therefore, the PIA has been conducted in accordance with the Treasury Board *Directive on Privacy Impact Assessment.* This *Directive* requires programs to conduct a PIA upon substantial modifications to existing programs or activities where personal information is used or intended to be used for an administrative purpose (section 6.3.1).

Privacy Impact Assessment Objectives

To ensure sound management and decision making as well as careful consideration of privacy risks with respect to the creation, collection and handling of personal information as part of government programs or activities.

Privacy Impact Assessment Findings, Risk Summary and Action Plan

▼ In this section

- Risk Summary
- Action Plan

Risk Summary

This PIA has identified ten low-level privacy risks related to external and internal breaches, misuse of information, over-retention, and failure to retain information. The external breach risks include the possibility that personal information sent between the requester, the application, and the intended department might be intercepted by a third party. External breaches also include the possibility that threat actors may be able to access unencrypted confirmation e-mails; however, the latter contain only the “label” (i.e. short title) that the requester has assigned to the request and the number that the system has assigned to it. There is a risk that the system could fail to encrypt data submitted to the application, thus rendering the personal information vulnerable to unauthorized access. The use of a third-party payment processing service also entails potential privacy risks relating to unauthorized access to and use of the necessary personal information collected by the third-party provider. Internal breaches include the possibility that people within the institution might view personal information records without proper authority. Potential misuses of personal information (records or metadata) also pose a risk to privacy. And finally, institutions also pose a privacy risk in the situation where they would dispose of information too early or too long after the retention period expires.

Action Plan

A Threat and Risk Assessment on the application was completed during the production implementation. In order to mitigate the risks mentioned above, the application will operate entirely within a secure environment that will ensure that all request data and documents transferred between the application and the institution are encrypted from the time that they are uploaded by the requester to the time that the request is received by

the institution. To mitigate the exposure of personal information, the application encourages requesters to include only personal information that is necessary for the purpose of their request. Risks related to the use of a third-party service provider are mitigated by measures that are explained and assessed in an existing PIA on this arrangement, which is in place between the Government and a number of departments: see Public Services and Procurement Canada: Receiver General Buy Button: Privacy Impact Assessment. Risks related to internal breaches, misuse of information and retention will be mitigated by an appropriate level of training of employees and having well-established Government-wide policies and institution-specific procedural guidelines (i.e. protocols, Values and Ethics code, retention policies). In addition to internal training on these issues for which each institution is responsible, the question of privacy breaches and how to deal with them will be addressed in the package of information developed by TBS for the sessions offered to institutions in support of their onboarding to the system. The link to the plan to be followed in the event of a cyber-incident (*Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018*) will be provided during these training presentations and also posted on GCcollab. Moreover, the application itself mitigates retention risks by automatically deleting all personally identifiable information associated with the request 30 calendar days after the request is forwarded to the intended responding institution. The residual aggregated information and metadata about the request is high-level information that cannot be reverse-engineered to identify a requester (e.g. selected institution, general geographic information such as country and province, date and time, etc.).

Date modified: 2018-12-31