PIA Summary for Public Posting

Access to Information and Privacy (ATIP) Online Service

March 2023

1. About Destination Canada

The Canadian Tourism Commission, operating as 'Destination Canada' (DC), is a Crown Corporation wholly owned by the Government of Canada. Established in 1995, DC was created to lead the Canadian tourism industry in marketing Canada as a four-season tourism destination. DC reports to Parliament through the Minister of Tourism and Associate Minister of Finance.

2. About the Project

In July 2022, DC was notified by the Treasury Board of Canada Secretariat (TBS) of updates to the Government of Canada's core Access to Information and Privacy (ATIP) policy suite. This included updates to the Policy on Access to Information, the Directive on Access to Information Requests, the Policy on Privacy Protection, and the Directive on Personal Information Requests and Correction of Personal Information. These updates were intended to codify best practices in the processing of ATIP requests, and to address technological changes in ATIP program administration, such as the prescribed use of TBS's ATIP Online service.

In September 2022, following the policy changes referenced above, DC was asked to on-board to the Government of Canada's new Service. Developed by the Office of the Chief Information Officer at TBS, the ATIP Online service platform was first introduced in 2020. It provides a centralized, secure, publicly facing platform for Canadians to submit access to information and personal information requests to participating institutions, including DC.

New functionalities within the platform enable individuals to submit ATIP requests as either a guest user or authenticated user, to attach and upload documents to support ATIP requests in a secure manner, and to pay applicable fees for access to information requests. The Service also allows requesters to receive institution-specific guidance when submitting requests, and to create a secure profile to track the status of requests and to receive responses to requests electronically through a secure channel. At the request of TBS, DC will begin using the ATIP Online service to receive and respond to ATIP requests beginning in April 2023.

3. Scope of the Privacy Impact Assessment

Although DC is not itself named in the Schedule to the *Privacy Act* (PA) it reports to Parliament through the Minister of Tourism and Associate Minister of Finance. As such, and in keeping with its designation

as a Crown Corporation, DC abides by the PA and its supporting policies and directives, as established by TBS.

Under the TBS Policy on Privacy Protection, all federal institutions subject to the PA are required to undertake an assessment of the privacy impacts associated with the development or design of new programs or services involving personal information (or when making significant changes to an existing program or service). This PIA performed by DC provides evidence of compliance with those requirements. It also provides assurances that DC's ATIP policies and practices are in keeping with the expectations and requirements of TBS for on boarding to the ATIP Online service.

The PIA was completed under the direction of DC's Executive Director, Legal. Consultations with ATIP personnel, and DC's information management (IM), and information technology (IT) were undertaken where needed. As completed the DC ATIP PIA iss intended to complement the ATIP Online service PIA conducted by TBS in November 2021, the results of which were used to inform DC's decision to use the new platform.

4. Privacy Analysis

Based on the results of the PIA, privacy risks arising from the processing of ATIP requests by DC and the receipt and administration of requests through the new ATIP Online service are expected to be low. Personal information to be collected by DC through the ATIP Online is consistent with that which is already collected, and limited to that which is authorized and required for the processing of requests. Personal information, once collected, is only used in relation to the requests they pertain to. All personal information collected is secured in a manner commensurate with its sensitivity and retained for only so long as it is needed.

Although DC's on-boarding to the ATIP Online service creates a new way in which requests may be received, DC's processing of those requests will remain largely in keeping with existing and established corporate practices and procedures. Potential impacts on the privacy of individuals are being managed by DC through appropriate legal, policy and technical measures geared at the protection of personal information. These include processes to ensure that the identity of a requester is kept confidential.

5. Risk Area Identification and Categorization

A: Type of Program or Activity	**Level of Risk to Privacy**
Program or activity that does NOT involve a decision about an identifiable individual. Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual.	☐ 1

DESTINATION CANADA

Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc…).	☑ 2
Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e., a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).	☐ 3
Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).	☐ 4
B: Type of Personal Information Involved and Context	**Level of risk to privacy**
Only personal information provided by the individual – at the time of collection –- relating to an authorized program & collected directly from the individual or with the consent of the individual for this disclosure / with no contextual sensitivities. The context in which the personal information is collected is not particularly sensitive. For example: general licensing, or renewal of travel documents or identity documents.	☑ 1
Personal information provided by the individual with consent to also use personal information held by another source / with no contextual sensitivities after the time of collection.	☐ 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	☐ 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	☐ 4
C: Program or Activity Partners and Private Sector Involvement	**Level of risk to privacy**
Within the department (amongst one or more programs within the department)	☐ 1
With other federal institutions	☑ 2

With other or a combination of federal/ provincial and/or municipal government(s)	☐ 3
Private sector organizations or international organizations or foreign governments	☐ 4
D: Duration of the Program or Activity	**Level of risk to privacy**
One time program or activity: Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	☐ 1
Short–term program: A program or an activity that supports a short-term goal with an established “sunset” date.	☐ 2
Long-term program: Existing program that has been modified or is established with no clear “sunset”.	☑ 3
E: Program Population	**Level of risk to privacy**
The program affects certain employees for internal administrative purposes.	☐ 1
The program affects all employees for internal administrative purposes.	☐ 2
The program affects certain individuals for external administrative purposes.	☑ 3
The program affects all individuals for external administrative purposes.	☐ 4
F: Technology and Privacy	**Level of risk to privacy**
Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	Yes
Does the new or modified program or activity require substantial modifications to IT legacy systems and / or services?	No
The new or modified program or activity involves the implementation of potentially privacy invasive technologies?	No

DESTINATION CANADA

G: Personal Information Transmission	Level of risk to privacy
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	☐ 1
The personal information is used in system that has connections to at least one other system.	☑ 2
The personal information may be printed or transferred to a portable device.	☐ 3
The personal information is transmitted using wireless technologies.	☐ 4
H: Risk Impact to the Individual or Employee	**Level of risk to privacy**
Inconvenience.	☑ 1
Reputation harm, embarrassment.	☑ 2
Financial harm.	☐ 3
Physical harm.	☐ 4
I: Risk Impact to the Department	**Level of risk to privacy**
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	☑ 1
Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	☐ 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	☐ 3
Reputation harm, embarrassment, loss of credibility.	☐ 4

Decrease confidence by the public, elected officials under the spotlight, departmental strategic outcome compromised, government priority compromised, and impact on the Government of Canada Outcome areas.	