PIA Summary for Public Posting

Assessment of the privacy impacts associated with the use of the ISSI event registration and management system and services platform ("**TEAM**")

August 2024

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 2000, 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.

2. About the Project

DC hosts several industry events held both domestically and in key international markets at varying intervals, including annually, every two years, and one-off ad hoc events that serve a specific purpose (each, a "**DC Event**"). These events are DC-produced and branded undertakings that help Canadian tourism businesses promote, market, and sell Canadian tourism to domestic and international stakeholders such as tour operators, media, and other tourism businesses.

DC Events allow stakeholders to network, build business relationships, and meet one-on-one for future partnership opportunities and negotiations. These DC Events often also include social networking and opportunities to explore the local region in a variety of activities and local tours. Some DC Events are managed by DC team members directly while others are managed by DC's event management vendors. Event management vendors operate as agents of DC, allowing DC to deliver large-scale events efficiently and effectively.

Following an internal assessment of its systems and its requirements, DC issued a negotiated request for proposal (the "**NRFP**") for a new event registration and service platform. Infinite Software Solutions, Inc. ("**ISSI**") was the successful proponent of this competitive procurement process with their event registration and management software and services ("**TEAM**") which is delivered through its web platform and mobile application (the "**Platform**").

The new Platform will provide for:

- Event registration website and development for each DC Event (each, a "**DC Event Page**").
- Integrated DC Event registration solutions to streamline registration processes for stakeholders, including:
    - Information collection, including contact information, meeting preferences, and dietary restrictions, as relevant;

- Activity scheduling (pre- and post-event tours, FAMS, dinners, golf, seminars, etc);
- Hotel room reservations/blocking; and
- Payment processing using an Elavon Converge merchant account owned by ISSI.

- On-site event coordination (as required).
- Appointment matching solutions (both web- and mobile-based).
- Marketing and communications (including invitations, confirmation, instructions, and reminder emails which may track opening, response and/or registration rates).
- Administrative access for DC for the delivery of and reporting on events, including post-event survey responses, all of which are controlled/restricted by administrator usernames and passwords which are uniquely generated for each DC Event Page.
- Access to self-service functionalities post-registration for those individuals who register and attend each DC Event ("**Registrants**") via web and mobile-based applications.
- Translations of the Platform and DC Event Pages for Korean and Spanish, as well as French, Chinese, and Japanese (provided by a third party) as needed for non-English speaking Registrants.

Although the Platform provides for additional functionality, efficiency, and integration of the DC Event registration and administration process, it will not significantly alter the actual scope of collection and processing of personal information.

To administer and deliver TEAM through the Platform for DC Events, DC must collect personal information about Registrants. This personal information may include:

- Name (first, last, preferred name);
- Address (street address, city, province or equivalent, country, postal code or equivalent);
- Contact information (telephone number and email address);
- Account Information (usernames, passwords, and other credentials);
- Image and likeness (account/profile picture), which is optional;
- Employer information (name and nature of business);
- Employment information (business unit, title, city of employment);
- Work contact information (email address and business card);
- Payment processing information (the Platform uses an Elavon Converge merchant account owned by ISSI; last 4 digits of the credit card number entered by the Registrant are stored;

- Social Media Accounts (username, profile, content);
- Medical information (medical conditions including accessibility or dietary restrictions); and
- User data and technical information (IP address, device information, and browsing history);

collectively, the "**PII**".

All the PII is collected directly from the individual. DC does not collect information supplemental to that which is required to facilitate the management of event registration setup, attendee appointment matching, optional activity selection, website development, scheduling support, and custom reporting at and for DC Events (the "**Purpose**").

3. Scope of the Privacy Impact Assessment

As a Crown Corporation that reports to Parliament through the Minister of Tourism, DC abides by the *Privacy Act*, RSC 1985, c P-21 ("**PA**") and its supporting policies and directives, as established by the Treasury Board of Canada Secretariat ("**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 report provides evidence of compliance with those requirements. This PIA was completed under the direction of DC's Executive Director, Legal. Consultations with the DC Event personnel and others were undertaken where needed.

4. Privacy Analysis

Based on the results of the present PIA, the privacy risks arising from the use of the Platform are expected to be low to moderate.

The risk level of low to moderate reflects the use of cloud-based solution with mobile application, administered by a third-party private sector service provider, the Purpose of the project, and the sensitivity of the PII collected (specifically limited payment information and/or medical, dietary, and accessibility information). That said, DC is satisfied, through its competitive procurement and due diligence process, and through this PIA process, that ISSI has the appropriate safeguards in place, and that the benefits provided to DC through the adoption of this solution outweigh the privacy risks. DC has entered into a SaaS Agreement detailing these safeguards.

Further, although the Platform provides additional functionality and integration of the of the event registration and administration process, the actual scope of collection and processing of the PII has not significantly changed since the adoption of the Platform. The PII collected by DC for storage and processing on the Platform is consistent with that which was already collected, and limited to that which is authorized and required for the Purpose. Once collected, the PII is only used in relation to the Purpose.

All PII collected is secured in a manner commensurate with its sensitivity and retained for only so long as it is needed. The processing of the PII 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.

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 ☒
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?	1 ☒

Does the new or modified program or activity require substantial modifications to IT legacy systems and / or services?	2 ☐
The new or modified program or activity involves the implementation of potentially privacy invasive technologies?	3 ☐
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 ☒
Reputational 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. 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.	4 ☒