PIA Summary for Public Posting

Assessment of the privacy impacts associated with the migration to and use of the Greenhouse Software, Inc. Application Tracking System ("ATS")

June 2024

1. About Destination Canada

The Canadian Tourism Commission, operating as 'Destination Canada', 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

For several years, DC has been seeking a new ATS to streamline their recruitment process by enabling more efficient internal recruitment, enhanced candidate screening, automated workflows, and an enriched applicant experience (the "**Project**"). The ATS is intended to assist with managing large volumes of applications from current DC employees who are applying for new roles and prospective DC employees (collectively, the "**Candidates**"), communicating with Candidates, storing Candidate personal information and resumes, issuing technical assessments, scheduling Candidate interviews, and reviewing and reporting on recruitment practices. By acquiring a new ATS with enhanced capabilities and functionalities, DC will be able to deliver a more efficient and effective recruitment process and an overall better Candidate experience.

Following an internal assessment of its systems and its requirements, DC issued a negotiated request for proposal for a new ATS. The ATS provided by Greenhouse Software, Inc. (the "**Platform**") was the successful proponent of this competitive procurement process.

The new Platform will provide for:

- Simplified job posting and distribution on job boards;
- Collection of Candidate demographic data, customized to the job posting and position;
- Candidate management from initial employment application to the final hiring decision;
- Candidate screening and filtering;
- Candidate interview evaluations;
- Supporting objective, equity conscious decision making, including by hiding Candidate information from hiring teams to reduce confirmation bias, implementing objective grading for take-home assessments, and creating defined skills assessment criteria;

- Customization of forms and workflows for recruitment processes, namely to allow prospective Candidates to set reminders and alerts for future job openings;
- Proactive alerts for hiring teams throughout the recruitment process, namely for keyword matching pre-created prospective Candidates profiles to new job openings;
- Automated, personalized emails including stage transitions, scheduling emails, and offer and acceptance emails;
- Self-service eSignature document creation, mapping, administering, and collection;
- Grouping and assignment of internal and external to-dos and tasks relating to the recruitment process;
- Administration and analysis of custom Candidate surveys and results which provide aggregated data to DC on time taken to contact a Candidate, time taken to fill a posted role, and Candidate demographics;
- Customizable, real-time reporting with analytical, data-driven features that allow hiring teams to gain insights into and compare the Candidate and hiring pipelines and to identify deficiencies, avenues for improvement, and opportunities for increased efficiencies in the recruitment processes using aggregate Candidate information; and
- Full and seamless integration with other software used by DC, including UKG Pro.

Although the Platform provides for additional and more efficient functionality of the Candidate recruitment process and integration with other DC programs and processes, it will not significantly alter or expand the actual scope of collection and processing of personal information by DC during the recruitment process.

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 DC's information technology (IT) and human resources (HR) personnel were undertaken where needed.

4. Privacy Analysis

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

The risk level of low to moderate reflects the use of a cloud-based solution administered by a third-party private service provider, the scope of the project (e.g. enterprise-wide) and the

potential involvement of sensitive categories of information, if self-reported by a Candidate, including Social Insurance Number or medical disability / accommodation information. That being said, DC has satisfied itself through its competitive procurement and due diligence process, and through this PIA process, that Greenhouse 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 Master Subscription Agreement with Greenhouse detailing these safeguards.

Further, although the Platform provides additional functionality through a new, integrated service with improved self-service functionality, the actual scope of collection and processing of the PII has not significantly changed as a result of the adoption of the Platform. 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. The PII to be collected by DC and stored and processed on the Platform is consistent with that which is already collected, and limited to that which is authorized and required for the Purpose. PII, once collected, 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.

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	1 ☒

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.	
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 ☒