PIA Summary for Public Posting

Migration to and use of the UKG Integrated Payroll and Human Resources Information System (HRIS) Platform

August 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.

2. About the Project

For over 10 years, DC used separate applications for its payroll processing and its human resources information system ("**HRIS**"). DC previously had a cloud-based system (ADP) for employee payroll and benefits, which was the subject of a Privacy Impact Assessment ("**PIA**") in December 2013. However, until fall 2020, DC was using separate systems to manage other human resources functions, such as employee information storage and employee leave management, in addition to the ADP system for payroll.

Following an internal assessment of its systems and its requirements, DC issued a negotiated request for proposal for a new, integrated, payroll and HRIS platform. UKG, with their UKG Integrated Payroll and Human Resources Information System (HRIS) Platform (the "**Platform**"), was the successful proponent of this competitive procurement process.

The new Platform will provide for:

- Administration of payroll for Canadian employees;
- Administration of leave entitlements (vacation and other short-term or long-term leave) for Canadian and non-Canadian employees;
- Collection and storage of employee personal information for Canadian and non-Canadian employees, including employee equity information;
- Administration of employee engagement and satisfaction surveys;
- Completion and storage of benefit enrollment forms during new employee onboarding;
- Self-service functionality for DC employees to update their personal information (e.g. address, emergency contact, direct deposit information), access their pay stub and tax information, and submit leave requests;
- Access to the self-service functionality via UKG App;

- Creation of reports for internal DC operational use; and
- Creation of reports for external use, in particular, for federal employment equity reporting.

Although the Platform provides for additional functionality and integration of the payroll and HRIS system onto one technological solution, it will not significantly alter the actual scope of collection and processing of DC employee personal information.

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 moderate reflects the use of a cloud-based solution and mobile device application administered by a third-party private service provider, the scope of the project (e.g. enterprise-wide) and the involvement of sensitive categories of information, including financial and banking information of Canadian employees. That being said, DC has satisfied itself through its competitive procurement and due diligence process, and through this PIA process, that the third-party processor, UKG, 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 vendor services agreement detailing these safeguards.

Further, although the Platform provides a new, integrated service, with improved self-service functionality, the actual scope of collection and processing of DC employee personal information has not significantly changed as a result of the adoption of the Platform. Employee personal information collected by DC for storage and processing on the Platform is consistent with that which is already collected, and limited to that which is authorized and required for the management and administration of the employment relationship. Once collected, employee personal information is only used in relation to maintaining an employer-employee relationship including internal payroll affairs and internal HR-related affairs.

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

DESTINATION CANADA

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 ☐

DESTINATION CANADA

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 ☒