

# PIA Summary for Public Posting

## Payroll and Benefit Migration (ADP) PIA

December 2013

### 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's legislated mandate is to: sustain a vibrant and profitable Canadian tourism industry; to market Canada as a desirable tourist destination; to support a cooperative relationship between the private sector and the governments of Canada, the provinces, and the territories with respect to Canadian tourism; and to provide information about Canadian tourism to the private sector and to the governments of Canada, the provinces, and the territories. It fulfills its mandate by working with various levels of government to conduct research and to administer marketing initiatives that increase international visits and tourism revenue. DC also works alongside several international partners to help promote Canadian tourism.

### 2. About the Project

In November 2012, DC elected to upgrade its PaySpecialist (payroll software) service to ADP's Performance Package. That package includes the cloud-based People@Work service (already in use as by DC a human resource information system) and ADP's Pay@Work service. DC's migration from ADP's self-hosted solution to ADP's cloud services for both payroll and benefits serves the need to further streamline operations while ensuring that its IT infrastructure is secure and well maintained. ADP's cloud services provide a best-in-class solution which limits costly investments in hardware and software infrastructure in the short and medium term. Not only does the service provide reductions in IT-related support and maintenance, it provides a modern and scalable solution for DC's evolving human resource management needs.

### 3. Scope of the Privacy Impact Assessment

Although DC is not itself named in the Schedule to the *Privacy Act*<sup>1</sup>, it reports to Parliament through the Minister of Innovation, Science and Economic Development of Canada (previously the Minister of Industry). As such, and in keeping with its designation as a Crown Corporation, DC abides by the Act and its supporting policies and directives, as established by TBS.

---

<sup>1</sup> [Privacy Act](#) (R.S.C., 1985, c. P-21).



Under the TBS [Policy on Privacy Protection](#), all federal institutions subject to the *Privacy Act* 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.

The purpose of the ADP PIA was to assess the privacy risks emanating from the migration of employee payroll and benefit information to a third-party cloud provider, and to provide recommendations to management on the mitigation of those risks.

#### 4. Privacy Analysis

Based on the findings of the ADP PIA, and consistent with DC's preliminary evaluation of risks, the present project is likely to present a moderate risk to the privacy of employees. Although the initiative does not involve the collection of any new personal information, personal information being transferred to the cloud may be sensitive in nature. Similarly, while information to be migrated to ADP's cloud services is to be used for their original purposes consistent with those for which the information was originally collected (and for which consent was obtained), the use of a foreign private host may increase the risk of disclosure to unauthorized third-parties. DC recognizes these risks and has made reasonable efforts to ensure that personal information protections are in place at ADP to protect employee information in a manner commensurate with that reflects the sensitivity of that information.

Notwithstanding the general risks attached to the use of a cloud computing solution for payroll and benefit processing, recommendations from the present PIA, as adopted, are expected reduce these risks to a low or acceptable level.

#### 5. Risk Area Identification and Categorization

<b>A: Type of Program or Activity</b>	<b>Level of Risk to Privacy</b>
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.	<input type="checkbox"/> 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...).	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> 3

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).	
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).	<input type="checkbox"/> 4
<b>B: Type of Personal Information Involved and Context</b>	<b>Level of risk to privacy</b>
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.	<input checked="" type="checkbox"/> 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.	<input type="checkbox"/> 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.	<input checked="" type="checkbox"/> 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	<input type="checkbox"/> 4
<b>C: Program or Activity Partners and Private Sector Involvement</b>	<b>Level of risk to privacy</b>
Within the department (amongst one or more programs within the department)	<input checked="" type="checkbox"/> 1
With other federal institutions	<input type="checkbox"/> 2
With other or a combination of federal/ provincial and/or municipal government(s)	<input type="checkbox"/> 3
Private sector organizations or international organizations or foreign governments	<input checked="" type="checkbox"/> 4

<b>D: Duration of the Program or Activity</b>	<b>Level of risk to privacy</b>
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.	<input type="checkbox"/> 1
Short-term program: A program or an activity that supports a short-term goal with an established "sunset" date.	<input type="checkbox"/> 2
Long-term program: Existing program that has been modified or is established with no clear "sunset".	<input checked="" type="checkbox"/> 3
<b>E: Program Population</b>	<b>Level of risk to privacy</b>
The program affects certain employees for internal administrative purposes.	<input type="checkbox"/> 1
The program affects all employees for internal administrative purposes.	<input checked="" type="checkbox"/> 2
The program affects certain individuals for external administrative purposes.	<input type="checkbox"/> 3
The program affects all individuals for external administrative purposes.	<input type="checkbox"/> 4
<b>F: Technology and Privacy</b>	<b>Level of risk to privacy</b>
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?	No
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
<b>G: Personal Information Transmission</b>	<b>Level of risk to privacy</b>
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	<input type="checkbox"/> 1

The personal information is used in system that has connections to at least one other system.	<input checked="" type="checkbox"/> 2
The personal information may be printed or transferred to a portable device.	<input type="checkbox"/> 3
The personal information is transmitted using wireless technologies.	<input type="checkbox"/> 4
<b>I: Risk Impact to the Individual or Employee</b>	<b>Level of risk to privacy</b>
Inconvenience.	<input checked="" type="checkbox"/> 1
Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
Financial harm.	<input checked="" type="checkbox"/> 3
Physical harm.	<input type="checkbox"/> 4
<b>H: Risk Impact to the Department</b>	<b>Level of risk to privacy</b>
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	<input checked="" type="checkbox"/> 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.	<input checked="" type="checkbox"/> 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	<input checked="" type="checkbox"/> 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.	<input checked="" type="checkbox"/> 4