Unclassified

Audit of the Management of Personal Information for Selected Programs

April 2018

Audit of the Management of Personal Information for Selected Programs

This publication is available for download at canada.ca/publicentre-ESDC .
It is also available upon request in multiple formats (large print, MP3, Braille, audio CD, e-text CD, DAISY or accessible PDF), by contacting 1 800 O-Canada (1-800-622-6232).
By teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No. : Em20-109/2018E-PDF
ISBN: 978-0-660-27331-0

ESDC
Cat. No. : SP-1186-08-18

Table of Contents

1 Background

1.1 Context

Employment and Social Development Canada (ESDC) delivers a wide range of programs and services that affect Canadians throughout their lives, including security for seniors, support for unemployed workers, and helping students finance their education. The following education and disability savings incentives are included within the ESDC suite of programs:

- Canada Disability Savings (CDS) Grant (CDSG) [1];
- Canada Disability Savings (CDS) Bond (CDSB) [2];
- Canada Education Savings Grant (CESG) [3]; and
- Canada Learning Bond (CLB) [4].

The education and disability savings incentives are delivered by the Canada Education Savings Program (CESP) Directorate, Learning Branch, through agreements between ESDC and financial institutions who offer Registered Disability Savings Plans (RDSP) and Registered Education Savings Plans (RESP). The Office for Disability Issues (ODI) is responsible for the policy and program authority for the CDS Grant and Bond, and is also responsible for the development of the agreement between ESDC and financial institutions who offer the disability savings incentives to their clients. The CESP is responsible for the delivery of the education and disability savings incentives and is the policy and program authority for the CESG and CLB.

The CDS Grant and Bond are paid into RDSPs of eligible beneficiaries to help Canadians with disabilities and their families save for the future. To be eligible for the disability savings incentives, a recipient must:

- Be eligible for the Canada Revenue Agency's (CRA) Disability Tax Credit;
- Be under the age of 60;
- Be a Canadian resident; and
- Possess a valid Social Insurance Number (SIN).

The CESG and CLB which are linked to RESPs are intended to encourage early savings for a child's post-secondary education. The CLB provides up to $2,000 to children born in 2004 or

[1] Component of the Canada Disability Savings Program (CDSP).

[2] Ibid.

[3] Component of the Canada Education Savings Program (CESP).

[4] Ibid.

later from low-income families, and those under the care of a public trustee. No personal contributions to an RESP are required to receive the CLB. Eligibility for the CLB is based, in part, on the number of qualified children and the adjusted income of the individual primary caregiver of the beneficiary. The CESG consists of a basic grant amount of up to $500 on annual personal contributions to an RESP for eligible children regardless of family income and an additional amount of CESG of up to $50 or $100 for children from low and middle income families. The CESG is available until the end of the calendar year in which the child turns 17, as long as:

- The child is a resident in Canada;
- The child has a valid SIN;
- The child has been named as a beneficiary in a RESP account; and
- A request is made for the grant.

In order to deliver the education and disability savings incentives, ESDC collects, retains, shares, uses, discloses and disposes of personal information on beneficiaries.

As a federal government institution[5], ESDC is required to manage personal information that it collects, uses and discloses in accordance with the *Privacy Act*. Within the *Privacy Act*, personal information is defined as information about an identifiable individual that is recorded in any form. In accordance with the *Privacy Act*, ESDC is responsible for the protection of personal information, including prevention of wrongful disclosure.

While personal information must be protected from wrongful disclosure, the *Privacy Act* does allow for personal information to be managed under the terms of agreements between the holder of the information and other parties. Other parties with which personal information may be shared include program areas within ESDC, other government departments (OGDs), provincial and territorial governments, foreign states/governments and private sector entities. The *Privacy Act* further outlines the requirements of federal government institutions regarding the management of personal information, including the collection, access to, use, disclosure and disposal of personal information.

1.2 Audit Objective

The objective of this audit was to assess controls in place for the management of personal information related to the CDSP and the CESP[6].

[5] As per *PART 4* of the *Department of Employment and Social Development Act*.

[6] The CESP and the CDSP include the education (CESG and CLB) and disability (CDSG and CDSB) savings incentives.

1.3 Scope

The scope of the audit included the management of personal information by the CESP Directorate for the education and disability incentives, including agreements under which personal information is shared with other parties during the period comprised between April 1st, 2016 and March 31st, 2017.

1.4 Methodology

This audit used a number of methodologies including document review, interviews, on-site observations, walkthroughs, as well as sampling and testing. The audit was conducted between May 2017 and November 2017 within the National Capital Region. The audit team examined the management of personal information holdings related to the education and disability savings incentives, as well as agreements for the sharing of personal information within ESDC, and between the CESP Directorate and OGDs, provincial governments and private sector entities.

2 Audit Findings

2.1 Oversight mechanisms are in place for the management of personal information

The *Privacy Act* governs the personal information handling practices for federal institutions. In support of the *Privacy Act*, ESDC implemented oversight mechanisms for the management of personal information, including departmental policies, procedures and guidelines and governance committees.

Policies, Procedures and Guidelines

ESDC has implemented the departmental Policy on Privacy Management which sets out the Department's application of the *Privacy Act*. This policy requires ESDC to:

- Establish, maintain and support a departmental privacy management program with resources sufficient for the coordination, protection and management of privacy activities.
- Monitor and assess the Department's privacy program's performance, reporting on outcomes and periodic evaluations and reviews.

Within ESDC, the Privacy Management Division prepares an Annual Report on the Administration of the *Privacy Act*, to highlight privacy management accomplishments and areas of concern/improvement within the Department. The report, tabled in Parliament, includes departmental statistics on privacy breaches.

The departmental Policy on Privacy Management is further supported by the departmental Directive on How to Respond to Security Incidents Involving Personal Information (Privacy Breach). The directive:

- Establishes plans and procedures for addressing privacy breaches.
- Defines roles and responsibilities in the event of a privacy breach within the Department.
- Defines internal procedures for notifying the Office of the Privacy Commissioner (OPC) and Treasury Board Secretariat (TBS), as well as the parties affected by the privacy breach.

It is noted that while the Directive includes timelines for the notification of the individuals affected by the privacy breach, there is no information on the timeliness of reporting privacy breaches to OPC or TBS.

For the period between April 1st, 2016 and March 31st, 2017[7], the audit team did not find any realized or suspected breaches of personal information related to the education and disability savings incentives.

Governance Committees

The departmental Policy on Privacy Management requires ESDC to establish a governance structure with clear accountabilities and defined objectives that are aligned with departmental and government-wide policies, priorities and plans, risk identification and mitigation strategies.

Within ESDC, the Privacy and Information Security Committee (PISC) serves as a sub-committee of the Corporate Management Committee on matters related to privacy and the protection of personal information. PISC, co-chaired by the Corporate Secretary and Departmental Security Officer and Director General, Internal Integrity & Security, Integrity Services Branch (ISB), is responsible for reviewing and providing advice to the Deputy Minister on Privacy Impact Assessments and Information Sharing Agreements involving personal information.

The audit found that PISC meets regularly, and that during the period between April 1st, 2016 and March 31st, 2017 two (2) agreements related to personal information managed by the CESP were reviewed by PISC. In accordance with the committee's Terms of Reference, PISC approved the CESP agreements to proceed with obtaining Assistant Deputy Minister approval and Deputy Minister signature with other parties.

Based on the results of our work, we concluded that the Department has established oversight mechanisms for the management of personal information, and these mechanisms are functioning as intended.

2.2 Agreements to govern personal information managed by the CESP are established

To administer the education and disability savings incentives, program areas work collaboratively with partners within ESDC, OGDs, provincial governments and private sector entities.

Agreements within ESDC, Other Government Departments and Provincial Governments

As a part of their operations, the CESP shares personal information related to the administration of the education and disability savings incentives within ESDC, OGDs and provincial governments. ESDC has entered into seven (7) agreements to share personal information with other parties. The agreements were approved by appropriate authorities of both parties.

[7] Management confirmed that for the selected programs there were no realized or suspected breaches of personal information during the period between April 1st, 2016 and March 31st, 2017, therefore detailed testing was not applicable for compliance with the departmental Directive on How to Respond to Security Incidents Involving Personal Information (Privacy Breach).

Six (6) out of seven (7) agreements were consistent with the requirements of the *Privacy Act* related to the collection, access to, use, disclosure and disposal of personal information. With respect to the Memorandum of Agreement for Professional Services between the Canada Education Savings Grant Program Human Resources Development Canada and Moncton Information Technology Centre Human Resources Development Canada, the audit team found the following issues related to access to personal information and disclosure:

- While the agreement states that it is the responsibility of the Moncton Information Technology Centre to treat all files, documents and information as confidential, there are no clauses restricting the access to information to those users with a requirement related to the administration of the education savings incentives or that restrict the disclosure of personal information;
- The agreement does not restrict the use of personal information acquired for the agreement's purpose beyond the identified purpose; and
- The agreement does not include requirements related to the disposal of personal information.

The Department has established an Information Sharing Agreement template for use by ESDC programs. In addition, agreements must be reviewed every five years to ensure that they remain up to date and/or to identify any amendments that may be required. It was found that three (3) out of seven (7) agreements have not been reviewed within the last five years. These agreements were signed in 1999, 2008 and 2009. Of these agreements, one is currently being reviewed, one was reviewed in 2010, but the results were never implemented. One agreement has never been reviewed.

It was observed that the agreement that came into force in 1999[8] was included in a triage exercise performed by the Privacy Management Division. This exercise concluded that the agreement had compliance gaps, but overall the agreement was rated as low risk. Based on this, no further review of the agreement was performed.

The agreement has been in force for over eighteen years. During that period, there have been changes in the environment in which the Department operates, particularly related to privacy and information security. Although this agreement is considered low risk, it could be appropriate to address compliance gaps when this agreement is re-evaluated.

There is also an opportunity for the Department to re-evaluate the 5-year refresh schedule considering the high number of agreements currently in place.

[8] Memorandum of Agreement for Professional Services between the Canada Education Savings Grant Program Human Resources Development Canada and Moncton Information Technology Centre Human Resources Development Canada

Agreements with Private Sector Organizations

ESDC enters into agreements with financial institutions for the delivery of the education and disability savings incentives. These agreements use standardized templates that include sections on applicable privacy laws and personal information.

Private sector organizations are bound by the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[9], which states that an organization is responsible for personal information under its control. PIPEDA establishes principles, by which private sector organizations should be managing personal information, including:

- Identifying Purposes: The purpose for which information is collected is identified by the organization at or before the time the information is collected;
- Limiting Collection: The collection of personal information is limited to what is necessary for the purposes identified by the organizations;
- Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected; and
- Security: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

It was found that agreements tested included clauses specifically related to the PIPEDA principles:

- Purpose/Collection: Agreements specify that personal information is collected for the purpose of delivering the benefits in accordance with all applicable laws governing the protection of personal information under its control.
- Use: Information shall be used solely for the purpose of the delivery of the program benefits.
- Disclosure/Retention: Information shall not be disclosed except for the purpose of administering the program.
- Security: Agreements do not include a clause specifically related to security of personal information (e.g. protection of personal information by administrative safeguards). However, the agreements have standard provisions related to confidentiality, privacy and personal information. Moreover, the audit team was informed that the Department meets annually with financial institutions to discuss operational changes.

As such, the audit team concluded that existing measures (signed standard agreements and PIPEDA requirements) are sufficient.

[9] http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

2.3 PROTECTED

PROTECTED

Recommendation

1. PROTECTED

Management Response

PROTECTED

2.4 Electronic transfer controls are applied during the sharing of personal information

ESDC shares personal information related to beneficiaries as part of the delivery of education and disability savings incentives. ESDC receives personal information on RDSP holders and RESP subscribers from financial institutions that offer these products.

Receipt of Personal Information

Personal information is sent to ESDC from financial institutions via Managed Secure File Transfer (MSFT), which allows external partners to send personal information to ESDC securely. To establish this process, ESDC issues partners with Entrust certificates that the partners use to encrypt personal information prior to sending information to ESDC via a secured portal. Received files are downloaded onto secure program servers and decrypted using the corresponding key.

During the audit, a sample of 34 transfers of personal information received from financial institutions was assessed to determine whether the files were sent in accordance with the terms of agreements.

It was found that 34 out of 34 transfers complied with agreement requirements that the information be encrypted and sent via MSFT. Additionally, it was found that the personal information included in the transfer was limited to the personal information elements required for the administration of the programs.

Sharing of Personal Information

While in agreements with financial institutions, the CESP receives personal information, and it also shares personal information with other program areas within ESDC, OGDs and provincial governments. Administrative safeguards are applied during the sharing of information between the programs and each of these parties, although they differ depending on the party receiving the other information.

- Personal information shared for the administration and delivery of the education and disability savings incentives within ESDC is sent unencrypted. Because the personal

information remains contained within the ESDC network[10] throughout the transfer process, there is no requirement to encrypt the information.

- Personal information for the administration and delivery of the education and disability savings incentives with OGDs and/or provincial governments is sent encrypted via MSFT.

During the audit, it was found that for three (3) out of seven (7) agreements, no transfer of personal information occurred during the period between April 1st, 2016 and March 31st, 2017. For the four (4) agreements for which transfers of personal information occurred, information was protected via administrative safeguards. Specifically, for agreements with OGDs information was transmitted using secure file transfer protocols based upon 256 bit Public Key Infrastructure encryption.

[10] The ESDC network is approved for the storage of up to Protected B information.

3 Conclusion

The audit concluded that controls are in place for the management of personal information related to the administration and delivery of the education and disability savings incentives. Oversight mechanisms have been established, including appropriate governance as well as departmental policies and procedures that are aligned with the *Privacy Act*. In support of these policies, ESDC has also established administrative safeguards that are functioning effectively for the protection of personal information. There are, however, opportunities to improve the disposal of information and to strengthen access controls and the audit trail within program databases.

4 Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only for the Audit of the Management of Personal Information for Selected Programs. The evidence was gathered in accordance with the Treasury Board *Policy on Internal Audit* and the *International Standards for the Professional Practice of Internal Auditing*.

Appendix A: Audit Criteria Assessment

Audit Criteria		Rating
ESDC has oversight mechanisms to protect the management of personal information	ESDC has established a governance structure for the management of personal information	Sufficiently controlled, low risk exposure
	Roles, responsibilities and accountabilities for governance committees and for individuals managing personal information have been established	Sufficiently controlled, low risk exposure
	Governance committees are fulfilling their oversight responsibilities with respect to the management of personal information	Sufficiently controlled, low risk exposure
	Has established policies, directives and guidelines for the management of personal information in line with those of TBS	Sufficiently controlled, low risk exposure
ESDC has adequate controls for the management of personal information	Have agreements governing the management of personal information with other parties	Sufficiently controlled, low risk exposure
	Have agreements for the management of personal information that are aligned with Government of Canada and ESDC standards	Sufficiently controlled, low risk exposure
	Monitor and periodically review agreements for the management of personal information	Controlled, but should be strengthened, medium risk exposure
	Comply with the terms of agreements for the management of personal information	Sufficiently controlled, low risk exposure
ESDC has established administrative safeguards for the protection of personal information	Processes for the management of personal information for the selected programs are in place and working effectively	Controlled, but should be strengthened, medium risk exposure
	Processes to identify, report, investigate and remediate possible breaches of personal information are established and operating as intended	Sufficiently controlled, low risk exposure

Appendix B: Glossary

CDSB	Canada Disability Savings Bond
CDSG	Canada Disability Savings Grant
CDSP	Canada Disability Savings Program
CESG	Canada Education Savings Grant
CESP	Canada Education Savings Program
CLB	Canada Learning Bond
CRA	Canada Revenue Agency
ESDC	Employment and Social Development Canada
ISB	Integrity Services Branch
LAC	Library and Archives Canada
MSFT	Managed Secure File Transfer
ODI	Office for Disability Issues
OGD	Other Government Departments
OPC	Office of the Privacy Commissioner
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PISC	Privacy and Information Security Committee
RDSP	Registered Disability Savings Plans
RESP	Registered Education Savings Plans
SIN	Social Insurance Number
TBS	Treasury Board of Canada Secretariat