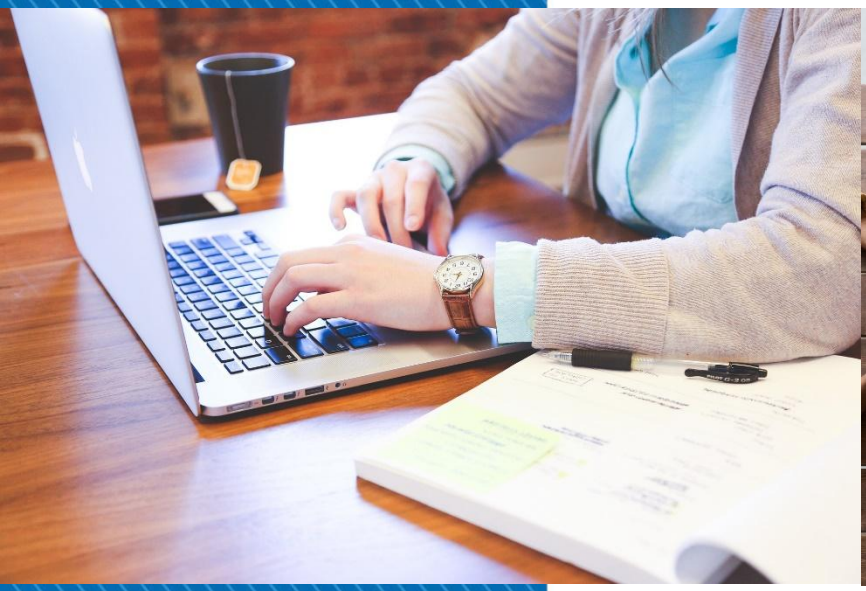
Data residency and sovereignty for settlement service organizations

PROSPECTS





June 2026

Social Research and Demonstration Corporation (SRDC)

Funded by:

Immigration, Refugees and Citizenship Canada

Financé par :

Immigration, Réfugiés et Citoyenneté Canada

SRDC SINCE 1991 SRSA

INNOVATION • EXPERIMENTATION • EVALUATION

SRDC Board of Directors

Richard A. Wagner
Former Partner, Norton Rose Fulbright LLP

Tim Aubry, Ph.D.
Emeritus Professor, School of Psychology,
University of Ottawa

Gordon Berlin
Past President, MDRC

Satya Brink, Ph.D.
International Consultant, Research, Policy Analysis and Strategic Policy advice
Education, Lifelong Learning and Development

Erica Di Ruggiero, Ph.D.
Director, Centre for Global Health
Director, Collaborative Specialization in Global Health
Dalla Lana School of Public Health, University of Toronto

Marie-Lison Fougère
Former Deputy Minister, Ministry of Francophone Affairs
Former Deputy Minister Responsible for Women's Issues

Renée F. Lyons, Ph.D.
Founding Chair and Scientific Director Emeritus,
Bridgepoint Collaboratory for Research and Innovation,
University of Toronto

Andrew Parkin, Ph.D.
Executive Director of the Environics Institute

Nancy Reynolds
Managing Partner, Sterling Lifestyle Solutions

Emile Tompa
Senior Scientist, Institute for Work & Health
Associate Professor, Department of Economics, McMaster University
Assistant Professor, Dalla Lana School of Public Health,
University of Toronto

SRDC President and CEO

David Gyarmati

The Social Research and Demonstration Corporation (SRDC) is a non-profit research organization, created specifically to develop, field test, and rigorously evaluate new programs. SRDC's two-part mission is to help policy-makers and practitioners identify policies and programs that improve the well-being of all Canadians, with a special concern for the effects on the disadvantaged, and to raise the standards of evidence that are used in assessing these policies.

Since its establishment in December 1991, SRDC has conducted over 550 projects and studies for various federal and provincial departments, municipalities, as well as other public and non-profit organizations. SRDC has offices located in Ottawa and Vancouver, and satellite offices in Alberta, British Columbia, Manitoba, Ontario, Quebec, and Saskatchewan.

For more information on SRDC, contact

Social Research and Demonstration Corporation
55 Murray Street, Suite 400
Ottawa, Ontario K1N 5M3
613-237-4311 | 1-866-896-7732
info@srdc.org | www.srdc.org

Vancouver Office
890 West Pender Street, Suite 440
Vancouver, British Columbia V6C 1J9
604-601-4070

Remote offices:
Alberta, British Columbia, Manitoba,
Ontario, Quebec, and Saskatchewan
1-866-896-7732

©Social Research and Demonstration Corporation. All rights reserved.

TABLE OF CONTENTS

DATA RESIDENCY AND DATA SOVEREIGNTY FOR SETTLEMENT SERVICE ORGANIZATIONS **1**

What does this mean for settlement service organizations? 3

Online survey platforms 4

DATA RESIDENCY AND DATA SOVEREIGNTY FOR SETTLEMENT SERVICE ORGANIZATIONS

One of the most complicated issues for organizations collecting data for evaluation or research is the responsibility of privacy protection. Organizations operating in Canada can be subject to multiple legislations, regulations, contractual obligations, and requirements.

For private-sector organizations, the federal Personal Information Protection and Electronic Documents Act (PIPEDA)[1] and provincial privacy legislations are usually applicable. Many online search engines and AI tools suggest that these laws do not forbid the use of US-based cloud platforms to store and process personal information. Some tools even detail the additional requirements a private entity must meet to inform clients (specifically in BC, Alberta, or Quebec). However, this "allowable use" interpretation is not always applicable to organizations contracted by the government.

Many settlement service organizations are under contract with Immigration, Refugees and Citizenship Canada (IRCC) to deliver settlement services. As a result, program operations, including data collection, are considered to be under the control of IRCC. Instead of the federal PIPEDA, these settlement organizations are subject to the federal Privacy Act because they are contractually obligated to handle data with the same rigour as the federal government itself[2].

1 As of 2026, no legislation at the federal level requires personal data collected by private corporations to be stored exclusively in Canada. For organizations operating commercial activities, the focus of the federal law Personal Information Protection and Electronic Documents Act (PIPEDA) is on accountability instead of physical geography. Private sector organizations are allowed to use a third-party processor in another country, but the Canadian organizations remain legally accountable for that data. PIPEDA's mandatory transparency means that organizations must inform their clients that their personal information may be stored or processed outside of Canada and may be subject to the laws and lawful access requests of that foreign jurisdiction. Provincial privacy legislations can override PIPEDA, often adding significant regional requirements. Quebec requires organizations to complete a rigorous Privacy Impact Assessment before personal information is transferred outside the province. Alberta requires organizations to explicitly notify clients about the data transfer and the specific location of the provider. While British Columbia applies similar notification rules to standard commercial entities, its public sector legislation, the Freedom of Information and Protection of Privacy Act (FIPPA), strictly mandates Canadian data residency. Under BC FIPPA, public bodies and their contracted service providers must ensure that personal information is stored and accessed only within Canada, unless an explicit statutory exemption applies.

2 IRCC provided guidance and conducted assessments for service provider organizations on privacy protection and security standards. While these aligned with the Treasury Board Directive, some stakeholders reported that IRCC applied compliance requirements with greater flexibility and practicality.

The federal Privacy Act does not specify "how" personal data is to be safeguarded. Instead, the Treasury Board of Canada creates strict internal policies to ensure government departments (and their contractors) meet their legal obligations. Under the current Directive on Service and Digital[3], the federal government takes a risk-managed approach to cloud computing and data residency:

- Unclassified Data: Non-sensitive data where disclosure causes no injury. Examples: Public reports, general departmental directories. It can sometimes be stored internationally, provided a rigorous security assessment proves the risks are mitigated.

- Protected A Data: It refers to information that warrants protection and would cause injury (though not significant injury) to an individual or organization if compromised. Examples: employee ID number and work telephone numbers.

- Protected B Data[4]: Compromise causes significant harm (examples of Protected B include medical files, personnel evaluations, home addresses, SINs, tax records, or sensitive program participant information such as competency or progress). Government policy generally dictates that Protected B data must be hosted in data centers physically located within Canada, and that encryption keys remain under the exclusive control of the Government of Canada.

In other words, data residency in the federal public sector, which includes settlement service organizations funded by IRCC, is not a statutory law written directly into the Privacy Act. Rather, it is a strict government policy and procurement standard designed to ensure the government and its contractors do not violate the broad security mandate of the Privacy Act.

Unfortunately, many major cloud platforms are owned by companies in the United States, including Microsoft 365, Google Cloud, and Amazon Web Services. Due to the extraterritorial reach of the United States CLOUD Act, these platforms can be compelled to transfer subscribers' data to the United States government. Government departments and contractors may still use a secure cloud platform owned by a United States company, but Privacy Impact Assessments (PIAs) frequently mandate Customer Managed Keys or client-side encryption. This prevents the cloud platform vendor from handing over intelligible data to foreign authorities.

---

3 https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601

4 There is also a "Protected C" classification. Protected C data, if compromised, could cause severe harm (e.g., in cases involving witness protection or criminal investigations). The security and protection measures for Protected C information are more stringent than those for Protected B, and data residency in Canada is required. As most settlement service providers do not handle Protected C information, it is beyond the scope of this article.

For example, the federal government has its own tenancy on the Microsoft Teams platform. This setup has been assessed and cleared to store and process personal information up to the level of Protected B because the government's IT infrastructure retains full control of the encryption keys. Most private sector subscriptions to Microsoft 365, Teams, or Google Workspace, however, rely on the provider's encryption management, which does not meet the requirements of a federal Privacy Impact Assessment.

WHAT DOES THIS MEAN FOR SETTLEMENT SERVICE ORGANIZATIONS?

Because many settlement service organizations must collect personal information on behalf of IRCC, and some of this data is explicitly classified as Protected B, they must safeguard this information exactly as IRCC does under the federal Privacy Act and Treasury Board directives. Even though it is possible to handle classified and unclassified data separately on different systems with distinct safeguards, it is generally easier to manage risk if settlement organizations keep all personal information collected in Canada within a secure system that passes a Privacy Impact Assessment. A cloud platform with Canadian tenancy can be used, provided the platform is officially cleared to handle data at the required security level, such as Protected B.

As of June 2026, avoid using standard subscriptions of Microsoft 365, OneDrive, Google Workspace, or Google Drive to store and process sensitive personal information, unless the organization's specific tenancy is explicitly cleared to handle Protected B information.

For an organization's internal data processing, a secure corporate network with all infrastructure located in Canada under the full control of the organization is better suited to handle personal information. Consult your organization's IT manager or provider to ensure your setup is adequate to maintain full data sovereignty in Canada.

For data capture and processing that unavoidably involves the cloud, such as online surveys, analysis software, or AI tools, organizations should look for a provider that is deemed, by the Public Services and Procurement Canada (PSPC), to be capable to host Protected B information if possible.[5]

[5] There is no certification mechanism that automatically grants a user of an online platform approval to host Protected B information. Although Canadian data residency is required, it is not sufficient to meet all Protected B requirements. While major cloud providers may be assessed by the Canadian Centre for Cyber Security to support compliance with technical standards of hosting Protected B information, organizations must also meet additional non-technical requirements. Specific platform examples are not provided here to avoid misinterpretation, given the strict government standards.

ONLINE SURVEY PLATFORMS

Many online survey tools are available, including popular platforms such as SurveyMonkey, Microsoft Forms, and Google Forms. By default, these platforms do not store data exclusively in Canada, so they are generally not suitable for collecting sensitive personal information classified as Protected B. However, they may be appropriate for unclassified or Protected A data. As a best practice, and to support compliance with applicable privacy legislation, organizations should inform respondents through the consent process that their information may leave Canada.

For anonymous surveys, data can be considered unclassified if the information collected cannot reasonably identify an individual, including through indirect identifiers or triangulation. In these cases, it is generally acceptable to use a secure online platform for data collection.

For surveys that include personal identifiers, such as individualized email invitations, popular online platforms may be acceptable if the information collected or stored would not cause significant harm if compromised. For example, data about program participation experiences or satisfaction are generally not sensitive, so organizations may use any secure online platform for post-program feedback surveys. However, if the survey collects sensitive personal information, such as employment status, income, or social or political opinions, organizations should avoid popular survey platforms that do not provide stronger data residency protections.

Online survey platforms in Canada that are cleared to host and process classified information up to the Protected B level may offer additional features by a third-party processor not in compliance with Protected B data residency protections. For example, sentiment analysis might be available for the survey platform's subscribers with the help of a generative AI model hosted by a US provider. It is the organization's responsibility to understand the scope and compliance of the platform they subscribe to. Security clearance is not automatically transferred without assessment.

OTTAWA • VANCOUVER • CALGARY • HAMILTON

MONTREAL • REGINA • TORONTO • WINNIPEG

www.srdc.org • 1 866 896 7732 • info@srdc.org

SRDC SINCE 1991 DEPUIS SRSA

INNOVATION • EXPERIMENTATION • EVALUATION