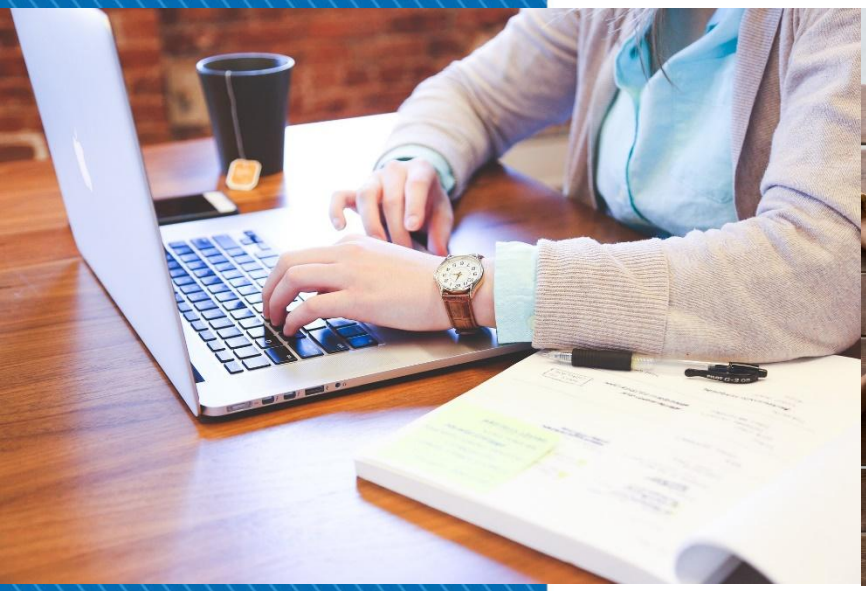
Résidence et souveraineté des données pour les organismes de services d'établissement

CAPACITÉS





Juin 2026

Société de recherche sociale appliquée (SRSA)

Financé par :

Immigration, Réfugiés et Citoyenneté Canada

Funded by:

Immigration, Refugees and Citizenship Canada

SRDC SINCE 1991 DEPUIS SRSA

INNOVATION • EXPERIMENTATION • EVALUATION

Conseil d'administration de la SRSA

Richard A. Wagner
Ancien associé principal, Norton Rose Fulbright S.E.N.C.R.L., s.r.l.

Tim Aubry, Ph.D.
Professeur émérite, École de psychologie, Université d'Ottawa

Gordon Berlin
Ancien président de MDRC

Satya Brink, Ph.D.
Consultante internationale, recherche, analyse des politiques et conseils en politiques stratégiques
Éducation, apprentissage tout au long de la vie et développement

Erica Di Ruggiero, Ph.D.
Directrice, Centre de la santé mondiale
Directrice, Spécialisation collaborative en santé mondiale
École de santé publique Dalla Lana, Université de Toronto

Marie-Lison Fougère
Ancienne sous-ministre, ministère des Affaires francophones
Ancienne sous-ministre déléguée à la Condition féminine

Renée F. Lyons, Ph.D.
Professeure émérite, Université Dalhousie
Présidente fondatrice et directrice scientifique émérite, Bridgepoint Collaboratory for Research and Innovation, Université de Toronto

Andrew Parkin, Ph.D.
Directeur exécutif de l'Environics Institute

Nancy Reynolds
Associée directrice, Sterling Lifestyle Solutions

Emile Tompa
Scientifique principal, Institut pour le travail et la santé
Professeur agrégé, Département d'économie, Université McMaster
Professeur adjoint, École de santé publique Dalla Lana, Université de Toronto

Président et chef de la direction de la SRSA

David Gyarmati

La Société de recherche sociale appliquée (SRSA) est un organisme de recherche sans but lucratif, créé dans le but précis d'élaborer, de mettre à l'essai sur le terrain et d'évaluer rigoureusement de nouveaux programmes. Notre mission, qui comporte deux volets, consiste à aider les décideurs et les intervenants à déterminer les politiques et programmes qui améliorent le bien-être de tous les Canadiens, en se penchant particulièrement sur les effets qu'ils auront sur les personnes défavorisées, et à améliorer les normes relatives aux éléments probants utilisées pour évaluer ces politiques.

Depuis sa création en décembre 1991, la SRSA a mené plus de 550 projets et études pour différents ministères fédéraux et provinciaux, des municipalités ainsi que d'autres organismes publics et sans but lucratif. La SRSA a des bureaux à Ottawa et Vancouver et des bureaux satellites en Alberta, en Colombie-Britannique, au Manitoba, en Ontario, au Québec, et au Saskatchewan.

Pour plus de renseignements sur la SRSA, contacter :

Société de recherche sociale appliquée
55, rue Murray, bureau 400
Ottawa (Ontario) K1N 5M3
613-237-4311 | 1-866-896-7732
info@srdc.org | www.srdc.org

Bureau de Vancouver
890, rue Pender Ouest, bureau 440
Vancouver (Colombie-Britannique) V6C 1J9
604-601-4070

Bureaux satellites :
Alberta, Colombie-Britannique, Manitoba, Ontario, Québec et Saskatchewan
1-866-896-7732

©La Société de recherche sociale appliquée. Tous droits réservés.

TABLE DES MATIÈRES

RÉSIDENCE ET SOUVERAINETÉ DES DONNEES POUR LES ORGANISMES DE SERVICES D'ÉTABLISSEMENT **1**

Quelles sont les implications pour les organismes de services d'établissement ? 3

Plateformes de sondage en ligne 4

RÉSIDENCE ET SOUVERAINETÉ DES DONNÉES POUR LES ORGANISMES DE SERVICES D'ÉTABLISSEMENT

L'un des enjeux les plus complexes pour les organisations qui collectent des données à des fins d'évaluation ou de recherche est la responsabilité liée à la protection de la vie privée. Les organisations opérant au Canada peuvent être soumises à de multiples lois, règlements, obligations contractuelles et exigences.

Pour les organisations du secteur privé, la Loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE)[1] ainsi que les lois provinciales sur la protection de la vie privée s'appliquent généralement. De nombreux moteurs de recherche en ligne et outils d'intelligence artificielle indiquent que ces lois n'interdisent pas l'utilisation de plateformes infonuagiques basées aux États-Unis pour le stockage et le traitement des renseignements personnels. Certains outils précisent même les exigences supplémentaires qu'une entité privée doit respecter pour informer ses clients (notamment en Colombie-Britannique, en Alberta ou au Québec). Toutefois, cette interprétation selon laquelle ces usages seraient « permis » ne s'applique pas toujours aux organisations ayant des contrats avec le gouvernement.

[1] En 2026, aucune loi au niveau fédéral n'exige que les données personnelles recueillies par des entreprises privées soient stockées exclusivement au Canada. Pour les organisations exerçant des activités commerciales, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE / PIPEDA) met l'accent sur la responsabilité plutôt que sur la localisation physique des données. Les organisations du secteur privé sont autorisées à recourir à un sous-traitant situé dans un autre pays, mais les organisations canadiennes demeurent légalement responsables de ces données. L'exigence de transparence prévue par la LPRPDE impose que les organisations informent leurs clients que leurs renseignements personnels peuvent être stockés ou traités à l'extérieur du Canada et peuvent être soumis aux lois et aux demandes d'accès légales de cette juridiction étrangère. Les lois provinciales sur la protection de la vie privée peuvent primer sur la LPRPDE et ajoutent souvent des exigences régionales importantes. Le Québec exige que les organisations réalisent une évaluation rigoureuse des facteurs relatifs à la vie privée avant tout transfert de renseignements personnels à l'extérieur de la province. L'Alberta exige que les organisations informent explicitement leurs clients du transfert de données ainsi que de la localisation précise du fournisseur. Bien que la Colombie-Britannique applique des règles de notification similaires aux entités commerciales standard, sa législation sur le secteur public, la *Freedom of Information and Protection of Privacy Act* (FIPPA), impose strictement la résidence des données au Canada. En vertu de la FIPPA de la Colombie-Britannique, les organismes publics et leurs fournisseurs de services contractuels doivent veiller à ce que les renseignements personnels soient stockés et accessibles uniquement au Canada, sauf exemption légale explicite.

De nombreux organismes de services d'établissement sont sous contrat avec Immigration, Réfugiés et Citoyenneté Canada (IRCC) pour offrir des services d'établissement. Par conséquent, les activités du programme, y compris la collecte de données, sont considérées comme étant sous le contrôle d'IRCC. Au lieu de la LPRPDE, ces organismes d'établissement sont assujettis à la Loi sur la protection des renseignements personnels, puisqu'ils sont contractuellement tenus de gérer les données avec la même rigueur que le gouvernement fédéral lui-même[2].

La Loi fédérale sur la protection des renseignements personnels (Privacy Act, en anglais) ne précise pas la manière dont les données personnelles doivent être protégées. C'est plutôt le Conseil du Trésor du Canada qui établit des politiques internes strictes afin de s'assurer que les ministères (et leurs fournisseurs contractuels) respectent leurs obligations légales. En vertu de la Directive sur les services et le numérique en vigueur[3], le gouvernement fédéral adopte une approche fondée sur la gestion des risques en matière d'infonuagique et de résidence des données :

- Données non classifiées : données non sensibles dont la divulgation ne cause aucun préjudice. Exemples : rapports publics, répertoires généraux des ministères. Elles peuvent parfois être stockées à l'international, à condition qu'une évaluation rigoureuse de la sécurité démontre que les risques sont maîtrisés.

- Données Protégées A : information nécessitant une protection et dont la compromission causerait un préjudice (mais pas un préjudice important) à une personne ou à une organisation. Exemples : numéro d'identification d'employé et numéros de téléphone professionnels.

- Données Protégées B[4] : une compromission entraîne un préjudice important (exemples : dossiers médicaux, évaluations de personnel, adresses personnelles, numéros d'assurance sociale, dossiers fiscaux ou informations sensibles sur les participants à des programmes, comme les compétences ou les progrès). Les politiques gouvernementales exigent généralement que les données Protégées B soient hébergées dans des centres de données

2 IRCC a fourni des orientations et réalisé des évaluations auprès des organismes fournisseurs de services en matière de protection de la vie privée et de normes de sécurité. Bien que ces exigences soient alignées sur la Directive du Conseil du Trésor, certains intervenants ont indiqué qu'IRCC appliquait les exigences de conformité avec davantage de souplesse et de pragmatisme.

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

4 Il existe également une classification **« Protégé C »**. Les données Protégé C, si elles sont compromises, peuvent entraîner des préjudices graves (par exemple dans des cas liés à la protection des témoins ou à des enquêtes criminelles). Les mesures de sécurité et de protection des informations Protégé C sont plus strictes que celles applicables aux données Protégé B, et la résidence des données au Canada est obligatoire. Comme la plupart des fournisseurs de services d'établissement ne traitent pas d'informations Protégé C, ce sujet dépasse le cadre du présent article.

situés physiquement au Canada, et que les clés de chiffrement demeurent sous le contrôle exclusif du gouvernement du Canada.

Autrement dit, la résidence des données dans le secteur public fédéral, qui inclut les organismes de services d'établissement financés par IRCC, n'est pas une exigence législative inscrite directement dans la Loi sur la protection des renseignements personnels. Il s'agit plutôt d'une politique gouvernementale stricte et d'une norme d'approvisionnement conçue pour garantir que le gouvernement et ses fournisseurs contractuels ne contreviennent pas au mandat général de sécurité prévu par cette loi.

Malheureusement, de nombreuses grandes plateformes infonuagiques appartiennent à des entreprises situées aux États-Unis, notamment Microsoft 365, Google Cloud et Amazon Web Services. En raison de la portée extraterritoriale du CLOUD Act américain, ces plateformes peuvent être contraintes de transférer les données des abonnés au gouvernement des États-Unis. Les ministères et les fournisseurs contractuels peuvent tout de même utiliser une plateforme infonuagique sécurisée appartenant à une entreprise américaine, mais les évaluations des facteurs relatifs à la vie privée (EFVP) exigent souvent l'utilisation de clés gérées par le client ou un chiffrement côté client. Cela empêche le fournisseur de la plateforme infonuagique de transmettre des données intelligibles aux autorités étrangères.

Par exemple, le gouvernement fédéral dispose de sa propre instance sur la plateforme Microsoft Teams. Cette configuration a été évaluée et autorisée pour stocker et traiter des renseignements personnels jusqu'au niveau Protégé B, car l'infrastructure informatique du gouvernement conserve le contrôle total des clés de chiffrement. Toutefois, la plupart des abonnements du secteur privé à Microsoft 365, Teams ou Google Workspace reposent sur la gestion du chiffrement par le fournisseur, ce qui ne satisfait pas aux exigences d'une évaluation des facteurs relatifs à la vie privée fédérale.

QUELLES SONT LES IMPLICATIONS POUR LES ORGANISMES DE SERVICES D'ÉTABLISSEMENT ?

Étant donné que de nombreux organismes de services d'établissement doivent recueillir des renseignements personnels au nom d'IRCC, et qu'une partie de ces données est explicitement classifiée au niveau Protégé B, ils doivent protéger ces informations exactement de la même manière qu'IRCC le fait en vertu de la Loi fédérale sur la protection des renseignements personnels et des directives du Conseil du Trésor. Même s'il est possible de traiter séparément les données classifiées et non classifiées sur différents systèmes dotés de protections distinctes, il est généralement plus simple de gérer les risques si les organismes d'établissement conservent tous les renseignements personnels collectés au Canada dans un système sécurisé ayant fait l'objet d'une évaluation des facteurs relatifs à la vie privée (EFVP). Une plateforme infonuagique

ayant une instance canadienne peut être utilisée, à condition que la plateforme soit officiellement autorisée à traiter des données au niveau de sécurité requis, comme le niveau Protégé B.

En date de juin 2026, il convient d'éviter d'utiliser les abonnements standard à Microsoft 365, OneDrive, Google Workspace ou Google Drive pour stocker et traiter des renseignements personnels sensibles, à moins que l'instance spécifique de l'organisation ne soit explicitement autorisée à traiter des informations de niveau Protégé B.

Pour le traitement interne des données d'une organisation, un réseau d'entreprise sécurisé dont toute l'infrastructure est située au Canada et entièrement sous le contrôle de l'organisation est mieux adapté pour gérer les renseignements personnels. Consultez le responsable informatique de votre organisation ou votre fournisseur afin de vous assurer que votre configuration est adéquate pour maintenir une souveraineté complète des données au Canada.

Pour la capture et le traitement de données qui impliquent inévitablement l'infonuagique, comme les sondages en ligne, les logiciels d'analyse ou les outils d'intelligence artificielle, les organisations devraient privilégier un fournisseur jugé, par Services publics et Approvisionnement Canada (SPAC), capable d'héberger des informations de niveau Protégé B, dans la mesure du possible[5].

PLATEFORMES DE SONDAGE EN LIGNE

Il existe de nombreux outils de sondage en ligne, notamment des plateformes populaires telles que SurveyMonkey, Microsoft Forms et Google Forms. Par défaut, ces plateformes ne stockent pas les données exclusivement au Canada ; elles ne sont donc généralement pas adaptées à la collecte de renseignements personnels sensibles classés « Protégés B ». Elles peuvent toutefois convenir pour des données non classifiées ou classées « Protégés A ». Conformément aux meilleures pratiques, et afin de garantir le respect de la législation applicable en matière de protection de la vie privée, les organisations doivent informer les répondants, dans le cadre du processus de consentement, que leurs informations sont susceptibles de quitter le Canada.

Dans le cas des sondages anonymes, les données peuvent être considérées comme non classifiées si les informations recueillies ne permettent pas, de manière raisonnable, d'identifier une

[5] Il n'existe aucun mécanisme de certification qui accorde automatiquement à un utilisateur d'une plateforme en ligne l'autorisation d'héberger des informations de niveau Protégé B. Bien que la résidence des données au Canada soit exigée, elle ne suffit pas à satisfaire l'ensemble des exigences liées au niveau Protégé B. Même si les principaux fournisseurs infonuagiques peuvent être évalués par le Centre canadien pour la cybersécurité afin de soutenir la conformité aux normes techniques relatives à l'hébergement de données Protégé B, les organisations doivent également respecter des exigences non techniques supplémentaires. Aucun exemple précis de plateforme n'est fourni ici afin d'éviter toute mauvaise interprétation, compte tenu des normes gouvernementales strictes.

personne, y compris par le biais d'identifiants indirects ou de triangulation. Dans ces cas, il est généralement acceptable d'utiliser une plateforme en ligne sécurisée pour la collecte des données.

Pour les sondages comportant des identifiants personnels, tels que des invitations par courriel personnalisées, les plateformes en ligne courantes peuvent être acceptables si les informations recueillies ou stockées ne causeraient pas de préjudice significatif en cas de compromission. Par exemple, les données relatives aux expériences de participation à un programme ou à la satisfaction ne sont généralement pas sensibles ; les organisations peuvent donc utiliser n'importe quelle plateforme en ligne sécurisée pour les enquêtes de satisfaction menées après le programme. Toutefois, si l'enquête recueille des informations personnelles sensibles, telles que la situation professionnelle, les revenus ou les opinions sociales ou politiques, les organisations doivent éviter les plateformes d'enquête courantes qui n'offrent pas de protections renforcées en matière de résidence des données.

Au Canada, les plateformes de sondages en ligne autorisées à héberger et à traiter des informations classifiées jusqu'au niveau « Protégé B » peuvent proposer des fonctionnalités supplémentaires fournies par un sous-traitant tiers qui ne respecte pas les exigences de protection de la résidence des données du niveau « Protégé B ». Par exemple, une analyse des sentiments pourrait être proposée aux abonnés de la plateforme de sondage à l'aide d'un modèle d'un modèle d'intelligence artificielle générative hébergé par un fournisseur américain. Il incombe à l'organisation de comprendre la portée et la conformité de la plateforme à laquelle elle est abonnée. L'habilitation de sécurité n'est pas automatiquement transférée sans évaluation préalable.

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