



Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Canada

COUNTRY **Canada**

INDUSTRY **Government & Public Services**

LAST UPDATED **27 October 2026**

KEY REGULATORS **Treasury Board of Canada Secretariat · Office of the Privacy Commissioner of Canada · Ministère de la Cybersécurité et du Numérique (Québec)**

Key takeaways

- No licence is needed to verify identities for Canadian public services, but federal departments must give each service an identity assurance level from 1 (little confidence) to 4 (very high confidence) and meet the Treasury Board's minimum evidence and linkage rules for that level.
- Anti-money laundering law does not apply to public services as such. Identity checks are governed by the Treasury Board identity rules, the federal Privacy Act and provincial laws, not by a customer due diligence rule.
- Online proofing is allowed and widely used. Federal departments must accept a trusted digital identity as an equal alternative to an in-person visit, and services already use photo ID plus a real-time selfie, bank-based checks and agent video calls.
- The federal privacy regulator found in 2024 that two large departments set their online assurance level too low after account takeover attacks. Expect Level 3, multi-factor sign-in and extra checks on high-impact changes such as direct deposit details.
- Sign-in is changing: CanadaLogin is replacing GCKey and bank sign-in service by service, and Québec has enacted a national digital identity that public bodies cannot make compulsory. Québec's government wallet app is planned, with no launch date announced.

Canada is open to digital identity proofing for public services, but it has no single national digital ID. The federal government sets the standard through Treasury Board policy, each province runs its own credentials, and every department decides which assurance level its service needs.

The principal authorities are the Treasury Board of Canada Secretariat, which owns the federal identity directive and standard; the Office of the Privacy Commissioner of Canada, which investigates federal institutions; and, in Québec, the Ministère de la Cybersécurité et du Numérique and the Commission d'accès à l'information.

The biggest obstacle for a provider is fit rather than permission: a method must meet the assurance level a department has documented, connect to the government's mandatory enterprise sign-in services, and satisfy privacy rules on biometrics and retention.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Identity for public services is regulated in two layers. Federal institutions follow Treasury Board policy and the Privacy Act; provinces legislate for their own public bodies.

Authority	Remit	Level	Official site
Treasury Board of Canada Secretariat	Directive on Identity Management and Standard on Identity and Credential Assurance; approves trust frameworks through the Chief Information Officer	Federal	tbs-sct.canada.ca
Office of the Privacy Commissioner of Canada	Investigates federal institutions under the Privacy Act; reports to Parliament	Federal	priv.gc.ca
Immigration, Refugees and Citizenship Canada	Passports, including online renewal, under the Canadian Passport Order	Federal	canada.ca/ircc
Canada Revenue Agency	CRA sign-in services and identity verification for tax and benefit accounts	Federal	canada.ca/cra
Employment and Social Development Canada	My Service Canada Account; publishes the CanadaLogin and digital credentials programme	Federal	canada.ca
Ministère de la Cybersécurité et du Numérique	Québec national digital identity, government authentication service and identity registry	Provincial (Québec)	quebec.ca

Commission d'accès à l'information	Québec privacy oversight, including declarations of biometric identity systems	Provincial (Québec)	cai.gouv.qc.ca
Government of British Columbia (Service BC)	BC Services Card and its app-based login	Provincial (BC)	gov.bc.ca

Each province's information and privacy commissioner (for example in Ontario and British Columbia) oversees its own public bodies.

2 Licensing and authorisation

There is no licence, registration or certification regime for identity verification providers serving Canadian governments. Access is controlled through policy and contract instead.

Federal institutions

The [Directive on Identity Management](#) In force since 1 July 2019 applies to the organisations covered by section 6 of the [Policy on Government Security](#): departments under section 2 of the Financial Administration Act and entities in its Schedules IV and V, unless excluded (s. 6.1). Three requirements decide how an outside identity service gets in:

- Departments accept trusted digital identities only when they come through an **approved trust framework** (s. 4.1.7).
- Departments must consult the Chief Information Officer for the Government of Canada before establishing agreements or adopting trust frameworks (s. 4.1.8).
- Departments must use **mandatory enterprise services** for identity management, credential management and cyber authentication (s. 4.1.9).

Non-compliance is handled through the Treasury Board's Framework for Management of Compliance (Policy on Government Security, s. 7.1), not through fines.

Québec public bodies

Under the [Loi sur le ministère de la Cybersécurité et du Numérique](#) [Act respecting the Ministère de la Cybersécurité et du Numérique], chapter I.1 (added by 2025, c. 26)

In force, the Minister provides the national digital identity services and public bodies must use them on the Minister's conditions, unless the government exempts a body (s. 10.5).

Identity framework (AML rules do not apply)

Public services are not reporting entities under the [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Act](#). The Act reaches government only where a department or Crown agent accepts deposit liabilities, issues, sells or redeems money orders, or sells prescribed precious metals (s. 5(1)). Outside those activities there is no customer due diligence, suspicious transaction reporting or AML record-keeping duty.

What governs identity instead is the Treasury Board framework. Program and service delivery managers must apply identity management requirements whenever unique identification is needed to administer a program enabled by legislation, identity must be disclosed before a service is received, or the accurate and rightful use of identity information is required (Directive, s. 4.1.1). They must also:

- confirm there is a need and the lawful authority to identify the person (s. 4.1.2);
- document identity risks, program impacts, the required assurance levels and risk mitigation options (s. 4.1.3);
- select only sufficient and appropriate identity attributes (s. 4.1.4); and
- apply the assurance levels and controls in the Standard on Identity and Credential Assurance (s. 4.1.6).

The four identity assurance levels

The [Standard on Identity and Credential Assurance](#) In force since 1 July 2019 defines four identity assurance levels and four credential assurance levels, from "little confidence" (Level 1) to "very high confidence" (Level 4). Table 1 of the Standard sets the minimum requirements, which must be met or the related risks appropriately managed (s. A.2.3.1).

Level	Evidence of identity	Accuracy check	Linkage to the person
Level 1	No restriction	Self-assertion accepted	No requirement
Level 2	One piece of evidence	Matches the claim; evidence confirmed as coming from an appropriate authority	No requirement
Level 3	Two pieces, at least one foundational	Foundational evidence confirmed with an authoritative source; supporting evidence confirmed as from an appropriate authority	At least one method

Level 4	Three pieces, at least one foundational	As Level 3	At least three methods
---------	---	------------	------------------------

The linkage methods are knowledge-based, biological or behavioural characteristic, trusted referee and physical possession confirmation. Where the accuracy checks cannot be applied, the Standard requires inspection by a trained examiner.

The two categories of evidence matter for product design. The [Policy on Government Security](#) (Appendix B) defines **foundational evidence** as evidence that establishes core identity information such as given names, surname, date and place of birth, with records of birth, immigration or citizenship as examples. **Supporting evidence** corroborates it and may add a photo, signature or address; the Treasury Board’s [Guideline on Identity Assurance](#) (2016) gives records of entitlement to travel, drive or obtain health insurance as examples. A passport or driver’s licence is therefore supporting evidence, and at Level 3 the instances of evidence are expected to come from different or independent authoritative sources.

4 Identity verification and onboarding

The Standard is technology-neutral; these services publish how they meet it remotely.

<p>Canada Revenue Agency</p> <p>The document verification service needs a person aged 16 or over, an original government photo ID (Canadian driver’s licence, provincial photo ID, permanent resident card, Secure Certificate of Indian Status, or a Canadian, Australian, British or New Zealand passport) and a real-time photo of the face. Health cards, expired documents and photocopies are refused. The alternative is a mailed security code.</p>	<p>Innovation, Science and Economic Development Canada</p> <p>My ISED Account offers four routes: validation through an existing CRA account, an Interac bank-login check, an Interac document check with a selfie (photos kept for 90 days, then deleted) and in-person verification at a Canada Post outlet.</p>
--	---

Service Canada

My Service Canada Account can be registered at once through the [Interac verification service](#) with a participating bank or credit union, or with a Personal Access Code that can take up to 10 business days.

British Columbia

The BC Services Card app can be set up by [sending a video or making a video call](#) (age 12 or over); a Service BC agent compares the face photo with the photo on the ID. Otherwise identity is verified in person.

Interac runs the CRA document service with a third-party provider's AI, which compares the live photo with the ID photo and checks authenticity; the CRA then matches ID details against its records ([privacy impact assessment](#), 12 November 2024).

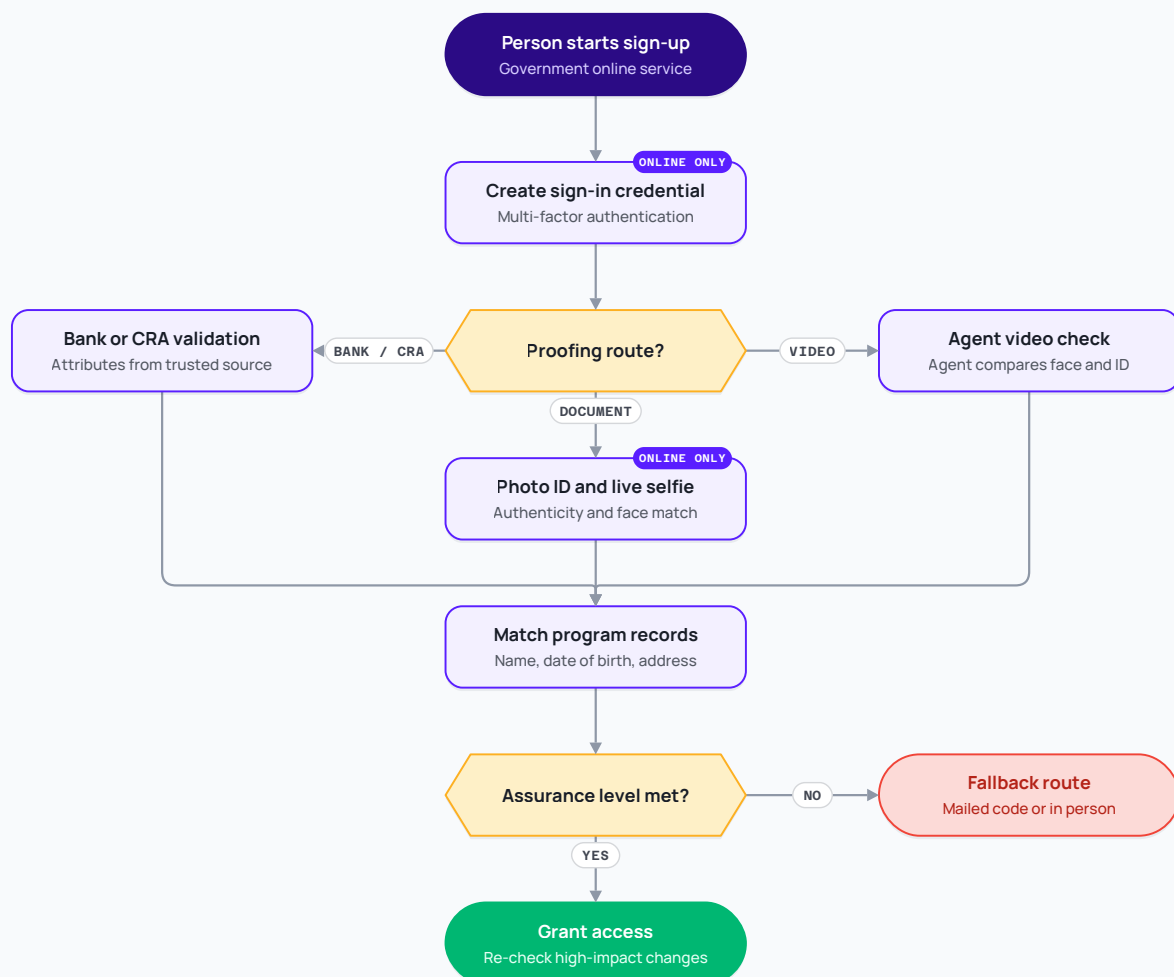


Figure 1. Typical remote identity proofing flow for a Canadian federal online service.

For passports, the [Canadian Passport Order](#) lets the Minister convert an applicant's photograph into a biometric template to verify identity, nationality and entitlement (s. 8.1(2)), and to use electronic and automated systems to make decisions.

5 Digital channels: what's different

Bottom line: the assurance standard is channel-neutral, but federal policy makes a trusted digital identity an equivalent alternative to an in-person visit, so the difference lies in which evidence and linkage methods a remote flow uses to reach the same level.

Requirement	In person	Online / remote	Difference
Assurance level and minimum requirements	Standard, Table 1	Standard, Table 1	Same
Status of digital identity	Default route	Equivalent alternative if from an approved trust framework	Differs
Checking the document	Officer or trained examiner	Document authenticity technology or authoritative-source confirmation	Differs
Linking the document to the person	Face compared by staff	Real-time selfie match, agent video, or bank or CRA account possession	Differs
Sign-in credential	Not needed	Credential with multi-factor authentication	Differs
Minimum age (examples)	Set by each service	CRA document check 16; BC video 12	Differs
Passport renewal eligibility	All renewals	Adults in Canada meeting online criteria	Differs
Privacy Act collection and accuracy duties	Apply	Apply	Same
Québec biometric declaration to the CAI	Required	Required	Same

Trusted digital identity as an equal route

Section 4.1.7 of the Directive requires departments to accept trusted digital identities from an approved trust framework "as an equivalent alternative to in-person interactions". Separate Levels 1 to 4 apply to trusted digital identities (Standard, s. A.2.4).

Online passport renewal

Since 28 July 2026, [online renewal](#) is open to all eligible adults in Canada. Applicants sign in to the IRCC Portal with two-factor authentication and upload a recent photo taken by a commercial photographer; details must be unchanged and delivery is in Canada only.

Optional digital identity in Québec

Québec's national digital identity "ne peut pas être imposée par un organisme public" [cannot be imposed by a public body] to obtain a government service (s. 10.3), so online proofing must sit alongside other routes.

6 Data protection and biometrics

Federal institutions are bound by the [Privacy Act](#). For identity proofing the key duties are to collect only information that relates directly to an operating program (s. 4), to collect it directly from the person where possible and explain the purpose (s. 5), to keep it as accurate, up to date and complete as possible (s. 6(2)), and not to disclose it without consent except as section 8 allows. The Directive adds that notices must be clear enough to obtain meaningful consent when a trusted digital identity is used (s. 4.1.7.4).

Biometrics in Québec

Under the [Act to establish a legal framework for information technology](#) (CQLR c. C-1.1), identity may be verified with biometric characteristics only if the process has been disclosed in advance to the Commission d'accès à l'information and the person gives express consent; only the minimum characteristics may be used, and the record must be destroyed once the purpose is met (s. 44). A biometric database must be disclosed at least 60 days before it goes into service (s. 45). The Commission also expects a non-biometric alternative for anyone who refuses. Québec's identity law bars the Minister from using registry data for profiling (s. 10.7) and leaves biometric government data to regulation (s. 10.9).

Provincial public-sector privacy laws

Québec public bodies must carry out a privacy impact assessment before acquiring or overhauling an information system or electronic service delivery project, and must disclose identification, location or profiling technology before using it ([CQLR c. A-2.1](#), ss. 63.5 and 65.0.1). In Ontario, since 1 July 2025, institutions must prepare a written privacy impact assessment before collecting personal information and report thefts, losses or unauthorised uses that pose a real risk of significant harm to the Information and Privacy Commissioner ([Freedom of Information and Protection of Privacy Act](#), ss. 38(3) and 40.1). British Columbia requires privacy breach notifications (FOIPPA, s. 36.3).

Retention

Retention is set service by service. ISSED's Interac document option keeps ID and selfie photos for 90 days and then deletes them; the CRA's privacy impact assessment does not state a retention period for its document images.

7 Sector-specific obligations

Federal sign-in services

A [GCKey](#) requires two-factor authentication and is revoked if unused for two years. The CRA makes multi-factor authentication mandatory, with a one-time passcode by text or call, a passcode grid or an authenticator app. CanadaLogin, built by the Canadian Digital Service so people prove their identity once, is replacing GCKey and Interac Sign-In Partner service by service. The PrairiesCan and PacifiCan portal, for example, [moved to CanadaLogin only](#) between 22 April and 31 July 2026.

Provincial credentials in federal services

The BC Services Card login is accepted by the CRA for personal tax and benefit information. The CRA's privacy impact assessment records that the BC Services Card and Alberta.ca Account integrations were assessed under the Pan-Canadian Trust Framework in 2020 and 2021.

Québec's government authentication service

Québec's Service d'authentification gouvernementale has been rolled out since December 2022 and is replacing clicSÉCUR; Québec and British Columbia have agreed to make their digital attestations interoperable.

Risk indicators and red flags

IDENTITY ABUSE IN GOVERNMENT ONLINE SERVICES

- **Credential stuffing:** sign-in attempts with usernames and passwords stolen from other breaches.
- **New accounts in a victim's name:** registrations created to apply for benefits or refunds.
- **Direct deposit or address change soon after sign-in:** the main step used to redirect payments.
- **Application filed by someone other than the applicant:** flagged as a risk for online passport renewal.
- **Phishing and paid "assistance" services:** third parties collecting applicants' details and credentials.
- **Lost, stolen, expired or photocopied ID:** refused by the CRA document check.
- **Selfie not taken in real time:** an uploaded or replayed image instead of a live capture.
- **Unmonitored logins:** suspicious sign-in patterns with no detection or response plan.

Enforcement and penalties

The Privacy Act contains no administrative monetary penalties. The Privacy Commissioner investigates complaints (s. 29), reviews compliance with sections 4 to 8 (s. 37) and can report specially to Parliament (s. 39(1)); obstructing the Commissioner carries a fine of up to \$1,000 (s. 68). Within government, breaches of Treasury Board policy are handled through the Framework for Management of Compliance.

Penalties fall on fraudsters rather than institutions. Under the [Criminal Code](#), identity theft and trafficking in identity information carry up to five years' imprisonment (s. 402.2(5)) and identity fraud up to ten years (s. 403(3)). A passport obtained with false or misleading information can be revoked (Canadian Passport Order, s. 10(2)(d)).

Leading case: CRA and ESDC

In a [special report tabled on 15 February 2024](#), the Commissioner found complaints about the 2020 credential stuffing attacks well-founded. Attackers reached about 26,000 CRA My Accounts and 6,000 My Service Canada Accounts (via GCKey), affecting about 34,000 and 14,000 people. Both bodies breached sections 8 and 6(2). A central finding was that both had assessed their services at identity and credential assurance Level 2 when Level 3 was warranted. Both accepted the recommendations, including aligning online identity verification with recognised standards and requiring multi-factor authentication for account recovery; both have since made multi-factor authentication mandatory.

10 Recent changes and what to watch

- **18 October 2026** **In force** : the CRA's document verification page lists a wider set of accepted IDs, including permanent resident cards and some foreign passports.
- **28 July 2026** **In force** : online passport renewal opened to all eligible adults in Canada, moving a high-assurance federal process online.
- **22 April to 31 July 2026** **In force** : PrairiesCan and PacifiCan moved to CanadaLogin as their only sign-in. Other services are migrating one at a time; check each service's own page.
- **15 June 2026** **Bill, not enacted** : Bill C-36, now at second reading in the House of Commons, would enact a new private-sector privacy law that treats biometric information capable of uniquely identifying a person as sensitive, which would affect identity vendors.
- **2025** **In force** : Québec's national digital identity chapter (2025, c. 26) created the identity registry and made public bodies use the Minister's identity services. The use of biometric government data and detailed identification rules are left to regulations under ss. 10.9 and 10.10.
- **1 July 2025** **In force** : Ontario's FIPPA amendments (2024, c. 24, Sched. 2) require privacy impact assessments before collection and breach reporting to the Commissioner, so Ontario digital identity projects need both.
- **Planned**: Québec's citizen digital identity and government wallet app are announced as optional, with no launch date published.

What this means for identity verification

- **Design to a level, not a method.** Map each check to the Standard's evidence, accuracy and linkage rows. A photo ID with a selfie match supplies supporting evidence and one linkage method; Level 3 also needs foundational evidence (such as a birth, citizenship or immigration record) confirmed against an authoritative source.
- **Offer several routes.** Federal services combine document and selfie checks, bank or CRA validation, agent video and in-person or mailed fallbacks; Québec forbids making digital identity compulsory.
- **Document breadth.** Support Canadian driver's licences, provincial photo ID, permanent resident cards, the Secure Certificate of Indian Status and Canadian and selected foreign passports, and reject health cards, photocopies and expired documents where the service does.
- **Live capture and document authenticity.** Remote document checks rely on technology that assesses authenticity and compares a real-time face image with the ID photo.
- **Strong credentials and change controls.** Pair proofing with multi-factor sign-in and re-checks before high-impact changes such as direct deposit or address updates.
- **Biometrics and retention.** Collect the minimum, set and disclose a retention period, and in Québec declare biometric identity systems to the CAI.
- **Federation.** Expect to integrate with CanadaLogin, GCKey, provincial credentials such as the BC Services Card login, or Québec's government authentication service rather than run a standalone login.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- ID document capture and verification, including NFC chip reading, for Canadian and foreign government photo IDs.
- Biometric liveness and face match against the ID photo to support the linkage methods required at higher assurance levels.
- Video KYC for agent-reviewed remote verification as an alternative route.
- No-code workflow builder to offer several proofing routes with fallbacks and an audit trail for each check.
- Cloud, on-premises or hybrid deployment to fit each institution's hosting and retention choices.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- Treasury Board, Directive on Identity Management (effective 1 July 2019), tbs-sct.canada.ca
- Treasury Board, Standard on Identity and Credential Assurance, Appendix A to the Directive (effective 1 July 2019), tbs-sct.canada.ca
- Treasury Board, Policy on Government Security (effective 1 July 2019, amended 6 January 2025), ss. 6, 7 and Appendix B, tbs-sct.canada.ca
- Privacy Act, R.S.C. 1985, c. P-21, ss. 4 to 8, 29, 37, 39, 41, 68, Justice Laws Website, laws-lois.justice.gc.ca
- Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17, s. 5(l), laws-lois.justice.gc.ca

- Criminal Code, R.S.C. 1985, c. C-46, ss. 402.2 and 403, [s. 402.2](#), [s. 403](#)
- Canadian Passport Order, SI/81-86, ss. 8.1 and 10, [laws-lois.justice.gc.ca](#)
- Office of the Privacy Commissioner, Special report to Parliament on cyber attacks on CRA and ESDC (15 February 2024), [priv.gc.ca](#)
- Canada Revenue Agency, Verify your identity (modified 18 October 2026), [canada.ca](#)
- Canada Revenue Agency, Privacy impact assessment: Authentication and Credential Management v4.0 (12 November 2024), [canada.ca](#)
- Canada Revenue Agency, The CRA is making it easier to access its digital services (11 April 2024), [canada.ca](#)
- IRCC, Canada expands online passport renewal to all eligible adults (28 July 2026), [canada.ca](#)
- IRCC, Renew a passport online in Canada (modified 21 September 2026), [canada.ca](#)
- IRCC, Apply online using the IRCC Portal (modified 13 October 2026), [canada.ca](#)
- IRCC, Privacy impact assessment summary: Simplified Renewal Passport Application in the IRCC Portal (26 November 2025), [canada.ca](#)
- ISED, How to verify your identity (My ISED Account) (modified 19 January 2026), [ised-ised.canada.ca](#)
- ESDC, Interac verification service for My Service Canada Account (modified 18 August 2026), [canada.ca](#)
- Government of Canada, Trusted access to digital services (modified 19 May 2026), [canada.ca](#)
- Government of Canada, GCKey help (modified 10 September 2026), [canada.ca](#)
- PrairiesCan, Sign-in help (modified 18 August 2026), [canada.ca](#)
- Parliament of Canada, Bill C-36 (45-1), An Act to enact the Protecting Privacy and Consumer Data Act, LEGISinfo status and first-reading text (15 June 2026), [LEGISinfo](#), [bill text](#)
- Treasury Board, Guideline on Identity Assurance (modified 4 March 2016), s. 3.4.1, [tbs-sct.canada.ca](#)
- Act to establish a legal framework for information technology, CQLR c. C-1.1, ss. 44 and 45 (updated to 15 October 2026), [legisquebec.gouv.qc.ca](#)
- Act respecting access to documents held by public bodies and the protection of personal information, CQLR c. A-2.1, ss. 63.5 and 65.0.1 (updated to 15 October 2026), [legisquebec.gouv.qc.ca](#)
- Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 (Ontario), ss. 38(3) and 40.1, consolidation from 15 September 2026, [ontario.ca/laws](#)
- Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165 (British Columbia), s. 36.3 (current to 20 October 2026), [bclaws.gov.bc.ca](#)
- Loi sur le ministère de la Cybersécurité et du Numérique, RLRQ c. M-17.1.1 [Act respecting the Ministère de la Cybersécurité et du Numérique], chapter I.1, ss. 10.2 to 10.10 (à jour au 15 octobre 2026), [legisquebec.gouv.qc.ca](#)

- Gouvernement du Québec, Programme Service québécois d'identité numérique (updated 8 June 2026), quebec.ca
- Commission d'accès à l'information, Biométrie [Biometrics], cai.gouv.qc.ca
- Government of British Columbia, Verify your identity by video (updated 2 November 2022), gov.bc.ca
- Government of British Columbia, BC Services Card Login (updated 14 September 2026), gov.bc.ca