PRIVACY PRINCIPLES AND PRACTICES FOR COMPLIANCE WITH LAW 25

A practical guide on privacy standards for the public and private sectors in Quebec and how to comply with them

OPEN NORTH

January 2026

CONTENTS

KEY TERMS

Before we begin, here are a few definitions of key terms that you will find throughout this guide:

TERM	DEFINITION
Law 25 (*Loi 25*)	An act to modernize legislative provisions for the protection of personal information, introduced progressively between 2021 and 2024 in Quebec.
Right to privacy	The fundamental right of individuals to control how their personal information is collected, used, disclosed, and retained by organizations.
Personal information	Data about an identifiable individual (e.g., phone number, address, age, gender, ethnicity).
Sensitive personal information	Personal information that requires heightened privacy protection, such as data related to health, finance, race, political opinions, sexual orientations, religious beliefs, and genetic data. (Note: What is considered sensitive can vary from person to person.)
Commission d'accès à l'information (CAI)	Quebec's independent public body responsible for overseeing and enforcing Law 25 for both public and private sector organizations.
Consent	Permission given by an individual for the collection, use, or disclosure of their personal information.
Confidentiality incident	Any event involving unauthorized access, use, communication, or loss of personal information, which requires documentation and potentially notification to the CAI and affected individuals.
Anonymization	A technical process that irreversibly alters personal information so it is no longer reasonably possible to identify an individual, following Quebec's specific regulatory requirements.

WHAT IS LAW 25?

Law 25, formally known as ***"An Act to modernize legislative provisions as regards the protection of personal information,"*** was introduced progressively between 2021 and 2024 in the Canadian province of Quebec. It is a comprehensive legislation that modernizes both private and public sector privacy laws and introduces several new legal compliance requirements.

Law 25 is considered the equivalent of the European Union's General Data Protection Regulation (GDPR) and represents the most demanding privacy law in North America. The legislation establishes stringent requirements for how organizations collect, use, store, and protect personal information, with potential fines reaching up to $25 million or 4% of worldwide revenue for non-compliance and fines for both companies and governments, as well as criminal sanctions for individuals.

WHY IS IT IMPORTANT TO COMPLY WITH LAW 25?

Beyond legal obligations and financial repercussions, compliance with Law 25 is essential for the following:

- **Building trust:** Organizations that demonstrate strong privacy practices earn greater confidence from citizens, customers, members, and beneficiaries. In our digital age, trust is a competitive advantage that directly impacts organizational success and community relationships;
- **Operational excellence:** Good privacy practices lead to better data governance, more efficient operations, and reduced cybersecurity risks. Organizations with clear data management processes experience fewer incidents and operate more effectively;
- **Future-proofing:** As privacy expectations continue to evolve globally, organizations with robust privacy frameworks are better positioned to adapt to future regulatory changes and technological developments;
- **Reputation protection:** Privacy breaches and non-compliance can result in significant reputational damage, negative media coverage, and loss of public confidence that takes years to rebuild.

This guide compares public and private sector requirements under Law 25 and provides practical guidance on how to comply with them. Whether you are serving citizens, customers, members, or beneficiaries, understanding how to properly handle personal information is essential for protecting both your organization and the individuals you serve.

TEN PRIVACY PRINCIPLES: A FOUNDATIONAL FRAMEWORK FOR CANADIAN PERSONAL DATA PROTECTION

Understanding the 10 principles listed below is key to understanding privacy standards and law in Canada, including Quebec. These principles, developed by the Canadian Standards Association, form the foundation of Law 25 and provide a comprehensive framework for responsible personal data handling.

The 10 privacy principles are as follows:

1. **Accountability** — taking responsibility for data protection;
2. **Identifying purposes** — being clear about why you collect personal data;
3. **Consent** — obtaining permission appropriately;
4. **Limiting collection** — collecting only what you need;
5. **Limiting use, disclosure, and retention** — respecting data boundaries;
6. **Accuracy** — keeping data current and correct;
7. **Safeguards** — implementing security measures to protect data;
8. **Openness** — being transparent about your privacy practices;
9. **Individual access** — giving people control over their personal data;
10. **Challenging compliance** — providing recourse when things go wrong.

By understanding these principles, you will understand the core of privacy standards and law in Canada, including Quebec's Law 25. The sections below will explore each principle in detail.

1 Accountability: taking responsibility for data protection

What it means

Your organization must take full responsibility for all personal information under its control, including information handled by third parties on your behalf.

In practice

This means designating someone within your organization as the privacy officer — the person responsible for ensuring privacy practices are followed. This could be the executive director, office manager, or a dedicated privacy coordinator, depending on your organization's size and structure.

Example

When an organization contracts with a third-party service provider to process online payments or manage membership databases, the organization remains accountable for protecting that personal data, even though the processing happens elsewhere.

2

Identifying purposes: being clear about why you collect information

What it means

You must identify and document why you are collecting personal information before or at the time you collect it.

In practice

Every form, application, or data collection process should have a clear, legitimate purpose that you can explain to the person providing their personal information.

Example

When people register for a program or service, clearly explain that you need their contact information to communicate about updates, their address for service delivery if applicable, and emergency contact details for safety purposes.

3

Consent: obtaining permission appropriately

What it means

You must obtain meaningful consent from individuals before collecting, using, or sharing their personal information, except in specific circumstances where the law permits otherwise.

In practice

Consent should be informed (people understand what they are agreeing to), voluntary (no coercion), and specific (clear about particular uses). The form of consent can vary depending on the sensitivity of the data.

Example

When people sign up for a service, they might provide basic consent for program administration, but you need explicit, separate consent to use their photos in promotional materials or to share their data with partner organizations. Registration forms should have separate, unchecked boxes for different purposes rather than bundling everything together.

4

Limiting collection: collecting only what you need

What it means

Collect only the personal data that is needed for the purposes you have identified.

In practice

Question every field on your forms and every piece of data you routinely collect. If you cannot directly connect it to your stated purpose, consider whether you really need it.

Example

For a program registration, you might need a name and contact information to communicate with participants and emergency contact details for safety. You probably do not need to know their occupation, income level, or detailed family information unless it is directly relevant to the specific service being provided.

5

Limiting use, disclosure, and retention: respecting information boundaries

What it means

Personal information should only be used or shared for the purposes for which it was collected, and should not be kept longer than necessary.

In practice

Establish clear policies about how long you keep different types of information and stick to those timelines. Do not use information collected for one purpose for completely different activities without obtaining new consent.

Example

Contact information collected for program notifications should not automatically be used for fundraising campaigns without specific consent. Client records might be kept for service delivery purposes, but they should be securely disposed of after the required retention period based on legal requirements and operational needs.

6

Accuracy: keeping information current and correct

What it means

Personal information should be as accurate, complete, and current as necessary for the purposes for which it is used.

In practice

Establish processes to verify information at the time of collection and to update it when you become aware of changes or errors.

Example

Regularly verify that contact information is current and accurate, especially emergency contacts and addresses for service delivery. Provide easy ways for people to report and correct errors in their files. If someone's circumstances change, make it simple for them to update their information.

7

Safeguards: implementing security measures to protect information

What it means

Protect personal information with security measures appropriate to the sensitivity of the data.

In practice

Implement physical security (locked filing cabinets, secure facilities), technical security (passwords, encryption, secure networks), and organizational measures (training, policies). The level of protection should match the sensitivity of the data.

Example

Sensitive personal data like health records or financial details requires stronger protection than general contact directories. This might include locked filing cabinets, password-protected computers, encryption for digital files, and limiting access to authorized personnel only. Even basic data should be protected from unauthorized access.

8

Openness: being transparent about your privacy practices

What it means

Make information about your privacy policies and practices readily available to the public.

In practice

Develop clear privacy policies using simple language and make them easily accessible. Be prepared to answer questions about how you handle personal data.

Example

Publish a clear data privacy policy on your website explaining how data is collected, used, and protected. Include contact information for privacy inquiries and make this information available in your offices. The policy should be written in plain language that your audience can understand.

9

Individual access: giving people control over their personal information

What it means

Upon request, individuals should be informed about what personal data you have about them and how it is being used and should be given access to their data.

In practice

Establish procedures for handling access requests, including verifying the identity of requesters and providing data in an understandable format within reasonable timeframes.

Example

People should be able to request copies of their own records, program applications, or other personal data you hold. Establish clear procedures and reasonable timelines for these requests. If someone believes their data is incorrect, they should be able to request corrections.

10

Challenging compliance: providing recourse when things go wrong

What it means

Individuals should be able to challenge your organization's compliance with these privacy principles and have their concerns addressed.

In practice

Establish a clear complaint process for privacy concerns, investigate complaints fairly, and take corrective action when necessary.

Example

Create a process for people to file privacy complaints, whether through a designated privacy officer or a formal procedure. Investigate complaints promptly and inform complainants of the results and any corrective actions taken. Be open to feedback and willing to improve your practices.

Privacy principles as a start for good data governance

Whether you are serving the public, customers, members, or beneficiaries, protecting personal information is fundamental to good data governance and responsible practices in any organization. The Canadian Standard Association's Ten Fair Principles provide a proven framework for building trust, reducing risks, and ensuring that personal information is handled with the care and respect it deserves. By embracing these 10 principles, organizations throughout Quebec can build stronger relationships with their communities while protecting the personal information entrusted to their care.

Next, we will discuss how Quebec's privacy laws reflect these 10 privacy principles in public and private organizations.

PERSONAL DATA PROTECTION IN QUEBEC: PRIVATE AND PUBLIC SECTOR REQUIREMENTS TO COMPLY WITH LAW 25

A coffee conversation between peers

Anna, executive director of a charitable organization, and Robert, a municipal clerk, meet to have coffee and discuss their respective challenges with Law 25. Both are responsible for personal data protection within their respective organizations. Anna's organization is subject to the private sector requirements, while Robert's municipality follows public sector rules. They are trying to understand how their privacy legal requirements overlap and how they differ, as they collaborate on a workshop to help other municipalities and nongovernmental organizations navigate Quebec's privacy requirements.

Anna: Robert, I'm still wrapping my head around Law 25. My board keeps asking me about compliance, especially since we work with vulnerable populations. Can we discuss how this all connects to those 10 privacy principles we'll present in our workshop?

Robert: Absolutely! The good news is that Law 25 essentially takes those 10 Canadian privacy principles and makes them legally binding in Quebec. Let's go through them one by one and see how they apply to both of us.

1 Accountability principle in Law 25

Robert: The first principle is **accountability**. Under Law 25. We both need to designate a privacy officer and publish their contact information on our websites.

Anna: Right, so I designated myself as our privacy officer since I'm the executive director. But what if I'm too busy with other responsibilities?

Robert: You can delegate this role to someone else — maybe your office manager or other staff member. The key is having someone who knows the law and can dedicate time to privacy matters. At our municipality, we appointed our IT coordinator because she understands both the technical and legal aspects.

Anna: That makes sense. And we both need clear governance policies too, right? With these policies, people will know how to proceed.

Robert: Exactly! Clear policies that everyone can access and understand.

2 Identifying purposes principle in Law 25

Anna: The second principle is identifying **purposes**. I assume this means we need to be explicit about why we're collecting personal information?

Robert: Correct! Law 25 requires that we clearly state why we're collecting personal data before or when we collect it. For example, when my municipality conducts property assessments, we explain that we need details for taxation purposes and municipal planning.

Anna: So for our program registrations, I need to explain that we collect contact information to communicate about programs, addresses for service delivery, and emergency contacts for safety. But I can't just collect random information "just in case"?

Robert: Exactly! Only collect what you actually need for your stated purpose.

Consent principle in Law 25

3

Anna: Now, **consent** is where I get confused. Do I need explicit permission for everything?

Robert: Here is where our sectors differ significantly. You, in the private sector, generally need explicit consent from individuals for collecting and using their personal information. The consent must be informed, free, specific, and presented separately from other information.

Anna: What do you mean by "separately"? Isn't it enough to have a single manifestation of consent for everything?

Robert: You can't bury consent language in a big block of text. In your case, each consent request needs its own checkbox. Like:

- ☐ "I consent to provide my personal data for the provided service" and, separately,
- ☐ "I consent to receive program updates by email."

Anna: Oh, I see this often on many websites. And for you in the public sector?

Robert: We can collect personal information without consent if it is necessary for our legal mandate — like property assessments, permit applications, or municipal service billing. But if we want to use that data for something else, like sending marketing emails about other city services, then we need consent.

4 Limiting collection principle in Law 25

Robert: The fourth principle is **limiting collection** — only collect what you need. Law 25 makes this a very strict requirement.

Anna: So, for our children's summer camp, I don't really need the child's health insurance number just to register them for arts and crafts, do I?

Robert: Probably not! You need emergency contact information and maybe allergy information, but the health insurance number might be excessive unless there is a specific health-related activity.

Anna: This is going to require me to review all our forms and justify every single field.

Robert: Same here. We're going through every permit application and service request form.

5 Limiting use, disclosure, and retention principle and Law 25

Anna: The fifth principle is about **limiting use, disclosure, and retention**. So personal information collected for one purpose cannot automatically be used for another?

Robert: Exactly! If you collect email addresses for program communications, you can't automatically add them to your fundraising newsletter without separate consent.

Anna: What about retention — how long should we keep personal data in our systems and files?

Robert: Law 25 says you must destroy or anonymize personal data once the purposes are fulfilled. But we also need to follow our legal retention requirements. For us, that means following our Archives Act obligations.

Anna: For us, it might be keeping program records for insurance purposes, but then securely destroying them when no longer needed.

6 Accuracy principle in Law 25

Robert: The **accuracy** principle requires keeping data current and correct. Law 25 strongly reinforces this.

Anna: So if someone moves or changes their emergency contact, we need systems to update that information?

Robert: Yes, and you need to make it easy for people to report and correct errors in their files as well. Both sectors have the same obligation here.

7 Safeguards principle in Law 25

Anna: Safeguards — this is about information security, right? What does Law 25 require?

Robert: Robert: Basically, three levels of security measures: **physical** (locked filing cabinets), **technical** (passwords, encryption), and **organizational** (staff training, policies). The protection level should match the sensitivity of the data.

Anna: Oh, I might need some extra budget for that. So our donor financial information needs stronger protection than our general mailing list?

Robert: Exactly! And if we use third-party services — like cloud storage or payment processors — we need contracts that require them to protect that data too.

8

Openness principle in Law 25

Robert: The **openness** principle means being transparent. Law 25 requires us to publish clear privacy policies on our websites.

Anna: In simple language that people can actually understand?

Robert: Yes! No legal jargon. People should be able to read your policy and understand what you do with their personal information.

9

Individual access principle in Law 25

Anna: Individual access — this is about people getting copies of their own data??

Robert: Right! Under Law 25, people can request access to their data, request corrections, withdraw consent, and even request that we stop sharing their information in certain cases. We have 30 days to respond to these requests.

Anna: Is there a "right to be forgotten" in Law 25 like in the European Union's GDPR?

Robert: Sort of. There's a right to "de-indexation" — people can request that we stop disseminating their data or remove hyperlinks to it if it's causing them harm. But for us in the public sector, this gets complicated because of public records and transparency requirements.

Anna: That sounds legally complex.

Robert: It is! That's why we need legal advice for those requests.

10 Challenging compliance principle in Law 25

Robert: The final principle is **challenging compliance** — providing recourse when things go wrong.

Anna: So we need a formal complaint process?

Robert: Yes, and incident response procedures. If there's a data breach, we must assess the risk, and if it is serious, notify both the Commission d'accès à l'information — the CAI — and the affected individuals.

Anna: But what is considered "serious"?

Robert: If the breach could lead to identity theft, financial fraud, or significant harm to the individuals involved. Law 25 requires that we keep a register of all incidents, even minor ones.

The consequences of non-Compliance

Anna: This is a lot to manage, but following these 10 principles makes it feel more organized. What happens if we don't comply?

Robert: The penalties are significant. For private organizations like yours, fines can reach $25 million or 4% of worldwide revenue. For public organizations like mine, the financial penalties are not as steep, but there is more oversight. Plus, individuals can now sue organizations directly for privacy violations.

Anna: That is serious motivation to get this right! At least we have the same oversight body — the CAI — monitoring both sectors.

Robert: Exactly. And the 10 principles give us a roadmap. If we follow them systematically, we'll be well on our way to compliance with Law 25.

Based on Anna and Robert's conversation, let us see how well your organization addresses these requirements.

LAW 25 COMPLIANCE QUICK ASSESSMENT

Common requirements (private and public sectors)

- [ ] **Accountability:** Have you designated a privacy officer and published their contact information?
- [ ] **Identifying purposes:** Do you have a documented inventory of all personal data collected and the purposes for collection?
- [ ] **Consent:** Is there a process to obtain explicit consent from individuals before collecting their personal data (private sector) or for secondary uses (public sector)?
- [ ] **Limiting collection:** Are you ensuring that collection of personal data is limited to what is necessary for the stated purpose?
- [ ] **Limiting use and disclosure:** Do you use data only for original purposes unless consent is obtained for new uses?
- [ ] **Data retention:** Do you have procedures to securely dispose of or anonymize personal data that is no longer needed?
- [ ] **Accuracy:** Have you established procedures to maintain current, correct information and handle correction requests?
- [ ] **Safeguards:** Does your organization have a comprehensive security policy with physical, technical, and organizational measures proportional to data sensitivity?
- [ ] **Openness:** Is your privacy policy written in simple language, accessible to the public?
- [ ] **Individual access:** Have you established procedures to respond to access, rectification, and data portability requests within legal deadlines (30 days for private sector, 20 days for public sector)?
- [ ] **Challenging compliance:** Do you have a formal complaint process and incident response procedures?
- [ ] **Privacy by default:** Are your technological products/services configured with the highest privacy settings by default?
- [ ] **Privacy impact assessments:** Do you conduct PIAs for new information systems and cross-border data transfers?
- [ ] **Incident register:** Do you maintain a register of all confidentiality incidents as required by Law 25?
- [ ] **Third-party contracts:** Have you established contracts with service providers ensuring they adhere to Law 25 requirements?
- [ ] **Automated decision making:** Do you inform individuals when they are subject to automated decision making or profiling?

Additional public sector requirements

- [ ] **Mandatory committee:** Have you established a "committee on access to information and the protection of personal information"?
- [ ] **20-day response:** Are you able to answer access requests within 20 days (extendable to 30 days)?
- [ ] **Archives integration:** Do your retention practices align with provincial archives requirements?
- [ ] **CAI notification:** Have you formally notified the CAI of your privacy officer appointment?

Additional private sector requirements

- [ ] **Express consent:** Do you obtain explicit, granular consent for sensitive data and secondary uses with separate, unchecked boxes?
- [ ] **30-day response:** Are you able to process individual requests within 30 days?
- [ ] **Right to erasure:** Do you have a process to evaluate requests to cease dissemination or de-index personal data?
- [ ] **Contract compliance:** Are consent requests presented separately from other information?

If you cannot check all applicable elements, immediate action is required to achieve Law 25 compliance.

Get started today

Hopefully this guide has given you a better understanding of the national framework that underpins Canadian privacy law and your specific obligations under Law 25, whether you are in the public or private sector.

If you require support to comply with your privacy requirements, Open North can support you through its targeted support service. Learn more about our privacy compliance services here, or contact us at info@opennorth.ca.

About Open North

Building trust in data, for the common good

Open North is a not-for-profit organization dedicated to advancing the common good. Working alongside governments and civic-minded organizations of all sizes, we provide data expertise to enhance decision making, drive innovation, improve public and civic services, and address society's most pressing challenges.

Our work focuses on building the capacity of organizations to make better decisions about managing their data so that it is useful, actionable, secure, and trustworthy throughout its entire lifecycle. At Open North, we combine deep expertise in data with a multidisciplinary approach. Our team includes urban planners, software engineers, community organizers, data scientists, cybersecurity and IT audit specialists, sociologists, geographers, and technology lawyers, bringing diverse perspectives to every project.

Open North is part of Montréal in Common, a project led by the City of Montréal as part of the Smart Cities Challenge, carried out with the financial support of the Government of Canada.

opennorth.ca

About the Smart Cities Challenge and Montréal in Common

Montréal in Common is an innovation community led by the City of Montréal whose partners are experimenting with solutions regarding access to food, mobility, and municipal bylaws, with a view to rethink the city. Montréal in Common projects are made possible thanks to the prize awarded to the City of Montréal by the Government of Canada as part of the Smart Cities Challenge.

Authors: Cristiano Therrien and Samuel Kohn

Canada Montréal SMART CITIES CHALLENGE Montréal en commun

Privacy principles and practices for compliance with Law 25