



Meeting Quebec's Law 25 without rebuilding what departments already run.

1 The Quebec Challenge

Law 25 gave Quebec residents real privacy rights and gave public bodies real obligations. Public-sector organizations must now meet requirements such as granular consent, privacy-by-design system changes, the designation of a person in charge of protecting personal information, breach notification to the Commission d'accès

à l'information and to affected residents, and, as of September 2024, the right to data portability. These obligations are managed by department, but residents experience government as a whole, which is exactly where compliance gets complicated.

2 Why It's Hard for Governments Specifically

- Personal information is duplicated across dozens of systems, each with its own consent record, account, and support queue.
- A resident's data footprint spans systems that no single team can see end to end. As a result, scoping a breach or responding to an access request means tracking down every department involved.
- Legacy systems that agencies depend on were not built with consent tracking, selective disclosure, or portability in mind. Replacing them is neither fast nor affordable.

How CitizenOne Helps

CitizenOne is a trusted identity and service-connection layer that sits across the systems departments already use, rather than a new large-scale system to replace them. It gives residents one adaptive account while providing departments with the consent, audit, and governance framework Law 25 requires. Each department keeps its own systems, data, and authorization decisions.

Law 25 Requirement	How CitizenOne Helps
Granular, purpose-specific consent for every service	Consent-based attribute sharing lets residents grant or withdraw access service by service, with a record of what was shared and why.
Privacy by design and data minimization	Progressive disclosure shares only the attributes a transaction needs; the system issues privacy-preserving, progressively disclosable credentials instead of copying full records.
Designated privacy officer and governance accountability	Service-provider dashboards give each department visibility into how its data is accessed, supporting the record-keeping responsibilities of the privacy officer.
Incident and breach notification obligations	A common resident profile with a consent and access trail helps scope and document an incident quickly instead of reconstructing it across disconnected systems.
Right to data portability and access requests	One resident account with legacy-account binding gives residents and agencies a single place to locate, review, and export information held about them.
Transparency in automated decision-making	Identity and eligibility signals stay separate from program decisions, so agencies retain and can explain the decision logic they are required to disclose under Law 25.



Proven in Quebec, not a pilot story

CitizenOne was shaped by real government implementations in Canada, developed in direct collaboration with provincial and municipal partners. Today, it supports millions of citizens and hundreds of services — privacy governance included, not bolted on afterward.

Value

For residents:

One account, fewer repeated consent requests, clear visibility into who has access to their information, and a straightforward way to exercise their Law 25 rights.

For government:

A documented, defensible consent and access trail, faster and better-scoped breach response, preserved investment in existing systems, and a built-in evidence base for the designated privacy officer rather than one assembled after the fact.

Let's talk

If you are weighing a Law 25 remediation project against a rebuild, we would welcome a working session to assess how CitizenOne aligns with your current systems and compliance obligations.

Contact us to book a free demo with a Portage CyberTech digital identity expert.

<https://www.portagecybertech.com/en/contact/>

Scan to learn more

