

Digital sovereignty through operational transparency

A Global Privacy Rights position paper on the Québec data sovereignty agenda

Mark Lizar



Global Privacy Rights

Transparency by Default. Privacy rights that work.

globalprivacyrights.org

SUBMISSION

23 September 2026

Digital sovereignty through operational transparency

A Global Privacy Rights position paper on the Québec data sovereignty agenda

Global Privacy Rights 23 September 2026

Summary

Digital sovereignty requires more than local hosting. It requires a visible, portable and testable account of who has authority over data, under which rules, for what purpose, and with what controls when data crosses an organisational or geographic boundary.

Données Souveraines Québec, launched in March 2026, sets out four strategic pillars: control over strategic data, freedom from technological lock-in, open source and open standards, and a sovereign economy that connects resilience with sustainable development. We support that direction. This paper argues that each pillar needs an operational transparency layer to become testable, and sets out what that layer consists of.

An organisation cannot demonstrate sovereignty by naming a local data centre. It has to be able to show, before collection or identification: who is accountable; what authority they hold; where data is stored and processed; which purposes and legal bases apply; which parties can access, transfer or change the data; what notice was presented; what was authorised, refused or withdrawn; and how another party can inspect and verify that record.

Digital sovereignty is therefore not the claim that data is sovereign because it sits in Québec. It is an operational condition in which authority, location, purpose, permission and change are explicit, evidenced and portable across jurisdictions.

1 The question sovereignty must answer

Sovereignty is usually described as authority attached to a territory, an institution or a community. Online, that authority is distributed across people, controllers, processors, infrastructure providers, software suppliers, regulators and standards bodies.

A person may be in Québec while their information is processed by a controller in another jurisdiction, stored by a cloud provider elsewhere, transferred to a sub-processor, and used by a system whose purpose and retention rules cannot be inspected. Local hosting reduces some risks. It does not by itself answer who controls the processing, under which law, or how the individual stops personal data crossing a border.

So the practical question is not only where the data is. It is:

Who can exercise authority over this data, for what purpose, under which legal and technical rules, and how can that authority be inspected before the data is disclosed?

That is a question about evidence, and it is where sovereignty needs operational transparency rather than a general assurance statement.

2 Authority positions that must remain distinct

Digital sovereignty is best treated as stakeholder-relative authority. Several positions have to be connected without being collapsed into one vocabulary.

Authority position	Who holds it	What must remain possible
Personal digital sovereignty	The individual, the PII principal	Inspect, decide, authorise, refuse, withdraw, and control identity disclosure
Private controller governance	The PII controller, processor or sub-processor	Manage lawful purposes, permissions, security, records, transfers, retention and accountability
Public governance	Regulators, public authorities and open standards communities	Inspect, audit, challenge, enforce and interoperate across jurisdictions

A controller's internal record may support accountability. It does not become the individual's sovereignty merely because it is authoritative inside the controller's own system. Personal authority needs its own representation in the interaction, including the ability to inspect the controller before identification is required.

A fourth position exists and this paper does not speak to its content. A collective authority position is held by a community over its own data, knowledge, language and territorial information, and it is not reducible to the sum of the individual rights of that

community's members. An individual authorisation cannot authorise the use of collective knowledge, and a collective authorisation cannot remove an individual right. Where both apply, both have to be satisfied. What that position requires is for the rights holders concerned to define, not for this paper to describe on their behalf. It is named here because a sovereignty framework that omitted it would be incomplete, and because a record structure designed only for individuals will not carry it later without redesign.

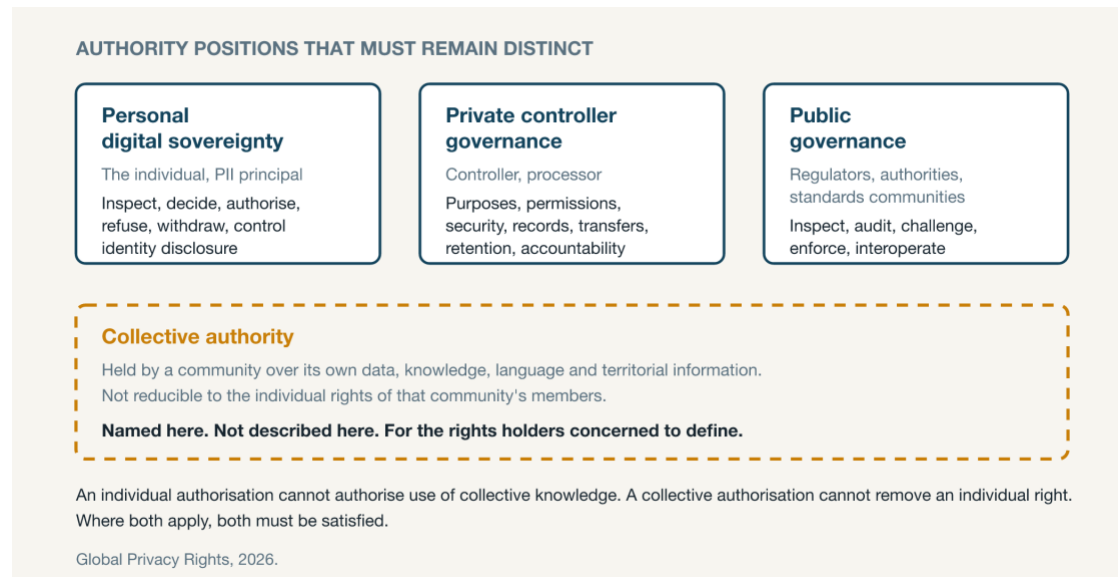


Figure 1. The authority positions a sovereignty framework has to keep distinct. Three are described here. The fourth is named and deliberately not described, because its content is for the rights holders concerned to define.

Figure 1. The authority positions a sovereignty framework has to keep distinct. Three are described here. The fourth is named and deliberately not described, because its content is for the rights holders concerned to define.

3 A response to the four pillars

Pillar one: control and local custody

The first pillar calls for mapping strategic assets and protecting them in infrastructure under local legal and physical control. Operational transparency adds the evidence that makes the position testable.

A sovereignty record should identify the accountable organisation, the jurisdiction, the storage and processing locations stated separately, the parties with access, the applicable transfer mechanism, the retention position, and the rights access point. A location field without an accountable identity is not sufficient. A local operator without a public record of its sub-processors is not sufficient. A record that cannot be inspected or compared over time is not sufficient.

Pillar two: freedom from lock-in

The manifesto calls for exit strategies, migration plans and investment in internal competence. These are sovereignty controls, because dependency is a transfer of practical authority to a supplier.

Operational transparency makes the exit condition measurable. A controller should be able to export its current controller identification record, its notices, permissions, processing references and change history in a standard form. A successor should be able to read and verify those artefacts without asking the previous supplier for permission and without a proprietary console.

The same test applies to any public register, including ours. A register should publish machine-readable records with stable references that can be copied and verified by a third party, so that the register itself is not a new dependency.

Pillar three: open source and open standards

Open source is necessary for inspection and adaptation, and source availability alone does not make the governance of a service transparent. A system can publish its code while leaving its authority model, its data purposes and its operational changes opaque.

Open standards provide the common language. Operational transparency supplies the record of how an organisation applies that language in a particular context: the controller identity, the notice presentation, the authorisation evidence, the rights access point, the processing context, and changes to the published position.

The objective is interoperability without forced uniformity. Québec, Canada, Europe and other jurisdictions use different legal terms and safeguards. A common record structure makes those differences visible and mappable instead of hiding them behind incompatible documents.

Pillar four: sovereignty, economy and sustainability

The manifesto connects digital sovereignty with local procurement, resilient organisations and sustainable development. That is also an information governance question.

When data is copied unnecessarily, retained without a clear purpose, or moved between systems without inspectable authority, the result is not only legal and security risk. It is duplicated infrastructure, avoidable storage and uncontrolled processing. A transparent purpose, retention and transfer record gives an organisation a basis for deciding what to collect, where to process it, and when to delete it.

Operational transparency does not measure environmental impact. It creates the evidence boundary within which location, processing volume, retention and supplier choices can be assessed honestly.

4 The operational transparency model

The chain of evidence is short, and the authority relationships in it should stay explicit.

1. **Controller identification record.** Who is accountable, in which jurisdiction, under what organisational authority.
2. **Transparency policy.** What purposes, legal bases, locations, parties, rights and controls are declared before any interaction.
3. **Notice record and presentation.** What was made available to the person before collection, identification or transfer.
4. **Notice receipt.** A reference to what was presented, without requiring the public register to identify the person.
5. **Authorisation or refusal evidence.** What permission was given, refused or withdrawn, in the context in which it occurred.
6. **Processing and change record.** What operational state relies on the authority, and when the purpose, location, recipient or control changes.

The chain should be both machine-readable and human-readable, resolvable before identification where possible, and it should support a rights access point without turning a public register into a surveillance mechanism against the people inspecting it.

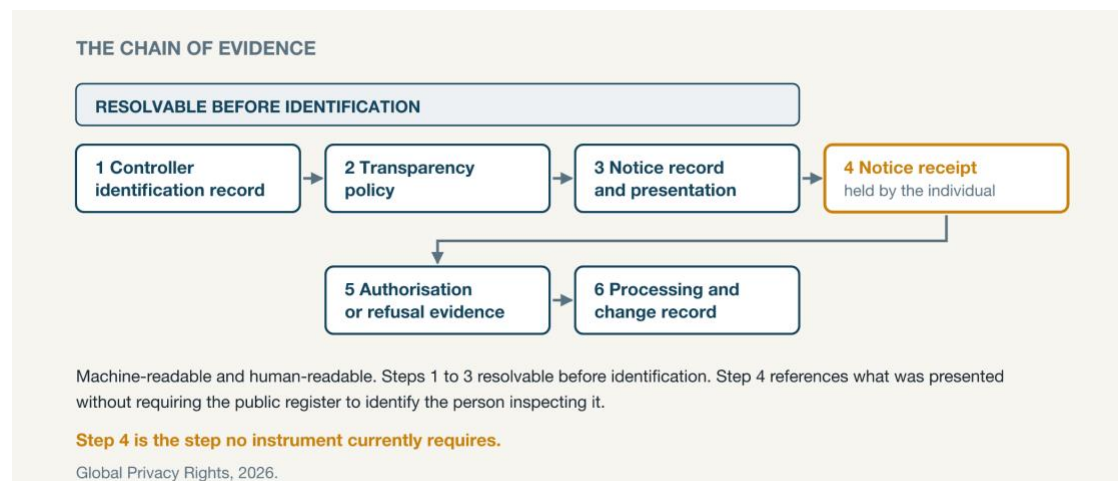


Figure 2. The chain of evidence. Steps one to three resolve before identification. Step four is the step no instrument assessed currently requires.

Figure 2. The chain of evidence. Steps one to three resolve before identification. Step four is the step no instrument assessed currently requires.

5 A proposed Digital Transparency Impact Assessment

This is proposed, not established. It extends a conventional data control assessment by asking whether the authority described in policy is visible in the operational record. Five questions.

Accountability. Who specifies the purpose, controls the data, stores it, processes it, and can change the processing? Are those roles named and distinguishable?

Jurisdiction and transfer. Where is the data stored and processed? Which jurisdiction governs the infrastructure, the controller, the processor, and the person? What happens when a location, recipient or transfer mechanism changes?

Authority and control. What can the controller do, the processor do, and the individual do? Can the individual inspect, refuse, withdraw or exercise rights without first surrendering unnecessary identity information?

Notice and evidence. What notice was presented first? Which identifiers, metadata, profiles or secondary purposes were disclosed? Can the notice and its version be resolved and verified later?

Security and exposure. What protects the transparency architecture itself? Does the system reveal who is inspecting whom? Can a public record be mirrored without exposing personal information? Does the event history make a material change visible?

The output is not a sovereignty certificate. It is a structured account of the evidence available, the authority boundaries, the unresolved risks and the actions required.

6 What the OPN project contributes, and what it does not

The OPN project is an open implementation project for operational transparency. It aligns with the disclosure requirements that Québec's Law 25 sets, and with international standards for notice and consent records. It does not certify compliance with Law 25 and makes no compliance claim.

It develops a public controller identification record, standardised notices, notice receipts, a notice event log, content-addressed records, and a public read side that can be copied and verified. Its role is not to replace a government, a regulator, a standards body or a court. It is to provide an open authority and evidence layer through which responsibility, purpose, jurisdiction, permission and change can be inspected before identification or data disclosure.

Global Privacy Rights is the Canadian operator and developer, working from Montréal, and the registry service is intended to run on Montréal-based infrastructure. That is a sovereignty decision, and it is stated as one: infrastructure location, operator, legal setting and transfer position should be visible together, rather than treating a local server as sufficient proof of control.

Where it actually stands, because the argument of this paper requires us to say so.

The assurance model is published at <https://globalprivacyrights.org/assurance> and every rung states what was not checked. Level 0 is live: a listing is self-asserted, it says so on its face, and it is a support and awareness signal rather than a certification. Verification against an authoritative source, and receipts that can be notarised, begin at Level 2, and

Level 2 is not yet built. Our own disclosure record is published at <https://globalprivacyrights.org/.well-known/transparency/cir.json> in the same form we ask of any listing.

A paper arguing that sovereignty claims should be inspectable has to survive being inspected. That is why the rung is stated rather than claimed.

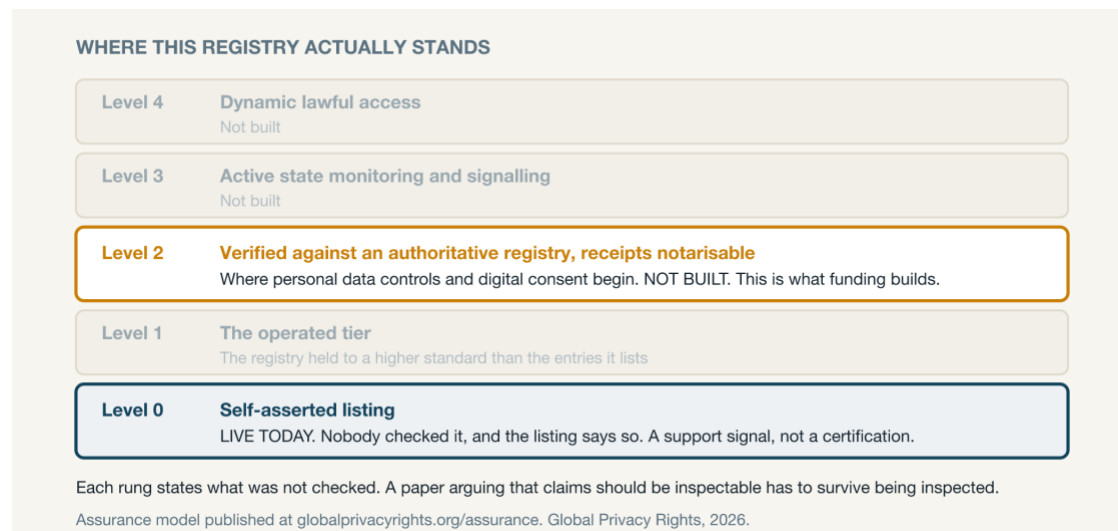


Figure 3. Where this registry stands on its own assurance model. Level 0 is live and self-asserted. Level 2, where verification and digital consent controls begin, is not built.

Figure 3. Where this registry stands on its own assurance model. Level 0 is live and self-asserted. Level 2, where verification and digital consent controls begin, is not built.

7 Local and foreign infrastructure

Local custody is appropriate where sensitivity, continuity and legal context require it, and it should be recorded as one part of a broader sovereignty assessment rather than as the conclusion of one.

A credible record discloses the physical and legal location of storage; the processing and support locations; the controller, processor and sub-processor roles; foreign law or extraterritorial access exposure where relevant; migration and exit arrangements; open standards and export formats; security and change controls; and the notice and rights mechanisms available to the person concerned.

That avoids two symmetrical errors. The first treats foreign infrastructure as automatically unacceptable without examining the actual authority and safeguards. The second treats local hosting as automatically sovereign without examining suppliers, software, access, transfer and operational control.

8 Why Québec, and a proposed collaboration

Québec has the strongest published accountability requirement in North America. Section 3.1 of its private sector Act requires the title and contact information of the person in charge of the protection of personal information to be published on the enterprise's website, and vests the function by default in the person exercising the highest authority. No federal Canadian instrument requires it, and neither does any framework we have assessed elsewhere. Our published assessment of the Act sets out both that strength and its limits, and is available at <https://globalprivacyrights.org/reports/whisspr-quebec-law-25-assessment-2026.pdf>.

The limit matters here, because it is the gap this paper is about. Law 25 requires the accountable person to be named publicly and binds the disclosure to the moment of collection, and it requires no record that either happened. The individual is given a cause of action with a statutory minimum award and nothing to bring to it.

So the sovereignty agenda in Québec starts from the best legal position on the continent and the same missing evidence as everywhere else. We propose a focused collaboration around four outputs.

1. **A shared vocabulary.** Map the four pillars onto controller identity, notice, authority, location, transfer, permission and change records, so that a sovereignty claim and a transparency record use the same terms.
2. **A worked assessment.** Apply the Digital Transparency Impact Assessment to one Québec or Canadian service, drawn from credit, health, public service delivery or cloud procurement.
3. **An open implementation profile.** Define the minimum machine-readable record an organisation publishes to make a sovereignty claim inspectable, without requiring a proprietary platform.
4. **A roadmap connection.** Add operational transparency as a cross-cutting workstream, linking local custody, exit planning, open standards, supplier governance and sustainable processing to the co-regulated governance of digital identification.

The work should begin with an evidence and vocabulary workshop, not with a claim that any party has already achieved digital sovereignty.

About Global Privacy Rights

Global Privacy Rights is a Canadian not-for-profit. It conducts and publishes research on what services actually disclose, through Transparency Lab, its lab, with Global Privacy Rights as publisher of record. Published assessments are available at <https://globalprivacyrights.org/research> and cover Bill C-36, Québec's Law 25, and China's AI Safety Governance Framework 3.0, with a comparative of all three produced on one method.

In Montréal it is the operator and developer of an operational transparency signalling registry, built as public infrastructure and running as a research and development pilot.

Sources and limits

This paper responds to the publicly published manifesto and roadmap of Données Souveraines Québec, at <https://www.donneessouveraines.quebec>. It is a position offered for discussion. It is not a joint statement, it is not endorsed by Données Souveraines Québec or by any public authority, and no endorsement should be inferred from it.

It does not repeat any quantitative or financial estimate from the manifesto. Statements about Québec's Law 25 rest on the official English consolidated text of chapter P-39.1 current to 10 June 2026, as assessed in the report cited in section 8. The French vocabulary should be reviewed by a French-language reader before any bilingual publication.

© 2026 Global Privacy Rights. This paper may be reproduced with attribution.