Verkada

Navigating the Canadian Privacy Landscape with Verkada

Disclaimer: This document is for informational purposes only and does not constitute legal advice. Organizations should consult with legal counsel to ensure their specific use of Verkada products complies with PIPEDA and applicable Canadian provincial privacy laws, including in Quebec (as recently amended by Law 25), Alberta and British Columbia.

A Collaborative Approach to Privacy: PIPEDA & Provincial Privacy Laws (QC, AB, BC)

The Canadian privacy landscape is evolving rapidly. Depending on where you operate, you may be required to navigate both federal requirements under Canada's Personal Information Protection and Electronic Documents Act (**PIPEDA**) and/or provincial requirements under Quebec's Act respecting the protection of personal information in the private sector (**Quebec Privacy Act**), Alberta's Personal Information Protection Act (**PIPA Alberta**) and British Columbia's Personal Information Protection Act (**PIPA BC**). In Quebec, this includes stringent obligations recently introduced by Law 25. At Verkada, we want to help simplify this process by providing the technical foundation and transparency you need to help you manage your data protection program across Canadian jurisdictions.

Shared Responsibility: Organizations and Service Providers
Privacy compliance in Canada is a shared responsibility. While the terminology differs slightly from the GDPR, the functional roles remain consistent:

- **You are the Organization (Accountable Entity):**
  Under Canadian privacy laws, the customer remains "accountable" for personal information under its control. For example, you determine the purposes for collection, set retention periods, and ensure "meaningful consent" is obtained from individuals. You decide which privacy features are appropriate for your specific environment.
  - » Legal Source: PIPEDA Schedule 1, Principle 4.1; Quebec Privacy Act, Section 3.1; equivalent provisions under PIPA Alberta and PIPA BC.

- **Verkada is the Service Provider:**
  We provide the infrastructure to help you secure and manage your data in accordance with our contractual obligations to you. Under Canadian privacy laws, when personal information is transferred to a service provider for processing, the transferring organization (i.e., the accountable entity) remains responsible for it.
  - » Legal Source: PIPEDA Schedule 1, Principle 4.1.3; Quebec Privacy Act, Section 18.3; equivalent provisions under PIPA Alberta and PIPA BC.

Operational Mapping: PIPEDA & the Quebec Privacy Act

The following table highlights how Verkada's platform maps to key Canadian regulatory requirements.

Requirement	How Verkada Helps	Legal References	Documentation & Resources
Accountability & Privacy Officer	Verkada's platform allows you to designate administrative roles. Under Canadian privacy laws, you must designate a person responsible for the organization's compliance with Canadian privacy laws (e.g., a Privacy Officer); our platform's audit logs help this designated person or their delegate(s) oversee data access permissions and monitor access.	PIPEDA Princ. 4.1; Quebec Privacy Act, Sec. 3.1	Verkada Help Center
Purpose & Consent	Our patented **Public Privacy Disclosures**, **including QR Codes**, enhance your ability to obtain "meaningful consent" by informing individuals of the purposes of surveillance before collection occurs.	PIPEDA Princ. 4.2 & 4.3; Quebec Privacy Act, Sec. 8	Display Privacy Notices
Individual Access Rights	Command includes self-service tools to export or delete footage, assisting you to respond to access and other data subject rights requests within the statutory 30-day limit.	PIPEDA Princ. 4.9 and Sec. 8; Quebec Privacy Act, Sec. 27	Verkada Help Center
Security Safeguards	We employ encryption at rest and in transit and are audited against ISO 27001/27701/27017/27018 and SOC 2, Type 2.	PIPEDA Princ. 4.7; Quebec Privacy Act, Sec. 10	Verkada Security Controls
Breach Notification	Verkada monitors for threats 24/7. We assist you in meeting your breach reporting obligations by notifying you without undue delay upon becoming aware of an incident that triggers our notification obligations to you.	PIPEDA Sec. 10.1; Quebec Privacy Act, Sec. 3.5	Security & Incident Response Data Processing Agreement
Privacy Impact Assessments (PIA)	We provide technical documentation to support your PIA. Under the Quebec Privacy Act, completion of a PIA is required for any project to acquire, develop or overhaul an information system involving the processing of personal information.	Quebec Privacy Act, Sec. 3.3	**Available upon request**

Data Residency & Transfers

Canadian Data Sovereignty

Verkada recognizes that data residency is a priority for Canadian organizations, particularly those in the public sector or those operating in Quebec.

- **Local Storage:**
  Customers can choose to store their camera video and image data in our **Canadian data region** on Canadian soil.

- **Transfer Assessments:**
  For organizations with operations in Quebec, the Quebec Privacy Act requires the completion of a privacy impact assessment before personal information is communicated outside the province. By selecting our Canadian data region for storage, you can simplify this assessment. Further, for data you transfer outside of Canada, Verkada is a registered participant in the Department of Commerce Data Privacy Framework. Its listing can be found here. We also agree to EU Standard Contractual Clauses in our Data Protection Addendum. For more information about Verkada's subprocessors, including their location, visit our website's Subprocessor page and sign up to receive notice of updates.
  » Legal Source: Quebec Privacy Act, Sec. 17.

Privacy Enhancing Technologies (PETs)

Verkada integrates specific technical measures designed to satisfy Canadian "Data Minimization" and "Openness" principles:

1. **Public Privacy Disclosures (QR Functionality):**
   Supports your ability to comply with PIPEDA's Openness principle. Visitors scan a code to see your privacy policy and contact details for your Privacy Officer.

2. **Privacy Regions:**
   "Block-out Zones" provide you functionality to ensure that your surveillance is limited to its stated purpose (e.g., monitoring a doorway) while respecting the reasonable expectation of privacy of individuals in sensitive areas (e.g., windows of adjacent buildings).

3. **Face Blur (Live and Archive):**
   Supports data minimization by blurring faces in real-time. For investigations, authorized users can apply blurring to bystanders during video export.

4. **Audit Logs:**
   PIPEDA and the Quebec Privacy Act emphasize accountability and safeguarding as key principles. Our immutable logs track every time video is viewed or exported, assisting organizations in meeting accountability and safeguarding obligations.

5. **Person of Interest (Faces Only):**
   Our facial recognition technology is disabled by default. If you choose to enable it, you can configure it to alert only on specific pre-determined profiles rather than identifying every person who enters the frame. "Faces Only" leverages Verkada's hybrid cloud architecture to decentralize the search process, performing facial analysis directly on the camera instead of in the cloud. When a person is detected, the camera's onboard processor creates a unique mathematical map of their facial features—a digital signature used solely for comparison. This signature is checked locally on the camera against the "Person of Interest" profiles you've designated; if there isn't a match, the biometric signature is instantaneously wiped from the camera's temporary memory and is never sent to the cloud. While the biometric signature is destroyed to protect privacy, the system still preserves a low-resolution thumbnail and basic attributes (like clothing color) in your "People History" logs. This allows you to still search for individuals based on their appearance without the system maintaining a permanent biometric record of their face.

6. **Retention Settings:**
   Verkada provides individually configurable retention settings at the device and platform level. You can select camera hardware with onboard storage ranging from 30 to 365 days for local, continuous recording. For added redundancy, the Command platform includes 30 days of cloud backup by default, which can be extended for long-term security needs.

Biometric Data in Quebec

Generally speaking, Quebec has the most stringent laws in Canada applicable to the processing of biometric data. Quebec's Act to establish a legal framework for information technology (**Quebec IT Act**) requires that organizations disclose to the **Commission d'accès à l'information** (**CAI**)**:**

- the use of a biometrics system to verify or confirm an individual's identity prior to utilizing such system (in addition to express consent of the individual); and/or

- the creation of a database of biometric characteristics and measurements no later than 60 days before the system is brought into service.

With respect to Verkada's biometrics capabilities, Verkada offers the following features:

- **Default Off:**
  Verkada's facial recognition is "Off" by default.

- **Granular Controls:**
  Our platform allows you to enable, disable, remove or disable facial analytics on a per-camera basis.
  - » Legal Source: Quebec IT Act, Secs. 44 and 45.