ONTARIO · MFIPPA READINESS

MFIPPA Compliance Brief

How a platform built in British Columbia against FOIPPA accommodates Ontario MFIPPA — the obligation-by-obligation crosswalk, the January 2027 timeline, and the limits of what a vendor can claim.

Prepared for	[Insert municipality name]
Service	TrueNorth Civic AI
Date	[Insert date]
Status	Vendor compliance brief — not legal advice

Contents

How to use this brief 3

1. Purpose and how to use this brief 3

2. Built in British Columbia against FOIPPA 4

3. Why FOIPPA experience transfers to MFIPPA 4

4. Obligation-by-obligation crosswalk 5

5. What changes on January 1, 2027 7

6. Bill 194: Ontario's AI governance requirements 7

7. What we claim — and what we do not 8

8. How TrueNorth supports a municipality 9

9. Next steps and contacts 10

How to use this brief

This brief is written for the person who will actually have to sign the Privacy Impact Assessment and answer questions from council: typically the Clerk, the CAO, or a designated privacy lead. It is deliberately short on marketing and long on the specifics a municipality needs.

THE SHORT ANSWER

Yes — TrueNorth can support an Ontario municipal deployment under MFIPPA. The platform's privacy and security architecture was designed against BC's FOIPPA, which imposes a stricter statutory data-residency rule than MFIPPA does. Ontario's privacy obligations are substantively aligned, and the remaining work is documentation: an MFIPPA-specific Privacy Impact Assessment and Ontario-specific governance templates, both of which are included in this kit.

HOW TO READ THE CROSSWALK

Section 4 is intentionally honest about equivalences. Where the two statutes differ in mechanism — for example, BC's statutory residency rule versus Ontario's risk-based expectation — the difference is stated rather than smoothed over. Municipal privacy reviewers tend to notice when a vendor overstates equivalence, and it costs more trust than it buys.

1. Purpose and how to use this brief

This brief does three things: it explains where TrueNorth came from and why a BC-built platform is a reasonable fit for an Ontario municipality; it maps each MFIPPA obligation to the corresponding FOIPPA obligation and to the control or document that addresses it; and it sets out the January 1, 2027 requirements in plain language, with a practical readiness sequence.

1. Confirm the deployment scope and the municipal programs it supports.
2. Read Section 4 with your privacy lead and note any obligation that needs local detail.
3. Complete the accompanying MFIPPA PIA template before first use.
4. Keep the completed brief and PIA with the procurement file and update them before any significant change in purpose.

2. Built in British Columbia against FOIPPA

TrueNorth Civic AI was founded in British Columbia and piloted with BC local governments. Its statutory research corpus, workflow templates, procurement materials and privacy documentation were all built BC-first, against the Freedom of Information and Protection of Privacy Act (FOIPPA).

Why the documents say "FOIPPA"	Our pre-approval kit, PIA template and procurement memo were authored for BC public bodies. The platform facts inside them — residency, encryption, retention, DLP — are province-agnostic. The statutory references are not, which is why this brief and the accompanying MFIPPA PIA template exist.
Why BC is the stricter test	FOIPPA Part 2.1 restricts the storage of, and access to, personal information outside Canada. MFIPPA contains no equivalent statutory residency mandate; Ontario treats residency as a risk-management and contractual expectation. Meeting the BC rule therefore exceeds the Ontario expectation.

In practical terms: the platform is already pinned to Canadian infrastructure because BC law required it. Ontario does not require it, but your municipality gets the benefit of it regardless.

3. Why FOIPPA experience transfers to MFIPPA

Ontario's own guidance describes the two statutes as substantially similar. The Freedom of Information and Protection of Privacy Manual published by Ontario states that "FIPPA and MFIPPA are considered substantially similar laws and are organized the same way."

Both Acts share the same architecture: a right of access to records, limited and specific exemptions, rules governing the collection, use, disclosure, retention and disposal of personal information, a duty to safeguard that information, and individual rights of access and correction. The differences that matter for a software deployment are narrower than the similarities.

TABLE 1 · JURISDICTION COMPARISON

Dimension	British Columbia (FOIPPA)	Ontario (MFIPPA)
Regulator	Office of the Information and Privacy Commissioner for British Columbia (OIPC)	Information and Privacy Commissioner of Ontario (IPC)
Residency	Statutory restriction on storage of and access to personal information outside Canada (Part 2.1)	No equivalent statutory residency mandate; addressed through safeguards, contracts and risk assessment
Privacy Impact Assessment	Long-standing expectation; formalized notice elements	Expressly mandatory in writing from January 1, 2027 (MFIPPA s.28(3)–(6))
Breach reporting	OIPC breach guidance and notification expectations	Mandatory RROSH reporting and individual notification from January 1, 2027
AI-specific law	FOIPPA applies; no standalone provincial AI statute	Bill 194 Schedule 1 adds AI transparency, accountability and oversight obligations for prescribed public sector entities
Records instruments	Personal information directories under FOIPPA	Personal information banks (PIBs)

This comparison is provided for orientation only. Your municipality's privacy and legal advisors determine how MFIPPA applies to a specific deployment.

4. Obligation-by-obligation crosswalk

The table below is the working version of the comparison. The final column identifies the specific control, document or configuration that supports the obligation. Bracketed items are completed by the municipality.

TABLE 2 · MFIPPA / FOIPPA CROSSWALK

Obligation	BC FOIPPA	Ontario MFIPPA	How TrueNorth supports it
Collection authority and necessity	Personal information may be collected only where authorized (FOIPPA s.26).	Collection must be expressly authorized by statute, for law enforcement, or necessary to a lawfully authorized activity (MFIPPA s.28).	Only account data and content staff choose to submit are collected. No background collection of resident data. The PIA template records purpose and necessity for each category.
Notice at collection	Notice at or before collection (FOIPPA s.27); PIA notice elements (s.69(5)).	Notice-of-collection requirements, including authority, purpose and contact information.	Pre-filled notice language and a notice checklist. The municipality inserts its own authority citation and privacy contact.
Limits on use	Use limited to the purpose collected or a consistent purpose (FOIPPA s.32).	Use limited to consent, the purpose collected or a consistent purpose (MFIPPA s.31).	Zero-training guarantee: customer content is never used to train models. Tenant policy controls and use-case templates constrain secondary use. No sale or reuse of content.

TABLE 2 · MFIPPA / FOIPPA CROSSWALK (CONTINUED)

Obligation	BC FOIPPA	Ontario MFIPPA	How TrueNorth supports it
Disclosure and service providers	Disclosure restricted; service-provider arrangements governed by FOIPPA.	Disclosure restricted (MFIPPA s.32), including to consultants and agents who need the record to perform their duties.	The vendor acts as a service provider under contract. Data is tenant-isolated, never disclosed to other customers, and subprocessors are identified. No disclosure for advertising or model training.
Retention and disposal	Information retained only as long as necessary; disposal requirements apply.	Retention for the prescribed period and disposal in accordance with the regulations (MFIPPA s.30).	Chat threads auto-purge at 30 days. Uploaded documents are retained 90 days by default and configurable by agreement. Deletion on request or at termination, confirmed in writing.
Safeguarding	Reasonable security arrangements are required.	Regulation 823 safeguards, plus an express statutory safeguarding duty from January 1, 2027.	TLS 1.3 in transit; AES-256 at rest; CMEK on qualifying plans; Cloud DLP redaction before model calls; role-based access; per-request tenant isolation; audit logging.
Access and correction	Individuals may request access to, and correction of, their personal information.	Part I access rights, including correction of personal information.	Audit trail and records export support access requests during the retention window. The municipality's FOI process remains the channel for formal requests.
Privacy Impact Assessment	PIA expected as part of privacy due diligence; notice elements specified.	Written PIA mandatory before collection from January 1, 2027; ten prescribed content elements (s.28(3)–(6)); copy to the IPC on request.	A pre-filled PIA mapped element-by-element to MFIPPA s.28(3), with data-flow, safeguards, retention and risk tables. The municipality reviews, completes and signs it.
Breach reporting	OIPC notification expectations for breaches involving personal information.	From January 1, 2027: assess against the RROSH threshold, report qualifying breaches to the IPC and notify affected individuals as soon as feasible; keep records.	Incident response commitments, audit logs and a named support channel. A breach-response workflow template aligned to the RROSH test is included in the kit.
AI-specific governance	FOIPPA applies to AI processing; no standalone AI statute.	Bill 194 Schedule 1: public information, accountability framework, risk management and human oversight for prescribed entities and circumstances.	Governance Hub with AI inventory, model registry, risk levels, self-assessments and transparency pages; human-in-the-loop checkpoints in every workflow.

5. What changes on January 1, 2027

Ontario's amendments arrived through Schedule 2 of Bill 194 (2024) and Schedules 7 and 11 of Bill 97 (2026). For a municipal institution, four changes matter most.

1. Now through December 31, 2026 — readiness. Complete or refresh the PIA for each AI tool before it collects personal information. Confirm the breach-response procedure, privacy contact and records-retention schedule. Update personal information banks and collection notices where an AI tool introduces a new use.
2. January 1, 2027 — mandatory PIAs. PIAs become expressly mandatory before collecting personal information, and must be updated before a significant change to the purpose for which information is used or disclosed. The PIA must be in writing and contain the ten prescribed elements, and a completed copy must be provided to the IPC on request.
3. January 1, 2027 — breach reporting and notification. The municipality must assess privacy breaches against the real risk of significant harm (RROSH) threshold, report qualifying breaches to the IPC as soon as feasible, and notify affected individuals. Breach records must be kept. The express statutory safeguarding duty also takes effect.
4. 2028 — first annual statistical report. Municipal institutions report breach statistics to the IPC beginning in 2028 for the 2027 reporting year, by March 31.

THE TEN PIA CONTENT ELEMENTS (MFIPPA S.28(3))

- The purpose for collecting, using or disclosing personal information, and why it is necessary.
- The legal authority the institution relies on.
- The types of personal information and how each is used or disclosed.
- The sources of the personal information.
- The position titles of officers, employees, consultants or agents with access.
- Any limitations or restrictions on collection, use or disclosure.
- The period of retention.
- Administrative, technical and physical safeguards, and risks to individuals.
- Steps to prevent or reduce those risks and mitigate harm.
- Any other prescribed information.

ONE PRACTICAL CONSEQUENCE FOR A SMALL TEAM

The PIA is not a procurement formality. It is a written record the municipality must be able to produce to the IPC on request. For a single system and a small user group, the practical approach is a short, complete PIA — roughly eight to twelve pages — rather than a large consulting document. The template in this kit is structured to that length.

6. Bill 194: Ontario's AI governance requirements

Schedule 1 of Bill 194 enacted the Enhancing Digital Security and Trust Act, 2024. Its AI provisions apply to "public sector entities," a definition that includes institutions within the meaning of MFIPPA — so Ontario municipalities are in scope.

The Act is framework legislation: it establishes the obligations, while the detailed requirements are left to regulations that are still being phased in. The practical position for a municipality today is in scope now, bound in detail later. The direction of travel is clear enough to prepare for.

TABLE 3 · BILL 194 OBLIGATION AREAS

Obligation area	What the Act contemplates	What a municipality can do now
Public information	Prescribed entities must publish information about their use of AI systems in prescribed circumstances.	Maintain a plain-language public page describing which AI tools are used, for what purposes, and how to ask questions.
Accountability framework	Develop and implement an accountability framework for AI use, with prescribed roles and documentation.	Adopt a short AI-use policy that names a responsible officer, approved tools, review requirements and escalation paths.
Risk management	Take prescribed steps to manage risks, including reporting and record-keeping.	Screen each tool with a PIA and an algorithmic impact assessment; record the risk level and mitigations.
Human oversight	In prescribed circumstances, disclose information and ensure an individual exercises oversight and can provide additional information.	Require named staff review before any AI output is used in a decision, communication or record.
Prohibited uses and standards	Regulations may prohibit certain uses and set technical standards.	Adopt an explicit “no autonomous decisions about individuals” rule and a vendor-review checklist.

The accompanying Bill 194 AI Readiness Checklist turns this table into a working document the municipality can complete and keep on file.

7. What we claim — and what we do not

Public-sector privacy review rewards precision. These are the boundaries we hold ourselves to.

WHAT WE DO CLAIM

Canadian data residency for all persistent data (Montréal); Gemini 3.x chat inference is processed in Google US/EU multi-regions (disclosed in the PIA); encryption in transit and at rest; customer-managed keys on qualifying plans; DLP redaction of Canadian identifiers before model calls; zero model training on customer content; role-based access and tenant isolation; audit logging; defined retention and deletion; documentation mapped to FOIPPA and MFIPPA.

WHAT WE DO NOT CLAIM

That this document is legal advice. That the platform by itself makes the municipality compliant. That the vendor holds its own SOC 2 or ISO certification. That Canadian residency eliminates every foreign legal risk. That a vendor-prepared PIA substitutes for the municipality’s own assessment and sign-off.

On certifications specifically: the platform runs on Google Cloud infrastructure whose facilities, networks and core services are covered by Google's SOC 2 Type 2 and ISO/IEC 27001 (plus 27017/27018) certifications. Those certifications apply to the underlying infrastructure; the application layer relies on the controls described in the security brief. TrueNorth does not assert an independent certification of its own.

On jurisdiction: the cloud provider is headquartered in the United States. Customer data is stored in Montréal, and Gemini 3.x model inference is processed in Google's US/EU multi-regions, but US legal instruments such as the CLOUD Act can theoretically reach providers headquartered there. We disclose that residual risk rather than describe the platform as "sovereign." The security brief sets out the mitigations.

8. How TrueNorth supports a municipality

A municipality does not need an enterprise governance program to adopt a single AI tool well. It needs a defensible set of documents, a small number of configured controls, and a vendor that answers the phone. The platform is designed so that the same controls serve a small office and a large department alike.

TABLE 4 · MUNICIPALITY SUPPORT MAP

What the municipality needs	How the platform and documents provide it
A PIA it can sign	Pre-filled PIA mapped to MFIPPA s.28(3), with vendor facts completed and municipality-specific fields bracketed for your privacy lead to complete and sign.
Administrative control	Staff, Admin and Super Admin roles. Tenant administration from a single settings area. Optional Microsoft Entra ID single sign-on so the municipality uses its existing Microsoft 365 identities.
Residency evidence	Production pinned to GCP northamerica-northeast1 (Montréal); environment validation refuses to start production in another region. Architecture and data-flow tables provided for the municipality's IT reviewer.
Retention the municipality can explain	30-day chat purge; 90-day document retention by default, adjustable by agreement; deletion at termination confirmed in writing. The retention schedule is written into the PIA so it matches the municipal records bylaw.
Predictable pricing	Published plans and current pricing are listed on truenorthcivicai.ca. The kit itself is free, and nothing in the approval path requires a paid engagement.
Someone to ask	A named contact for privacy and security questions, incident reporting and procurement follow-up: sales@truenorthcivicai.ca.

9. Next steps and contacts

1. Confirm the deployment scope — users, the programs they support, and whether Microsoft 365 single sign-on is preferred.
2. Complete the PIA using the MFIPPA template, with your privacy lead reviewing and signing. We will answer vendor questions in writing.
3. Choose the plan that fits your municipality. Current plans and pricing are published on truenorthcivicai.ca; the kit itself is free.
4. Configure and train — roles, retention, DLP behaviour, and a short staff orientation before first use.

Vendor contact	sales@truenorthcivicai.ca · truenorthcivicai.ca
Security and privacy	support@truenorthcivicai.ca — incident reports and disclosure inquiries.

This brief is provided for information and procurement support. It is not legal advice. Your municipality remains the institution responsible under MFIPPA for determining how the Act applies, for completing and approving its Privacy Impact Assessment, and for its own records, notice and breach-response practices. Statutory references were current as of October 2026; regulations under Bill 194 and Bill 97 continue to be phased in.