Bill 97 MFIPPA Readiness Checklist for Small Ontario Municipalities

Are you ready for January 1, 2027?

A plain-language self-assessment from Tectonix Technologies Inc. Fifteen minutes, no cost, no obligation.

What changed, in one minute

Bill 97, the Plan to Protect Ontario Act (Budget Measures), 2026, received Royal Assent on April 24, 2026. Schedule 11 extends to municipal institutions the privacy regime that provincial institutions have had since 2025. For your municipality, three duties take effect **January 1, 2027**:

1. **Privacy Impact Assessments (MFIPPA s. 28(3)).** Unless the regulations provide otherwise, a written assessment must be prepared before personal information is collected, and the Act prescribes eight items it has to contain. This is a standing process, not a one-time project.
2. **Breach reporting (MFIPPA s. 30.1).** A privacy breach must be reported to the Information and Privacy Commissioner and to the affected individual where there is a real risk of significant harm. Breach records have to be kept, and annual breach statistics reported to the IPC. The first municipal report covers 2027 and is due to the IPC in 2028.
3. **Safeguards (MFIPPA s. 30(5)).** An express statutory duty to protect personal information with reasonable administrative, technical and physical measures.

All three duties rest with the **head of the institution**, not the clerk personally, though the clerk usually does the coordinating. They apply to every institution MFIPPA covers, whatever its size and whether or not anyone on staff has privacy in their job description. Library, police services and conservation authority boards are caught the same way a township is.

The checklist

Tick only what is in place today. An unticked box is work to do before January 1, 2027.

A. Governance

- ☐ A named person is responsible for coordinating privacy compliance.
- ☐ Council or senior staff have been briefed on the January 1, 2027 obligations.
- ☐ There is a line in the 2027 budget for privacy compliance work, internal or external.
- ☐ The head of the institution understands the duties sit with them.

B. Privacy Impact Assessments

- ☐ You have a written PIA template or process ready to use.
- ☐ Staff know an assessment has to happen **before** any new collection of personal information: new software, new form, new program, new camera.
- ☐ Someone in the organization knows how to complete a PIA to the standard MFIPPA s. 28(3) sets out.
- ☐ You have identified the collections you already run, such as payroll, permits, recreation registration, bylaw enforcement and CCTV, and know which will need assessment.

C. Breach response

- [ ] You have a written breach-response plan: who to call, what to do, in what order.
- [ ] Staff can recognize a privacy breach, such as a misdirected email, a lost laptop or a wrong attachment, and know who to escalate it to for assessment.
- [ ] You know how to assess "real risk of significant harm" to decide when notification is required.
- [ ] You know how and where to notify the IPC, and how to notify affected individuals.
- [ ] You keep a record of privacy breaches, and know that annual statistics go to the IPC.

D. Safeguards

- [ ] Personal information is access-restricted to staff who need it.
- [ ] You have basic technical protections such as access controls, backups and encryption where appropriate, and could describe them if the IPC asked.
- [ ] Third-party vendors that touch your personal information are contractually required to protect it.
- [ ] You have reviewed physical security for paper records and for devices holding personal information.

E. Documentation

- [ ] Your privacy practices are written down, not just habit.
- [ ] You could hand the IPC your assessments, breach records, policies and safeguards documentation if it asked.

Reading your score

There are 19 boxes. Count the ones you ticked.

15 to 19. Most of the core elements are in place. Check that your records actually back up each item you ticked.

8 to 14. Start with Sections B and C. They take the longest because they require new processes, written records and staff instructions.

7 or fewer. Start by assigning an owner and putting the breach-response process in writing. Without those, the first breach becomes the moment you work out who assesses it, who reports it and to whom.

What happens if you are not ready?

Bill 97 expands the IPC's oversight. It can review an institution's information practices where there are reasonable grounds to believe the Act has been contravened, and it can make compliance orders. In practice that means that after a breach the IPC may ask to see your assessments, your breach records and your safeguards documentation. Those are easier to write now than under a deadline set by someone else.

Where to go next

The IPC publishes free guidance and worksheets. Start with these:

Planning for Success: Privacy Impact Assessment Guide, which includes downloadable PIA worksheets.

FIPPA and MFIPPA amendments FAQ, alongside the IPC's updates on obligations for provincial and municipal institutions.

Those cover how the work is done. This checklist is about where your institution stands before you start.

Where Tectonix fits

Tectonix Technologies Inc. is a small Canadian corporation providing MFIPPA readiness reviews and privacy impact assessments to small Ontario municipalities. Sahib Johar, the Principal Consultant, leads every engagement directly, and scope and fees are confirmed in writing before any work starts.

To talk through the items you could not tick, a scoping call costs nothing. Reply to this email or write to **booking@tectonix.ca**.

Sahib Johar, CIPP/C, CISSP
Principal Consultant | Tectonix Technologies Inc.
tectonix.ca

Last reviewed 2026-08-17.