BILL 150

Readiness Roadmap

A Compliance Planning Tool for Nova Scotia Municipalities

PREPARING FOR APRIL 1, 2027

A scored, plain-language compliance planning tool aligned to the *Freedom of Information and Protection of Privacy Act (Chapter 13, Acts of 2025).*

Prepared for the
NSFM Spring Conference
May 1, 2026

Allan Haggett

Sovereign Copilot

allan@sovereigncopilot.ca

How to Use This Tool

This is a scored planning tool for the transition to full Bill 150 compliance by April 1, 2027. It is ordered by lead time — the longest and hardest tasks come first. Each stage carries a point value reflecting its statutory weight and risk-reduction value, not the effort required to complete it.

Target: 100 points by April 1, 2027.

Recommended cadence: report your score monthly to your senior management team or council as a single-line governance indicator.

Example: "Bill 150 Readiness Score: 58 / 100. On track for 75 by February 2027."

WHAT THE SCORE IS — AND WHAT IT IS NOT

An honest disclaimer about the scoring

This score is a project-management tracking tool. It is not a compliance attestation and carries no legal or regulatory weight. The Information and Privacy Commissioner does not recognise a numeric "readiness score." What the Commissioner will recognise are the artifacts each stage produces: a privacy policy, a privacy assessment report, a data residency register, a tool suitability log, training records.

Use the score to communicate progress. Use the artifacts to demonstrate compliance. The two are different things, and conflating them is the most common failure mode of frameworks like this one.

Data Lifecycle Annex

As a reference to the management of data assets, this roadmap is accompanied by Annex D — **How Personal Information Moves Through Your Municipality**, a plain-language guide to the data lifecycle under Bill 150.

Legislative Context and Scope

Bill 150 (formally *An Act Respecting the Right of Access to Records of Public Bodies and the Right of Privacy with Respect to Personal Information Held by Public Bodies, Chapter 13 of the Acts of 2025*) was assented to on October 3, 2025 and takes effect on April 1, 2027. It replaces both the *1993 Freedom of Information and Protection of Privacy Act* and *Part XX of the Municipal Government Act*, consolidating provincial and municipal privacy and access law into a single statute.

For municipalities, the most material changes are:

- A statutory obligation to maintain a privacy policy and a public-facing privacy-complaint procedure (s. 52).
- A mandatory privacy assessment before launching or substantially changing any new program, system, or activity that handles personal information (s. 53).
- A privacy breach notification regime with a defined "significant harm" threshold (s. 78).
- Restrictions on storing, accessing, or disclosing personal information outside Canada (s. 76), with a separate hard deadline of May 1, 2027 for new contracts (s. 147).
- An expanded role for the Information and Privacy Commissioner, including powers to authorize the disregard of an access request, conduct reviews, and inspect premises (Parts III and IV).

PRIVACY ASSESSMENT or PRIVACY ASSESSMENT

> A **Privacy Assessment (PA)** , also referred to as a **Privacy Assessment (PA)** is a mandatory review conducted by a public body to evaluate the collection, use, or disclosure of personal information in its activities according to requirements set by the regulations.
>
> These assessments are required before the launch of any new project, program, or system involving personal data, or before implementing substantial changes to an existing initiative.
>
> The PA process is described in detail in Annex A.

Planning Timeline

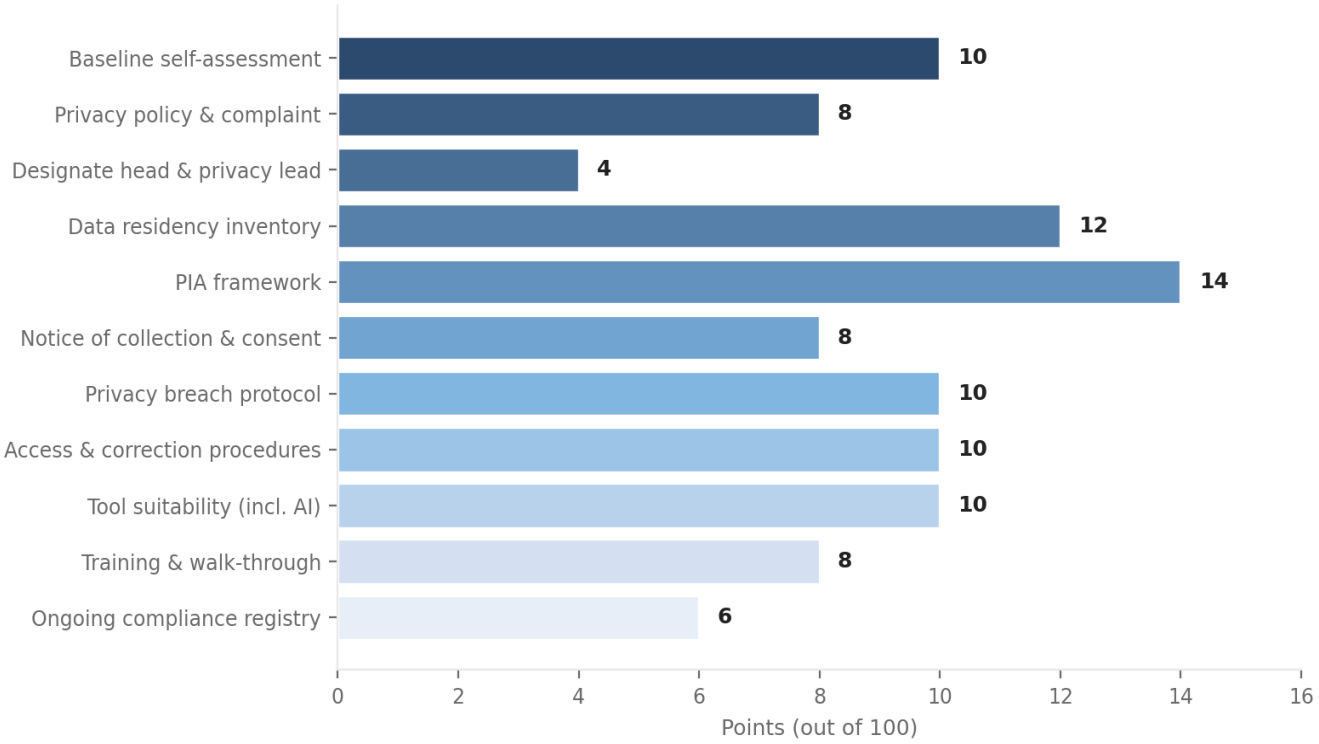
Working backwards from April 1, 2027. Adjust to your municipality's capacity. Cumulative score targets are shown beneath each milestone.

Cumulative Readiness Score (target by date)

Period	Focus	Cumulative target
May–Aug 2026	Foundations: governance roles, privacy policy, complaint procedure, data residency inventory, PA framework	**32**
Sep–Oct 2026	Visibility: notice-of-collection updates, breach protocol, AI/shadow tool audit	**50**
Nov–Dec 2026	Governance: tool suitability process, access and correction procedures	**70**
Jan–Feb 2027	Validation: training delivery, scenario walk-through	**86**
Mar 2027	Sign-off: CAO/Clerk readiness certification, ongoing-compliance registry	**94**
Apr 1, 2027	Act takes effect. Quarterly review cycle begins.	**100**

Stage Weighting

Points are assigned by statutory weight and risk-reduction value, not by the effort required. Foundational obligations (privacy policy, PA framework, data residency) carry more weight than downstream operational items. AI governance is treated as a subset of general tool suitability, not a free-standing pillar — Bill 150 does not mention AI by name.



The eleven stages (including the baseline self-assessment) sum to exactly 100 points.

Baseline Self-Assessment

Complete this baseline before beginning any stage. One point per "yes," up to ten. This establishes your starting score.

#	Question	Pts
1	Do you have a current, written privacy policy that meets the requirements of Bill 150 s. 52?	1
2	Have you formally designated a "head" of your local public body under s. 134, by bylaw or other instrument?	1
3	Do you have a complete inventory of all software tools and systems that process personal information?	1
4	Do you know whether each of those tools stores, processes, or transmits data outside Canada?	1
5	Do you have a documented privacy breach response protocol consistent with s. 78?	1
6	Do you have a documented process for responding to access-to-information and correction requests?	1
7	Do your collection forms (online and paper) include the notice required by s. 56?	1
8	Have you conducted a Privacy Assessment in the last 24 months?	1
9	Do you have a written acceptable-use policy governing staff use of new software, including AI tools?	1
10	Have your senior staff received any formal training on Bill 150 or the modernised FOIPOP?	1

Your baseline score: ____ / 10

0–3: start at Stage 1 immediately. 4–6: foundations exist; focus on the gaps. 7–10: well advanced; use the roadmap to formalise and document what you have.

The Stages

Stages are ordered by lead time, longest first. Each stage states the Bill 150 requirement, the standard operating procedure, the artifact you must produce, the responsible role, and the point value. Each stage also includes a "single clerk path" recognising that many Nova Scotia villages and rural municipalities operate with minimal administrative staff.

STAGE 1

Privacy Policy and Complaint Procedure

8 points • Target: June 2026 • *Bill 150 s. 52*

WHY IT'S HERE

Section 52 requires every public body to "establish and maintain a privacy policy meeting the requirements prescribed by the regulations" and to make its internal privacy-complaint procedures available to the public. This is the single most basic obligation under Part II and is likely the first thing a Commissioner's review would look for. It is foundational; almost every other stage assumes it exists.

STANDARD OPERATING PROCEDURE

- Draft a privacy policy covering: purposes of collection, categories of personal information held, custody and control, retention, security arrangements, complaint procedures, and contact information for the head and any designated privacy lead.
- Adopt the policy by council resolution.
- Publish the policy on the municipality's website and make a printed copy available at the municipal office.
- Draft a public-facing internal complaint procedure that explains how a resident can raise a privacy concern, the timelines for response, and the right to escalate to the Commissioner under s. 101.

ARTIFACTS PRODUCED

1. Adopted Privacy Policy
2. Public Privacy Complaint Procedure
3. Council resolution
4. Publication record

OWNER

CAO or Clerk, with council approval.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (8 points available)

- Privacy policy drafted: 2 pts
- Privacy policy adopted by council: 2 pts
- Complaint procedure drafted and published: 2 pts
- Both documents posted publicly and at municipal office: 2 pts

STAGE
2

Designate the Head and Privacy Lead

4 points • Target: June 2026 • *Bill 150 s. 134, s. 135*

WHY IT'S HERE

Section 134 requires every local public body to designate, by bylaw or other legal instrument, the person or group of persons who will act as "head" for the purposes of the Act. Section 135 permits delegation of the head's powers and duties. Without this designation in writing, no other obligation under the Act can be cleanly discharged. It is a small administrative item with disproportionate downstream consequences.

STANDARD OPERATING PROCEDURE

- Confirm whether the existing CAO or Clerk is automatically the head under s. 3 of the Act, or whether a formal designation by bylaw is required.
- Pass a designation bylaw or resolution naming the head.
- Where appropriate, delegate specific powers and duties under s. 135 to a named privacy lead, in writing, with any limitations or conditions.
- File the designation and any delegations with the municipal records.

ARTIFACT PRODUCED

Designation bylaw or resolution. Written delegation instrument (if applicable).

OWNER

Clerk, with council approval for the bylaw or resolution.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (4 points available)

- Head designation in place: 2 pts
- Written delegation instrument filed (if applicable): 2 pts

STAGE
3

Data Residency and Tool Inventory

12 points • Target: August 2026 • *Bill 150 s. 76, s. 147*

WHY IT'S HERE

Section 76 prohibits the disclosure, storage, or access of personal information outside Canada except in accordance with the regulations. Section 147 imposes a separate, hard deadline of May 1, 2027 for new contracts: contracts with a commitment date on or after that day fall under the new rules; existing contracts continue under the previous Personal Information International Disclosure Protection Act until they end. The municipality must therefore know, for every tool, where the data lives — and must be able to evidence that knowledge before any procurement decision after April 1, 2027.

STANDARD OPERATING PROCEDURE

- Build a register of every tool, system, and service that processes personal information. Include vendor, primary data location, sub-processors where known, and contract end date.
- Classify each entry: data stored in Canada; data stored outside Canada under a known exception; data stored outside Canada with no exception; status unknown.
- For each entry that is non-compliant or unknown, capture the contract commitment date — this determines whether s. 76 (new rules) or the legacy rules apply.
- Draft a remediation plan: replace, reconfigure, renegotiate, or document an applicable exception. Tie the plan to the contract end dates to align replacement with renewal cycles.

ARTIFACT PRODUCED

Data Residency Register. Remediation Plan tied to contract renewals.

OWNER

Clerk or designated privacy lead, with input from any IT contractor.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (12 points available)

- Inventory of all personal-information-handling tools complete: 4 pts
- Each tool classified for data residency status: 4 pts
- Remediation plan with contract commitment dates documented: 4 pts

STAGE 4

Privacy Assessment Framework

14 points • Target: August 2026 • *Bill 150 s. 53*

WHY IT'S HERE

Section 53 requires a privacy assessment before undertaking any **new** project, program, system, or activity involving the collection, use, or disclosure of personal information, and before substantially changing one. Subsection 53(3) confirms that this obligation is forward-looking — projects already in operation when the Act takes effect are not retroactively subject to s. 53. Building a PA framework from scratch may take weeks: a template, trigger criteria, a review process, and at least one trained person. Everything downstream depends on it.

STANDARD OPERATING PROCEDURE

- Develop a PA template scaled to a small municipality. Required elements: project description, data inventory, risk assessment, mitigation strategy.
- Define written trigger criteria for what constitutes a "new" or "substantially changed" project, system, or activity.
- Establish a review and approval workflow with a named sign-off authority (typically the head or delegate).
- Pilot the framework on one real upcoming project to validate it before April 1, 2027.

ARTIFACT PRODUCED

PA Template. PA Trigger Criteria Checklist. PA Review and Approval Log. One completed PA on a pilot project.

OWNER

Clerk or designated privacy lead.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (14 points available)

- PA template created: 4 pts
- Trigger criteria documented: 3 pts
- Review and approval workflow established: 3 pts
- First PA completed on a real project using the framework: 4 pts

STAGE
5

Notice of Collection and Authority to Collect

8 points • Target: September 2026 • *Bill 150 s. 54, s. 55, s. 56*

WHY IT'S HERE

Sections 54 and 55 limit when and how personal information may be collected. Section 56 requires that the individual be informed, at the time of collection, of (a) the purpose for collection, (b) the legal authority to collect, and (c) the contact information of an officer responsible for answering questions about the collection. Most municipal forms — building permit applications, recreation registrations, dog licences, library memberships — do not currently meet this obligation. Remediating forms is mechanical but volume-intensive, and is best done before the Act takes effect.

STANDARD OPERATING PROCEDURE

- Inventory every form, online and paper, that collects personal information.
- Draft a standard notice-of-collection block specifying purpose, legal authority, and contact.
- Apply the notice to every form. For forms with multiple collection purposes, draft a tailored notice.
- Review each form's collection against the s. 54 authority test: is this collection authorised by an enactment, necessary for an operating program, or otherwise within s. 54?

ARTIFACT PRODUCED

Form Inventory. Standard Notice-of-Collection Block. Updated forms (online and paper). Collection-Authority Map (form to s. 54 basis).

OWNER

Clerk, with departmental owners for sector-specific forms (recreation, planning, etc.).

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (8 points available)

- Form inventory complete: 2 pts
- Standard notice-of-collection drafted: 2 pts
- All forms updated with notice: 2 pts
- Collection-authority map documented: 2 pts

STAGE
6

Privacy Breach Protocol

10 points • Target: October 2026 • *Bill 150 s. 78, s. 79*

WHY IT'S HERE

Section 78 requires the head of a public body, on becoming aware of a privacy breach where it is reasonable to believe an affected individual could experience significant harm, to notify both the individual and the Commissioner. Section 78(1) defines "significant harm" in nine categories — identity theft, significant bodily harm, significant humiliation, damage to reputation or relationships, and others. A small municipality is most likely to encounter a breach through email misdirection, lost equipment, or a contractor incident. A protocol drafted before a breach is far cheaper than one drafted during one.

STANDARD OPERATING PROCEDURE

- Draft a breach response protocol covering: detection, internal escalation to the head, containment, the s. 78 significant-harm assessment (with a checklist mapped to the nine categories), notification to affected individuals and the Commissioner, and post-incident review.
- Identify a backup decision-maker for the case where the head is unavailable.
- Maintain a breach log even for incidents that do not meet the notification threshold — the pattern matters for governance.
- Run one annual scenario walk-through (see Stage 10).

ARTIFACT PRODUCED

Privacy Breach Response Protocol. Significant-Harm Assessment Checklist. Breach Log Template.

OWNER

Head of public body. CAO or Clerk in most municipalities.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (10 points available)

- Protocol drafted: 4 pts
- Significant-harm checklist completed: 3 pts
- Breach log template created and live: 3 pts

STAGE 7

Access and Correction Procedures

10 points • Target: November 2026 • *Bill 150 Part I, ss. 12–29; ss. 61–68*

WHY IT'S HERE

Part I prescribes detailed procedures for receiving and responding to access requests (30 business days, with extensions and fee rules) and Part II ss. 61–68 prescribes the parallel correction-request procedures. Section 68 imposes a one-year obligation to track who else received the personal information so that corrections can be propagated. Most municipalities have informal practices that do not match the statute precisely. Updating procedures now avoids procedural appeals later.

STANDARD OPERATING PROCEDURE

- Document the end-to-end access-request workflow, including receipt, fee estimate (s. 26), severance (s. 10), third-party notice (s. 50), response (s. 23), and review/appeal pathways (ss. 80, 90).
- Document the parallel correction-request workflow including the s. 67 annotation requirement and the s. 68 disclosure-recipient tracking.
- Build a disclosure register: when personal information is shared with a third party or another public body, log it for one year so corrections under s. 68 can be propagated.
- Train the staff member who will operate these procedures.

ARTIFACT PRODUCED

Access Request Workflow. Correction Request Workflow. Disclosure Register. Standard response and notice templates.

OWNER

Clerk or designated FOIPOP administrator.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (10 points available)

- Access workflow documented: 3 pts
- Correction workflow documented: 3 pts
- Disclosure register operational: 2 pts
- Response and notice templates ready: 2 pts

STAGE
8

Tool Suitability Process (including AI)

10 points • Target: December 2026 • *Bill 150 s. 53 (PA trigger); s. 76 (residency); s. 58 (security)*

WHY IT'S HERE

Once the PA framework (Stage 4) and data residency rules (Stage 3) are in place, the municipality needs a single, lightweight gate that every new tool — AI or otherwise — must pass through before being adopted. This stage covers all software, not only AI. AI is included as a special case requiring additional explainability questions, but Bill 150 itself does not single AI out, and neither should the suitability process.

STANDARD OPERATING PROCEDURE

- Create a one-page Tool Suitability Form covering: purpose, personal information involved, data residency (per Stage 3), security arrangements (s. 58), and whether a PA is triggered (per Stage 4).
- For AI-capable tools, add three additional questions: can the tool's logic be explained to a resident or to the Commissioner? Is there a human signatory for any decision the tool informs? Does the tool retain or train on inputs?
- Establish a review authority. In a single-clerk municipality, this is the Clerk, advised by the IT contractor and council where material.
- Maintain an Approved Tool Register and a Rejected Tool Log with reasons.
- Conduct one shadow-tool survey: ask staff what they are already using informally. Cross-reference against the Approved Tool Register.

ARTIFACT PRODUCED

Tool Suitability Form. Approved Tool Register. Rejected Tool Log. Shadow Tool Audit Report.

OWNER

Clerk or CAO.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (10 points available)

- Suitability form created: 3 pts
- Review authority established and first three tools assessed: 3 pts
- Shadow tool audit completed: 2 pts
- Approved and rejected tool registers operational: 2 pts

STAGE
9

Training and Walk-Through

8 points • Target: February 2027 • *Implicit; required for defensible compliance*

WHY IT'S HERE

Compliance is only defensible if staff understand and follow the procedures. This stage validates everything above. The walk-through (a scripted scenario, not a generic "tabletop exercise") tests the protocols against a realistic incident.

STANDARD OPERATING PROCEDURE

- Deliver training to all staff who handle personal information, covering: the privacy policy and complaint procedure (Stage 1), notice-of-collection requirements (Stage 5), the breach protocol (Stage 6), the access and correction procedures (Stage 7), and the tool suitability process (Stage 8).
- Conduct one scripted walk-through. Suggested scenario: a resident whose building permit was denied asks under s. 12 for the records used in the decision and under s. 61 for correction of an error in those records. Walk through receipt, fee estimate, severance, third-party notice, response, and the s. 68 register update.
- Capture training attendance and the walk-through findings.

ARTIFACT PRODUCED

Training Materials. Training Attendance Records. Walk-Through Summary and Findings.

OWNER

CAO or Clerk.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (8 points available)

- Training materials prepared: 2 pts
- Training delivered to all relevant staff: 3 pts
- Walk-through completed and findings logged: 3 pts

STAGE
10

Ongoing Compliance Registry

6 points • Target: March 2027 • *Implicit; supports defensible compliance over time*

WHY IT'S HERE

Compliance is not a one-time event. The municipality must maintain auditable records of ongoing governance. This stage converts the readiness project into a recurring operations cycle.

STANDARD OPERATING PROCEDURE

- Establish a quarterly review cycle for the Approved Tool Register, the Data Residency Register, and the Disclosure Register.
- Schedule annual PA reviews for all active programs that handle personal information.
- Add a standing agenda item to senior staff or council meetings for compliance reporting (one line: the readiness score plus any open items).
- Final readiness sign-off by CAO or Clerk before April 1, 2027.

ARTIFACT PRODUCED

Quarterly Review Schedule. Annual PA Review Calendar. Standing Agenda Item Template. CAO/Clerk Readiness Sign-Off.

OWNER

CAO or Clerk.

Single clerk path: where the municipality has no separate IT or privacy roles, the Clerk or CAO discharges all responsibilities under this stage. The artifact, not the title, is what matters.

SCORING (6 points available)

- Quarterly review schedule established: 2 pts
- Annual PA calendar set: 2 pts
- CAO/Clerk readiness sign-off completed: 2 pts

Milestones — What the Score Means

These thresholds describe organisational state, not legal sufficiency. The Commissioner does not recognise the score; the Commissioner recognises the artifacts.

5 — **Baseline**
Self-assessment complete. You know where you stand.

25 — **Visibility**
You know what tools you have and where data flows.

50 — **Control**
Policy, governance, and ownership are in place.

75 — **Evidence**
Artifacts exist and are auditable by the Commissioner.

100 — **In-force ready**
All stages complete. Operational maintenance ongoing.

If You Do Nothing Else: The Five Things

If your municipality cannot complete the full roadmap before April 1, 2027, we would recommend that start with at least these five things. They cover the most acute statutory exposure, with the least staff time.

We are in no way recommended that shortcuts be taken, but we are sensitive to resource limitations.

#	Action	Stage / Section	Why
1	**Adopt a privacy policy and publish a complaint procedure**	Stage 1 — s. 52	This is the most basic statutory obligation under Part II. A council resolution and a website page can discharge it in a single afternoon of preparation.
2	**Designate the head in writing**	Stage 2 — s. 134	A one-paragraph bylaw or resolution. Without it, no other obligation is cleanly discharged.
3	**Inventory your tools and their data locations**	Stage 3 — s. 76, s. 147	You cannot answer the Commissioner without it. The contract date matters: May 1, 2027 is the procurement deadline.
4	**Update collection forms with a notice-of-collection**	Stage 5 — s. 56	Mechanical, low-cost, and the most visible form of compliance to residents.
5	**Draft a privacy breach response protocol**	Stage 6 — s. 78	Cheaper to write before a breach than during one.

About the author

This roadmap was prepared by Allan Haggett, an IT business analyst with 30 years' experience bridging technical complexity and executive decision-making, mostly in highly regulated environments. He has delivered multiple integration projects for the French government, the Canadian Navy, Canadian Air Force, and financial services clients. Currently at Cambridge Financial in Halifax, Allan specializes in financial systems integration and AI adoption. He has delivered AI strategy sessions to Nova Scotia nonprofits and business groups.

Allan and his team at Sovereign Copilot (sovereigncopilot.ca) are currently developing a Bill 150 compliant version of Sovereign Copilot, a deterministic, data sovereign, compliance retrieval system for Canadian municipalities that returns cited answers from verified municipal documents — with a complete audit trail of every query made.

Annex A — Privacy Assessment Overview

A Privacy Assessment (PA) is a formal assessment conducted by a public body to determine whether a new or significantly changed project, program, system, or activity meets the privacy requirements of Bill 150 and its regulations.

Minimum Requirements

At a minimum, a PA must include:

- Project Description — a detailed overview of the project, program, or service.
- Data Inventory — the specific personal information that will be collected, used, or disclosed, including from whom and on what authority.
- Risk Assessment — an evaluation of the potential risks to personal privacy, considering sensitivity, volume, and disclosure pathways.
- Mitigation Strategy — the measures that will be taken to mitigate identified risks, mapped one-to-one against them.

The Artifact

The PA report is the record of the assessment. It serves as evidence of compliance and must be produced if the Information and Privacy Commissioner requests it for review.

Record Keeping

The head of the public body is required to maintain the record of the PA results. This ensures the public body remains accountable for the privacy decisions made during development.

Grandfathering — s. 53(3)

Section 53(3) is important: PIAs are not required for projects, programs, systems, or activities that were already undertaken or instituted on or before the date the Act comes into force. The PA obligation is forward-looking. Existing systems do not need to be retroactively assessed under s. 53, though substantial future changes to them will trigger the obligation.

Wilful Misconduct vs. Accidental Breach

Bill 150 distinguishes between wilful misconduct (offences under s. 139, with fines up to $10,000 for individuals and $50,000 for corporations under s. 140) and accidental privacy breaches (handled under s. 78). The fines apply only where the act was wilful. Mistakes are addressed through breach notification, not prosecution.

Annex B — Statutory Cross-Reference

Each stage of this roadmap maps to specific sections of Bill 150. This table is provided so the document can be defended to a Commissioner, an auditor, or council.

Stage	Title	Bill 150 Sections
1	Privacy Policy and Complaint Procedure	s. 52
2	Designate the Head and Privacy Lead	s. 3 (definition of head); s. 134; s. 135
3	Data Residency and Tool Inventory	s. 76; s. 147 (transitional)
4	Privacy Assessment Framework	s. 53
5	Notice of Collection and Authority to Collect	ss. 54, 55, 56
6	Privacy Breach Protocol	ss. 78, 79
7	Access and Correction Procedures	Part I (ss. 12–29); ss. 61–68
8	Tool Suitability Process	s. 53 (trigger); s. 58 (security); s. 76 (residency)
9	Training and Walk-Through	Implicit
10	Ongoing Compliance Registry	Implicit

Annex C — Authoritative Resources

This roadmap is unofficial.

The following are the authoritative sources for Bill 150 compliance in Nova Scotia. They should be consulted before any formal compliance decision is made.

- Bill 150 itself — Chapter 13 of the Acts of 2025. The legislation prevails over any guidance, including this document, where they conflict.
- Office of the Information and Privacy Commissioner for Nova Scotia (oipc.novascotia.ca) — the regulator. Watch for guidance documents specific to Bill 150 implementation.
- Service Nova Scotia — the department responsible for the general supervision and management of the Act under s. 9. Watch for regulations published under s. 143.
- Nova Scotia Federation of Municipalities (NSFM) and the Association of Municipal Administrators of Nova Scotia (AMANS) — check for sector-specific training and peer guidance.

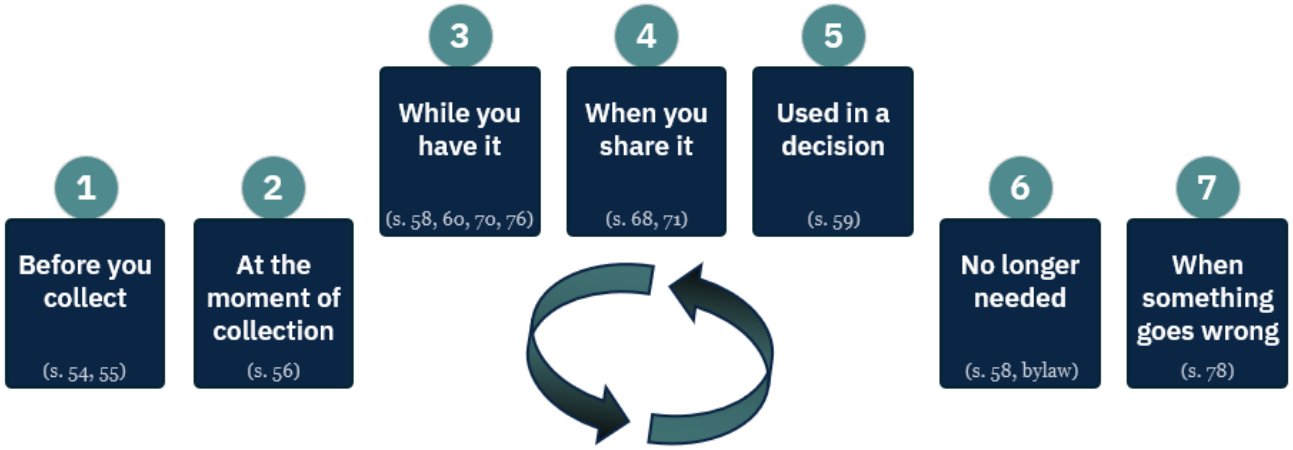
Feedback, corrections, and suggestions are welcome. Subsequent versions will incorporate the regulations as they are published.

Annex D — How Personal Information Moves Through Your Municipality

Here we provide a plain-language overview of the data lifecycle from the point of view of Bill 150 This is meant for municipal staff and management who are not IT specialists.

The filing-cabinet way of thinking

For most of municipal history, "personal information" meant paper in a filing cabinet. The cabinet had a key, the key had an owner, and you could see who came in and out. Bill 150 still works that way — it just applies the same idea to anything that holds personal information, paper or digital. If you can think about a filing cabinet, you can think about Bill 150.
The Act follows information through seven moments in its life. Each moment has a rule.



What about information you already have?

Bill 150 takes effect on April 1, 2027 [171]. It does not require you to delete, migrate, or re-paper personal information you already hold on that date. The Act is forward-looking. Your existing records, existing forms, and existing systems do not become non-compliant simply because the Act comes into force.

Three specific reassurances:

Privacy Assessments are not retroactive [53(3)]. Section 53(3) confirms that PIAs are required only for new projects or for substantial changes to existing ones [53(1)]. You do not need to assess every system you already operate.

Existing contracts continue under the old data-residency rules [147(2)]. Section 147 protects contracts signed before May 1, 2027 — they continue under the previous Personal Information International Disclosure Protection Act until the contract ends, including any renewals already provided for [147(2)]. Plan to align replacement with renewal cycles, not with the April 1 date.

Forms collected under the old rules are not retroactively defective. The s. 56 notice-of-collection obligation applies to collections made on or after April 1, 2027 [56(1), 171]. You do not need to re-contact every resident who ever filled out a permit application.

In short: Bring new things into compliance from April 1, 2027 onward, and bring older things into compliance as they renew, change substantially, or as your retention bylaw catches up with them. No emergency migration is required.