PIA checklist

Data hosting and personal information processing for Quebec law firms

Legal review: to be completed before definitive publication

Working version dated August 20, 2026

What this worksheet is for

This checklist helps a law firm document a privacy impact assessment before a project involving personal information, especially where a service provider may process or store it outside Quebec. It structures the work; it does not replace the PIA report or legal analysis tailored to the firm.

How to use it

- [ ] Appoint an owner and attach supporting contracts, evidence, and data-flow diagrams.
- [ ] Assess compliance, risks, and safeguards in the firm's actual operating context.
- [ ] Review the PIA when the provider, location, purpose, or sensitivity of the data changes.

Assessment record

Project or provider name _____

Assessment owner _____

Person in charge of the protection of personal information _____

Assessment start date _____

Decision date _____

Next review date _____

Scope, attachments, and people consulted

01 Define the project and its necessity

Describe what the firm needs to accomplish before assessing a tool or provider.

- [ ] The purpose is specific, legitimate, and understood by the people concerned.
- [ ] The firm has explained why the project is necessary and which problem it solves.
- [ ] Less intrusive options have been identified and compared.
- [ ] The personal information collected, used, or disclosed is limited to what is necessary.
- [ ] Volume, frequency, duration, and categories of people concerned are documented.
- [ ] Solicitor-client privilege and other duties specific to the firm are part of the assessment.

Notes, rejected options, and rationale

02 Map the information and data flows

A simple map should show where each data category enters, travels, is copied, and leaves.

- [ ] Personal information categories and sensitivity levels are inventoried.
- [ ] Source systems, backups, logs, attachments, and test environments are included.
- [ ] Each service provider, processor, and subprocessor is named with its role.
- [ ] The country and, where possible, hosting and processing region are confirmed in writing.
- [ ] Support, administrative, and emergency access from outside Quebec are identified.
- [ ] Transfers to calendars, email, analytics, or artificial intelligence services are included.
- [ ] Export, return, and deletion at the end of the contract are tested or documented.

Flows, locations, providers, and supporting evidence

03 Review the legal and contractual framework

Section 17 requires a prior PIA where personal information is disclosed or stored outside Quebec.

- [ ] The firm has determined whether information will be disclosed, processed, or stored outside Quebec.
- [ ] The legal framework applicable in each relevant jurisdiction has been assessed.
- [ ] Sensitivity, purpose, and safeguards have been taken into account.
- [ ] The level of protection has been found adequate in light of the identified risks.
- [ ] A written agreement defines roles, permitted uses, confidentiality, and security safeguards.
- [ ] The agreement addresses incidents, notices, audits, subprocessors, government requests, and termination.
- [ ] Commercial promises have been verified in the contract, not only on a marketing page.

Legal advice, clauses to negotiate, and references

04 Assess risks and safeguards

Assess likelihood and severity before and after safeguards are applied.

- [ ] Risks of unauthorized access, disclosure, alteration, loss, or destruction are described.
- [ ] Risks related to privileged access, shared accounts, and subprocessors are assessed.
- [ ] Encryption in transit and at rest, key management, and technical limits are documented.
- [ ] Multifactor authentication, roles, audit logs, and access revocation are addressed.
- [ ] Backups, continuity, restoration, and recovery testing are assessed.
- [ ] Retention periods and verifiable deletion are configured.
- [ ] An owner, due date, and evidence are assigned to each compensating measure.
- [ ] Residual risk is explicit and accepted by a person with the required authority.

Risk register, safeguards, owners, and due dates

05 Decide, deploy, and monitor

A useful PIA remains connected to decisions and continues to evolve after launch.

- [ ] Launch prerequisites and stop criteria are written down.
- [ ] Users are trained on settings, prohibited uses, and incident response.
- [ ] The project is reflected in the firm's policies, records, notices, and procedures.
- [ ] A post-launch control confirms that actual data flows match the PIA.
- [ ] Changes to the provider, subprocessors, and processing locations are monitored.
- [ ] A review is triggered by a material change or incident.
- [ ] Evidence, versions, approvals, and decisions are retained with the PIA report.

Deployment, monitoring, and review plan

Decision and approval

- [ ] Approved
- [ ] Approved with conditions
- [ ] Deferred until safeguards are implemented
- [ ] Rejected

Reasons for the decision _____

Conditions and deadline _____

Approver's name and role _____

Signature _____

Date _____

Legal review completed by _____

Comments and reservations

Official starting sources

1. Act respecting the protection of personal information in the private sector, s. 17
2. Commission d'accès à l'information, PIA guidance
3. Commission d'accès à l'information, guides and templates

General information only. This worksheet is not legal advice and does not establish that a project is compliant. Have the assessment adapted and reviewed for your situation before making a decision.