Quebec Law 25 Compliance Checklist for Microbusinesses

2727 Coworking · 2727 Coworking · 2026-09-19 · quebec law 25 compliance checklist · law 25 small business · quebec privacy law · privacy officer · efvp · privacy impact assessment · saas compliance · data breach response · virtual office privacy

Executive Summary

Quebec's private-sector privacy law applies to an enterprise handling personal information in the course of business, whether it holds the information itself or through another party (legisquebec.gouv.qc.ca). The Commission d'accès à l'information (CAI) expressly includes sole proprietors and self-employed workers (cai.gouv.qc.ca). There is no general exemption for a business with **1 to 20 people**. The practical minimum is therefore not a large compliance department. It is named accountability, a current data map, written rules proportionate to the business, usable notices, request and incident procedures, and evidence that those controls operate.

The person exercising the enterprise's highest authority is the default privacy officer. That function may be delegated **in writing**, but the highest-authority person remains accountable (legisquebec.gouv.qc.ca) (cai.gouv.qc.ca). The officer's title and contact details must be public. Governance policies must cover retention and destruction, staff roles through the data life cycle, and complaints, while remaining proportionate to the enterprise's nature and scope (legisquebec.gouv.qc.ca).

The most consequential decision point is a new **customer relationship management system (CRM), software as a service (SaaS), cloud platform or artificial intelligence (AI) tool**. A privacy impact assessment, called an évaluation des facteurs relatifs à la vie privée (EFVP) in Quebec, is required for a project to acquire, develop or overhaul an information system or electronic service delivery system involving personal information (legisquebec.gouv.qc.ca). A separate EFVP is required before communicating personal information outside Quebec, and the transfer must receive adequate protection and be governed by a written agreement reflecting the assessment (legisquebec.gouv.qc.ca). The compact workflow is: describe the project and data, confirm triggers, assess necessity and proportionality, map locations and recipients, identify risks and controls, approve conditions, sign the contract, then revisit the EFVP when the project changes.

If a confidentiality incident occurs, log **every** incident, assess sensitivity, likely consequences and likelihood of harmful use, consult the privacy officer, contain the event, and notify the CAI and affected people promptly when serious injury is possible (cai.gouv.qc.ca). Keep the register for at least **five years** (cai.gouv.qc.ca). Access and rectification requests generally require a written answer within **30 days** (legisquebec.gouv.qc.ca). A **90-day** rollout can put this minimum system in place, but a template alone is not compliance. The test is whether the records match actual collections, systems, vendors, decisions and deletions.

Introduction and Background

This report is a **Quebec Law 25 compliance checklist** for owners and operations leads at businesses with 1 to 20 people. “Law 25” is shorthand for the reform statute that amended Quebec privacy laws. The day-to-day rules discussed here are now found mainly in the consolidated Act respecting the protection of personal information in the private sector and its regulations. The CAI’s implementation schedule ran from **September 22, 2021 to September 22, 2024**, with most provisions taking effect on September 22, 2023 (cai.gouv.qc.ca). Portability followed on **September 22, 2024** (cai.gouv.qc.ca).

Scale matters operationally, but not as a blanket exemption. Civil Code article 1525 defines carrying on an enterprise to include an organized economic activity performed by one or more people (legisquebec.gouv.qc.ca). A solo consultant’s first prospect spreadsheet, a startup’s first employee file and a small shop’s online booking system can therefore create real duties. The legal definition covers information about a natural person who can be identified directly or indirectly.

This is an operational research guide, not individualized legal advice. It separates statutory duties from recommended controls. A five-person agency and a twenty-person clinic should not use identical safeguards because sensitivity, quantity, purpose, distribution and storage differ. Governance must be proportionate to the enterprise’s activities. The correct objective is a small, traceable system that grows when business events increase risk. ISO states that its privacy-management standard can be used by any organization handling personally identifiable information (iso.org).

Applicability, Accountability and the Minimum Governance Pack

Decide whether the private-sector law applies

Begin with activities, not headcount. List each place the business handles information about customers, employees, contractors, applicants, prospects, website visitors and business contacts. The Act generally applies when personal information is handled while carrying on an enterprise. Specified business-contact information connected with a person's duties receives narrower treatment, and journalistic, historical or genealogical material used for legitimate public information is excluded (legisquebec.gouv.qc.ca). Public bodies and certain health and social-services information operate under specialized regimes, so a regulated business should map overlapping laws rather than assume Law 25 is the only rule.

The first accountability actions are concise:

- **Name the owner.** Record the highest-authority person as privacy officer unless a written delegation says otherwise.
- **Publish the contact.** Put the officer's title and contact information on the website, or make it available through another appropriate means if there is no website (legisquebec.gouv.qc.ca).
- **Fund the role.** The CAI says the delegate should receive the necessary human, technical and financial resources (cai.gouv.qc.ca).
- **Approve governance.** Have the officer approve the written policies and practices, then retain dated approval evidence.

Assemble six working records

A microbusiness does not need six lengthy manuals. It needs six linked records that reflect reality. Quebec public-sector implementation material also identifies size, activities, resources, clientele and information holdings as useful tailoring factors (quebec.ca):

- **Data inventory.** Category, person type, purpose, source, system, access roles, vendor, location, retention trigger and disposal method. A regulator's private-sector self-assessment likewise asks for an inventory of collected personal information (oipc.bc.ca).
- **Retention schedule.** Minimum or maximum period, event that starts the clock, legal basis, system owner and destruction evidence. There is no universal period suitable for every organization (priv.gc.ca). Clear internal procedures should set minimum and maximum retention periods (priv.gc.ca).
- **Public privacy information.** The collection notice, technology-facing privacy policy, privacy-officer contact, governance summary and complaint route.
- **Rights procedure.** Identity check, intake date, search locations, exceptions review, response approval, delivery and closure.

- **Vendor and EFVP file.** Screening questionnaire, assessment, approved safeguards, contract, data location, subprocessor changes and review date. Canadian guidance says owned, contracted and otherwise used systems should all be in baseline-control scope (cyber.gc.ca).
- **Incident file.** Triage form, decision log, notification templates, incident register and lessons learned.

The federal privacy regulator recommends inventorying what information is retained, why and for how long (priv.gc.ca). NIST similarly recommends mapping data from collection to disposal and adopting formal disposal policies (nist.gov) (nist.gov). Those are implementation methods, not substitutes for Quebec law.

Notices, Consent, Retention and Individual Requests

Build the notice from the data map

Before collecting information, confirm a serious and legitimate reason and determine the purposes. Collect only what is necessary for those purposes by lawful means (legisquebec.gouv.qc.ca). At collection, explain purposes and means, access and rectification rights, withdrawal of consent, and, where relevant, the possibility of communication outside Quebec. On request, further information includes internal access categories, retention duration and the privacy officer's contact details.

A business collecting through technological means must publish or otherwise disseminate a privacy policy in simple, clear language (legisquebec.gouv.qc.ca). The CAI says the policy should identify relevant third parties and contexts, safeguards, cookies where applicable, rights, remedies and policy changes (cai.gouv.qc.ca). A regulator self-assessment also treats retention periods as a written-policy component (oipc.bc.ca). People must be notified when that policy changes (cai.gouv.qc.ca).

Treat consent as a decision, not a checkbox

Valid consent must be manifest, free, informed and tied to specific purposes. It must be requested for each purpose in simple, clear terms, and a written request must stand apart from other information (legisquebec.gouv.qc.ca). Express consent is required for the use or communication of sensitive personal information (legisquebec.gouv.qc.ca). The CAI advises interpreting consent exceptions restrictively (cai.gouv.qc.ca).

For prospect lists, do not treat a prior interaction as unlimited permission. Commercial prospecting is not a compatible secondary purpose under the private-sector Act (legisquebec.gouv.qc.ca). Federal anti-spam rules may also apply. Federal guidance says an inquiry can support implied consent for only **six months**, and unsubscribe requests must be implemented within **10 business days** (ised-isde.canada.ca) (ised-isde.canada.ca).

Run requests against a calendar

Use a single intake address and immediately record the due date. An access or rectification request must be in writing from a person who establishes identity. The privacy officer must answer in writing no later than **30 days** after receipt; silence is deemed refusal (legisquebec.gouv.qc.ca). Access is free, subject to reasonable reproduction or transmission charges, and a refusal must be reasoned and cite its statutory basis.

Portability covers eligible computerized information in a structured, commonly used technological format, subject to serious practical difficulties. Information created or inferred by the business and information obtained from third parties are excluded (cai.gouv.qc.ca). Rectification applies to inaccurate, incomplete or equivocal information. Deindexing or cessation of dissemination exists only under specified conditions, so it should not be described as an unconditional deletion right.

Once purposes are fulfilled, destroy the information or anonymize it for serious and legitimate purposes, subject to applicable retention law (legisquebec.gouv.qc.ca). De-identified information remains personal information and is not equivalent to destruction (cai.gouv.qc.ca).

Event-to-Obligation Checklist

Table 1 converts common microbusiness events into an owner, minimum evidence and review cycle. “Trigger review” means the privacy officer determines which duty applies, rather than presuming every event requires the same paperwork.

Business event	Immediate obligation and control	Owner	Evidence and review
First customer or prospect list	Confirm a serious and legitimate reason, define each purpose, necessity and consent basis before collection. Provide the notice at collection.	Privacy officer plus sales lead	Inventory row, notice version, consent record; review when fields or purposes change.
First employee or applicant	Inventory recruitment, payroll, benefit and performance records. Limit access to people who need the information for their duties (cai.gouv.qc.ca).	Privacy officer plus employer	Access matrix and retention schedule; review at hire, role change and departure.
New CRM, SaaS, cloud or AI tool	Pause procurement for an EFVP trigger decision. Map inputs, outputs, vendor access, model use, locations, retention, deletion and portability. Vendor review should include unauthorized-access notice, end-of-contract destruction and data-centre location (cyber.gc.ca).	Project owner plus privacy officer	Trigger memo, EFVP, approval conditions, contract; revisit on material change.
Data sent or accessible outside Quebec	Complete the cross-border EFVP before communication. Confirm adequate protection and execute a written agreement.	Privacy officer plus contract owner	Country and subprocessor map, legal-context assessment, safeguards, signed agreement.
New website form, analytics or cookies	Update collection notice and privacy policy. Make privacy settings highest by default where the statutory rule applies, noting the browser-cookie exception.	Product or web owner	Screenshots, settings export, policy version and change notice.
Virtual office, mailbox or shared workspace	Treat mail scanning, visitor interactions, shared desks and meeting-room conversations as handling points. Define authorized recipients, private conversations, screen locking, paper transport and secure storage.	Privacy officer plus workspace user	Workspace checklist and authorized-name list; review at plan, staff or mail-process change.
Confidentiality incident	Contain, preserve facts, assess serious injury, log every incident, notify when threshold is met and track remediation.	Incident lead plus privacy officer	Incident register, assessment, notices, corrective-action record.

Business event	Immediate obligation and control	Owner	Evidence and review
Access, rectification, portability or eligible deindexing request	Verify identity, start the **30-day** clock, search mapped systems, document exceptions, approve and securely deliver.	Privacy officer	Intake, search log, decision, response and closure date.
Purpose fulfilled or account closed	Check legal holds and category-specific retention, then destroy or properly anonymize. Obtain vendor deletion evidence.	System owner plus privacy officer	Deletion report, certificate or anonymization decision; sample quarterly.

The matrix makes a microbusiness's compliance system event-driven. The same event can activate several rows. Adding a cloud CRM, for example, can change the notice, consent design, vendor contract, outside-Quebec analysis, retention method and request search procedure. A virtual office does not transfer accountability to the workspace provider. It adds physical and vendor handling points that the business must control. Contracts should define security requirements and data handling (priv.gc.ca).

EFVP, Vendors, Cloud and Transfers Outside Quebec

Recognize the three EFVP triggers

The three operational triggers most relevant here are:

- **Information systems and electronic services.** Acquisition, development or overhaul involving collection, use, communication, retention or destruction of personal information requires an EFVP. An off-the-shelf tool is not automatically outside the trigger. The CAI states that an EFVP is required for every covered system project (cai.gouv.qc.ca).
- **Communication outside Quebec.** Conduct an EFVP before the communication, including when a person or body outside Quebec will collect, use, communicate or retain information for the business (legisquebec.gouv.qc.ca).
- **Research disclosure without consent.** A distinct process applies before disclosure without consent for study, research or statistical production (cai.gouv.qc.ca).

Use a compact six-step workflow

Table 2 is a defensible EFVP workflow for a small organization. It scales depth to the data and project, not to a fixed page count.

Step	Decision questions	Minimum evidence
1. Describe	What business outcome, system change and information life cycle are proposed?	One-page project description, data-flow diagram and system owner.
2. Trigger	Is this acquisition, development or overhaul? Will information be communicated or processed outside Quebec? Is research disclosure involved?	Dated trigger decision, including reasons if no EFVP proceeds.

Step	Decision questions	Minimum evidence
3. Necessity and proportionality	Is each field necessary? Are purpose, sensitivity, quantity, distribution and storage medium proportionate?	Field-level necessity review and risk rating.
4. Vendor and geography	Who can access the data, where, through which subprocessors, for how long, and under which legal framework?	Vendor answers, location map, subprocessor list and contract gaps.
5. Controls and residual risk	Can collection be reduced? Are access, encryption, logging, export, deletion, incident notice and continuity adequate?	Mitigation owner, due date, test and residual-risk decision.
6. Approve and revisit	Did the privacy officer participate from the outset? What conditions apply? What change requires reassessment?	Signed decision, contract, launch checklist and review trigger.

The statutory proportionality factors include sensitivity, purposes, quantity, distribution and storage medium. The privacy officer must be consulted from the outset and can recommend project controls, assigned responsibilities, documentation safeguards and training (legisquebec.gouv.qc.ca). The CAI advises revisiting the EFVP when the project changes, including an agreement change or system overhaul (cai.gouv.qc.ca). Before deployment, official UK guidance likewise recommends SaaS security due diligence (ncsc.gov.uk).

Put safeguards into the contract and the configuration

A service mandate involving necessary disclosure must be written. The contract should limit use to performing the mandate, prevent retention after expiry, require prompt notice of a confidentiality violation or attempt, and permit the privacy officer to verify compliance (legisquebec.gouv.qc.ca). For cross-border handling, also capture destination law, contractual safeguards, adequate protection and any risk mitigation in the written agreement.

Practical diligence should test the service, not merely collect a policy link:

- **Identity and access.** Require unique accounts, least privilege, multifactor authentication for administrators and timely offboarding. The Canadian Cyber Centre recommends two-factor authentication for cloud administrator accounts (cyber.gc.ca).
- **Central administration.** Manage SaaS centrally and assign the correct access level to each user (ncsc.gov.uk). Apply role-based least privilege (ico.org.uk).
- **Data location.** Record primary, backup, support and disaster-recovery locations. Canadian guidance recommends evaluating the legal jurisdictions where providers store or use sensitive information (cyber.gc.ca).
- **Incident operations.** Set notice channels, timing, minimum facts, evidence preservation and cooperation duties. Treat the cloud provider as a vendor in supply-chain management (ised-isde.canada.ca).
- **Exit and deletion.** Confirm export format, return, backup aging and deletion evidence. The federal regulator recommends secure disposal when information no longer serves the business (priv.gc.ca).
- **Operational security.** Enable automatic patching where suitable, encrypted backups and restoration tests (cyber.gc.ca) (tsapps.nist.gov).

For a coworking or virtual-office user, add locked paper storage, private conversations, locked screens and controlled mail handoff. Physical access to personal-information storage should be restricted (priv.gc.ca). Official guidance recommends private areas for sensitive conversations, a clear-desk rule and locking a computer when leaving a workstation (gov.uk) (gov.uk) (gov.uk). Remote-work guidance recommends taking only necessary records for a finite period, transporting paper in a locked bag and encrypting portable devices (oipc.ab.ca) (oipc.ab.ca) (oipc.ab.ca). Paper records should remain in locked cabinets when not in use, and sensitive mail can use tracked delivery where appropriate (ico.org.uk) (ico.org.uk).

Incident Response and Evidence

A confidentiality incident includes unauthorized access, use or communication, loss, or another breach of protection. When there are reasonable grounds to believe one occurred, the business must take reasonable measures to reduce injury and prevent recurrence. The serious-injury assessment considers **sensitivity**, **anticipated consequences** and the **likelihood of injurious use**, with the privacy officer consulted (legisquebec.gouv.qc.ca). If serious injury is possible, notify the CAI and affected individuals promptly.

Table 3 is a severity worksheet. It structures the statutory factors without inventing a numeric notification threshold.

Factor	Questions to record	Evidence
Sensitivity	Does the information concern finances, identity credentials, health, employment, precise location or another sensitive context? Was it encrypted or otherwise unreadable?	Data categories, classification, sample records and key status.
Anticipated consequences	Could use affect finances, identity, dignity, employment, safety, reputation or access to services? What protective steps are available?	Scenario analysis and mitigation options.
Likelihood of injurious use	Who received or could access it? Was access confirmed? Can the information be recovered, revoked or remotely erased?	Logs, recipient confirmation, device status and containment results.
Overall decision	Does the combination present a risk of serious injury? What facts support the decision?	Officer consultation, dated rationale and approval.

Do not use a point score as an automatic substitute for judgment. The register must include all incidents, even those that do not present serious-injury risk. Required records include circumstances and dates, discovery date, estimated affected count, serious-injury reasoning, notice dates and corrective measures. Keep and update the register for at least **five years** after awareness.

The response sequence is:

- **Contain.** Disable access, recover records, preserve logs and prevent recurrence.
- **Triage.** Identify systems, information, people, time period, recipients and third parties.
- **Assess.** Apply the three statutory factors and consult the privacy officer.
- **Notify.** If the serious-injury threshold is met, notify the CAI and affected people promptly. Only three specified circumstances permit a public notice instead of direct notice (cai.gouv.qc.ca).

- **Record.** Log the incident regardless of notification outcome, then update the record as facts change.
- **Improve.** Assign corrective actions, test completion and feed changes into training, contracts and EFVPs.

A concise evidence binder should hold the appointment or delegation, public-contact screenshot, approved governance pack, dated inventory, notices, consent records, request log, incident register, EFVPs, vendor contracts, training attendance, access reviews and deletion evidence. The Canadian baseline organizes security into **13 control categories** (cyber.gc.ca). CyberSecure Canada also asks applicants to review and implement **13 controls**, and its certification mark is valid for **two years** (ised-isde.canada.ca) (ised-isde.canada.ca). ISO/IEC 27701:2025 describes a privacy information management system as something established, implemented, maintained and continually improved (iso.org). A microbusiness can apply that cycle without seeking certification.

Data Analysis and Evidence

Small firms are not an edge case. Quebec had **228,622 small employer businesses with 1 to 99 employees** in December 2024 (ised-isde.canada.ca). Micro-enterprises with 1 to 4 employees accounted for **59.1%** of Canadian businesses, while more than three quarters had 1 to 9 employees (ised-isde.canada.ca) (ised-isde.canada.ca). Nationally, businesses with **1 to 19 employees represented 91.2%** of employer businesses and employed **4.5 million people**, or **24.4%** of employment, in 2024 (www150.statcan.gc.ca) (www150.statcan.gc.ca). The checklist therefore addresses the dominant employer-size segment, not a niche.

Technology adoption makes the EFVP decision operationally important. In the second quarter of 2026, **19.9%** of Canadian businesses with 1 to 4 employees reported using AI to produce goods or deliver services during the previous year (www150.statcan.gc.ca). Among those AI-using microbusinesses, **24.0%** trained existing staff and **10.7%** used external consultants or vendors (www150.statcan.gc.ca) (www150.statcan.gc.ca). OECD evidence found **41%** of small businesses acquired cloud-computing services in 2021 (oecd.org). Different populations and periods prevent direct comparison, but both datasets show that vendor and system change is routine.

Preparedness data reveal a documentation gap. In 2023, **26%** of Canadian businesses had written cybersecurity policies. Statistics Canada's survey had a final sample of **12,462 enterprises** and a **71% response rate**, giving the estimate useful national context (www150.statcan.gc.ca) (www150.statcan.gc.ca). In a separate BDC poll of **484 respondents** in September 2024 (bdc.ca), **37%** reported an informal cyber-incident plan, **52%** reported no plan and **76%** performed regular backups (bdc.ca) (bdc.ca). These studies measure cybersecurity, not Law 25 compliance, and should not be treated as breach-rate or compliance-rate estimates. They support one narrower conclusion: written, tested operating procedures cannot be assumed in small firms.

The enforcement framework is consequential but should not be converted into a probability claim. A monetary administrative penalty for an enterprise can reach the greater of **$10 million or 2% of worldwide turnover** for the preceding fiscal year (cai.gouv.qc.ca). The enterprise penal-fine range begins at **$15,000** and can reach the greater of **$25 million or 4% of worldwide turnover** (cai.gouv.qc.ca). Administrative penalties apply to specified failures, not automatically to every imperfect document. No available evidence supports a microbusiness-specific probability of penalty, and none should be invented.

30/60/90-Day Implementation Plan

The sequence below prioritizes visibility, high-frequency events and proof of operation.

Days 1 to 30: establish control

- **Appoint.** Confirm the highest-authority person or sign a written delegation. Publish the officer's title and contact details.
- **Inventory.** Interview each process owner and map customer, prospect, employee, applicant, website, mail, access-control and vendor data.
- **Freeze blind procurement.** Require a privacy trigger check before activating a new CRM, cloud service, AI tool or electronic service.
- **Open the registers.** Create request, incident, vendor and EFVP logs, even if initially empty.
- **Contain obvious exposure.** Remove shared accounts, turn on multifactor authentication, restrict file permissions, lock paper and encrypt portable devices.
- **Set leadership.** Assign IT-security responsibility to a leadership role and connect that role to the privacy officer (cyber.gc.ca).

Days 31 to 60: align public promises and operations

- **Set retention.** Assign a trigger and period to each inventory category. Record external legal requirements and define destruction evidence.
- **Rewrite notices.** Match each form, call script, contract intake and employee workflow to actual purposes and disclosures.
- **Publish governance information.** Provide the clear-language policy and complaint route, then record the version and approval date.
- **Clear the vendor queue.** Assess active vendors by sensitivity, quantity, location and access. Start with payroll, CRM, email, cloud storage, analytics, AI and virtual-office handling.
- **Train by role.** Give short scenarios to sales, operations, managers and administrators. A regulator's self-assessment frames staff guidance around expectations for collection, use and disclosure (oipc.bc.ca).

Days 61 to 90: test and evidence

- **Run a request drill.** Retrieve one sample person's data from email, CRM, file storage and vendors; test export and secure delivery within the **30-day** window.
- **Test backups.** Verify that backup data is encrypted, access is restricted and a restoration actually works (cyber.gc.ca).

- **Test restoration.** NIST separately recommends regular backups and tests of those backups (tsapps.nist.gov).
- **Run an incident exercise.** Test intake, containment, factor assessment, contact lists, CAI notice preparation and register completion. Canadian guidance recommends a written plan that states who is responsible (cyber.gc.ca).
- **Finish priority EFVPs.** Resolve safeguards and contract amendments before high-risk launches or cross-border communications.
- **Delete a real cohort.** Apply the retention schedule to an eligible category and retain deletion evidence.
- **Report to the owner.** Record open risks, exceptions, overdue actions and the next quarterly review.

The outcome at day 90 should be a working control loop. Quarterly reviews can sample new systems, access lists, incidents, requests, vendor changes and deletions. Annual review should reapprove governance, refresh training and reconcile the public policy to the inventory. For mobile devices, the CIS Controls navigator specifies an automatic lock period no longer than **two minutes** (cisecurity.org). This is a recommended benchmark, not a Quebec statutory deadline.

Implications and Future Directions

The central management implication is that privacy work should attach to change management. Procurement, hiring, marketing, product releases, workspace changes and offboarding are better control points than an annual policy rewrite. This reduces the chance that a system is launched before its EFVP, contract, notice and deletion method are understood.

AI adoption makes field-level necessity and vendor transparency more important. A microbusiness should record whether prompts contain customer or employee information, whether the provider uses inputs to improve models, where processing occurs, how administrators access content, what export is available and how deletion reaches backups. The EFVP should distinguish an internal productivity experiment from an electronic service delivered to customers, but neither should bypass the trigger decision. NIST describes multifactor authentication as one of the fastest and least expensive protections available (tsapps.nist.gov).

Cloud and shared workspace models also reinforce shared responsibility. Canadian cloud guidance states that the customer’s accountability cannot be delegated to the provider and recommends treating the cloud provider as a vendor (ised-isde.canada.ca) (ised-isde.canada.ca). A provider may supply secure facilities or technical features, but the business still decides what it collects, who may access it, what appears in mail scans, where a client conversation occurs and when data is deleted.

Finally, proportionality should be used to improve judgment, not excuse missing basics. A solo consultant may have a short policy and spreadsheet inventory; a twenty-person business handling financial or health-adjacent records may need deeper access logging, segregation, testing and specialist review. Both should be able to show who decided, what evidence was considered, which controls were approved and when the decision will be revisited.

Frequently Asked Questions (FAQs)

What are the Quebec Law 25 small business requirements?

At minimum, identify and publish the privacy officer, implement proportionate governance policies, inventory personal information, give compliant notices, obtain valid consent where required, control access and vendors, manage retention and destruction, answer rights requests, assess EFVP triggers and maintain an incident process and register. Small size changes proportionality, not the need for accountable controls.

What are the Law 25 privacy officer requirements?

The highest-authority person is the default officer. All or part of the function may be delegated to any person in writing, but accountability remains with the highest-authority person. Publish the officer's title and contact information and provide enough resources to perform the role.

Does every small business need an EFVP for SaaS?

Not because a product is labelled SaaS. The key question is whether the initiative is a project to acquire, develop or overhaul an information system or electronic service delivery system involving personal information. A separate EFVP trigger applies before communication outside Quebec. Document the trigger decision before rollout.

What are Quebec Law 25 consent requirements?

Consent must be manifest, free, informed, understandable and tied to specific purposes. Request it separately for each purpose, and present a written consent request distinctly from other information. Sensitive-information consent must be express. First ask whether the collection or proposed use is necessary and whether a statutory exception genuinely applies.

What is the Quebec data breach response requirement?

The statutory term is a confidentiality incident. Contain it, prevent recurrence, consult the privacy officer and assess sensitivity, anticipated consequences and likelihood of harmful use. Notify the CAI and affected people promptly if serious injury is possible. Record every incident and keep the register for at least five years.

Does Law 25 compliance change for virtual offices?

The governing duties remain with the business. A virtual office adds handling points such as authorized mail recipients, envelope images, scanned contents, pickup identity checks and retention of physical mail. Put relevant requirements into the service arrangement and the business's own procedures. Do not describe the address provider as the privacy officer unless a valid written delegation actually says so.

Is a privacy-policy template enough?

No. The published text must match actual purposes, data, technologies, recipients, locations, retention and individual rights. Compliance evidence also includes appointment records, inventories, approvals, EFVPs, contracts, access reviews, incident and request records, training and destruction proof.

Conclusion

The practical answer to **Law 25 compliance for microbusinesses** is a compact operating system, not a history lesson or a binder of generic templates. Ownership starts with the person exercising the highest authority, even when the privacy function is delegated. The minimum governance pack connects a live data inventory to retention, notices, consent, rights requests, vendor review, EFVP decisions, incident response and evidence.

Business events should drive the work. The first customer list activates purpose and notice questions. The first employee adds access and employment-record controls. A CRM, cloud or AI rollout requires an EFVP trigger decision before launch. Access outside Quebec calls for a cross-border assessment and written agreement. A confidentiality incident starts containment, factor-based assessment, notification analysis and a five-year register entry. A request starts a 30-day calendar.

For a 1-to-20-person Quebec business, proportionality means shorter records and clearer ownership, not absent controls. The strongest 90-day program is one that can demonstrate actual decisions: what was collected, why it was needed, who accessed it, where a vendor handled it, when an EFVP occurred, how a request was answered and when obsolete data was destroyed. That evidence makes the checklist useful during growth, procurement and operational change, which is where privacy risk actually moves.
