



2727 COWORKING / RECHERCHE ET CONSEILS PRATIQUES

Loi 25 : liste de vérification pour les microentreprises du Québec

Find a practical home for your work at 2727 Coworking in Montreal. Explore private offices, day workspaces and meeting rooms, plus business-address and virtual-mailbox services for your company.

Publié par 2727 Coworking · 2026-09-19 · [liste-verification-conformite-loi-25-quebec](#) · [loi-25-petite-entreprise](#) · [loi-quebecoise-protection-renseignements-personnels](#) · [responsable-protection-renseignements-personnels](#) · [efvp](#) · [evaluation-facteurs-relatifs-vie-privee](#) · [conformite-saas](#) · [intervention-atteinte-securite-donnees](#) · [protection-renseignements-personnels-bureau-virtuel](#)

Article original : <https://2727coworking.com/articles/fr/loi-25-verification-microentreprises-quebec>

Dans cet article

1. Sommaire
2. Introduction et contexte
3. Champ d'application, imputabilité et dossier minimal de gouvernance
4. Avis, consentement, conservation et demandes des personnes concernées
5. Liste de vérification des obligations selon les événements
6. EFVP, fournisseurs, infonuagique et transferts à l'extérieur du Québec
7. Intervention en cas d'incident et preuves
8. Analyse des données et éléments probants
9. Plan de mise en œuvre sur 30/60/90 jours
10. Incidences et perspectives
11. Foire aux questions (FAQ)
12. Conclusion

Sommaire

La loi québécoise sur la protection des renseignements personnels dans le secteur privé s'applique à une entreprise qui traite des renseignements personnels dans le cadre de ses activités, qu'elle les détienne elle-même ou par l'intermédiaire d'un tiers (legisquebec.gouv.qc.ca). La Commission d'accès à l'information (CAI) inclut expressément les entreprises individuelles et les travailleurs autonomes (cai.gouv.qc.ca). Il n'existe aucune exemption générale pour une entreprise de **1 à 20 personnes**. Le minimum pratique ne consiste donc pas à créer un grand service de conformité. Il consiste à désigner une personne responsable, à tenir à jour

une cartographie des données, à établir des règles écrites proportionnées à l'entreprise, à fournir des avis utilisables, à prévoir des procédures de traitement des demandes et des incidents, et à conserver des preuves du fonctionnement de ces mesures.

La personne qui exerce la plus haute autorité au sein de l'entreprise est, par défaut, responsable de la protection des renseignements personnels. Cette fonction peut être déléguée **par écrit**, mais la personne qui exerce la plus haute autorité demeure imputable (legisquebec.gouv.qc.ca) (cai.gouv.qc.ca). Le titre et les coordonnées du responsable doivent être rendus publics. Les politiques de gouvernance doivent porter sur la conservation et la destruction des renseignements, les rôles du personnel tout au long du cycle de vie des données et les plaintes, tout en demeurant proportionnées à la nature et à l'étendue des activités de l'entreprise (legisquebec.gouv.qc.ca).

Le point de décision le plus déterminant est l'adoption d'un nouveau **système de gestion de la relation client (CRM), logiciel en tant que service (SaaS), plateforme infonuagique ou outil d'intelligence artificielle (IA)**. Une évaluation des facteurs relatifs à la vie privée (EFVP), comme on l'appelle au Québec, est requise pour tout projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services qui implique des renseignements personnels (legisquebec.gouv.qc.ca). Une EFVP distincte est requise avant de communiquer des renseignements personnels à l'extérieur du Québec, et le transfert doit offrir une protection adéquate et être encadré par une entente écrite qui tient compte de l'évaluation (legisquebec.gouv.qc.ca). La démarche simplifiée consiste à décrire le projet et les données, à confirmer les éléments déclencheurs, à évaluer la nécessité et la proportionnalité, à cartographier les lieux et les destinataires, à déterminer les risques et les mesures de contrôle, à approuver les conditions, à signer le contrat, puis à réexaminer l'EFVP lorsque le projet change.

Si un incident de confidentialité survient, consignez **chaque** incident, évaluez la sensibilité des renseignements, les conséquences probables et la probabilité d'une utilisation préjudiciable, consultez le responsable de la protection des renseignements personnels, circonscrivez l'incident et avisez rapidement la CAI et les personnes concernées lorsqu'un préjudice sérieux est possible (cai.gouv.qc.ca). Conservez le registre pendant au moins **cinq ans** (cai.gouv.qc.ca). Les demandes d'accès et de rectification exigent généralement une réponse écrite dans un délai de **30 jours** (legisquebec.gouv.qc.ca). Un déploiement sur **90 jours** peut permettre de mettre ce système minimal en place, mais un modèle ne suffit pas à assurer la conformité. Le critère est de savoir si les dossiers correspondent aux collectes, aux systèmes, aux fournisseurs, aux décisions et aux suppressions réels.

Introduction et contexte

Ce rapport est une **liste de vérification de la conformité à la Loi 25 du Québec** destinée aux propriétaires et aux responsables des opérations d'entreprises de 1 à 20 personnes. « Loi 25 » est une appellation abrégée de la loi de réforme qui a modifié les lois québécoises sur la protection des renseignements personnels. Les règles courantes présentées ici se trouvent maintenant principalement dans la version à jour de la Loi sur la protection des renseignements personnels dans le secteur privé et dans ses règlements. Le calendrier de mise en œuvre de la CAI s'étendait du **22 septembre 2021 au 22 septembre 2024**, la plupart des dispositions étant entrées en vigueur le 22 septembre 2023 (cai.gouv.qc.ca). La portabilité a suivi le **22 septembre 2024** (cai.gouv.qc.ca).

La taille compte sur le plan opérationnel, mais ne constitue pas une exemption générale. L'article 1525 du Code civil définit l'exploitation d'une entreprise comme incluant une activité économique organisée exercée par une ou plusieurs personnes (legisquebec.gouv.qc.ca). Le premier tableur de clients potentiels d'un consultant indépendant, le premier dossier d'employé d'une entreprise en démarrage et le système de réservation en ligne d'un petit commerce peuvent donc entraîner de véritables obligations. La définition juridique vise les renseignements concernant une personne physique qui peut être identifiée directement ou indirectement.

Il s'agit d'un guide de recherche opérationnel, et non d'un avis juridique personnalisé. Il distingue les obligations légales des mesures de contrôle recommandées. Une agence de cinq personnes et une clinique de vingt personnes ne devraient pas utiliser les mêmes mesures de protection, puisque la sensibilité, la quantité, la finalité, la circulation et le stockage des renseignements diffèrent. La gouvernance doit être proportionnée aux activités de l'entreprise. L'objectif approprié est un petit système traçable qui évolue lorsque les événements de l'entreprise accroissent le risque. L'ISO indique que sa norme de gestion de la protection de la vie privée peut être utilisée par toute organisation qui traite des renseignements permettant d'identifier une personne (iso.org).

Champ d'application, imputabilité et dossier minimal de gouvernance

Déterminer si la loi sur le secteur privé s'applique

Commencez par les activités, et non par l'effectif. Dressez la liste de tous les endroits où l'entreprise traite des renseignements sur les clients, les employés, les contractuels, les candidats, les clients potentiels, les visiteurs du site Web et les contacts d'affaires. La Loi s'applique généralement lorsque des renseignements personnels sont traités dans le cadre de l'exploitation d'une entreprise. Certains renseignements professionnels liés à l'exercice des fonctions d'une personne font l'objet d'un traitement plus restreint, et les renseignements à caractère journalistique, historique ou généalogique utilisés à des fins légitimes d'information du public sont exclus (legisquebec.gouv.qc.ca). Les organismes publics et certains renseignements de santé et de services sociaux relèvent de régimes particuliers ; une entreprise réglementée devrait donc recenser les lois qui se chevauchent plutôt que de présumer que la Loi 25 est la seule règle applicable.

Les premières mesures d'imputabilité sont simples :

- **Désignez le responsable.** Inscrivez la personne qui exerce la plus haute autorité comme responsable de la protection des renseignements personnels, à moins qu'une délégation écrite ne prévoie autre chose.
- **Publiez les coordonnées.** Affichez le titre et les coordonnées du responsable sur le site Web, ou rendez-les accessibles par un autre moyen approprié s'il n'y a pas de site Web (legisquebec.gouv.qc.ca).
- **Financez la fonction.** La CAI indique que la personne délégataire devrait recevoir les ressources humaines, techniques et financières nécessaires (cai.gouv.qc.ca).

- **Approuvez la gouvernance.** Faites approuver les politiques et les pratiques écrites par le responsable, puis conservez une preuve datée de cette approbation.

Constituer six documents de travail

Une microentreprise n'a pas besoin de six longs manuels. Elle a besoin de six documents liés entre eux qui reflètent la réalité. La documentation québécoise de mise en œuvre destinée au secteur public présente aussi la taille, les activités, les ressources, la clientèle et les renseignements détenus comme des facteurs utiles pour adapter les mesures (quebec.ca) :

- **Inventaire des données.** Catégorie, type de personne, finalité, source, système, rôles d'accès, fournisseur, lieu, événement déclencheur de la période de conservation et méthode d'élimination. L'outil d'autoévaluation d'un organisme de réglementation pour le secteur privé demande également un inventaire des renseignements personnels recueillis (oipc.bc.ca).
- **Calendrier de conservation.** Durée minimale ou maximale, événement qui déclenche le délai, fondement juridique, responsable du système et preuve de destruction. Il n'existe pas de durée universelle qui convient à toutes les organisations (priv.gc.ca). Des procédures internes claires devraient fixer des durées minimales et maximales de conservation (priv.gc.ca).
- **Information publique sur la protection des renseignements personnels.** L'avis de collecte, la politique de confidentialité applicable aux moyens technologiques, les coordonnées du responsable de la protection des renseignements personnels, le résumé de la gouvernance et la marche à suivre pour déposer une plainte.
- **Procédure d'exercice des droits.** Vérification de l'identité, date de réception, lieux de recherche, examen des exceptions, approbation de la réponse, transmission et clôture.
- **Dossier des fournisseurs et des EFVP.** Questionnaire de vérification préalable, évaluation, mesures de protection approuvées, contrat, lieu où se trouvent les données, changements de sous-traitants et date de révision. Les lignes directrices canadiennes indiquent que les systèmes détenus, utilisés en vertu d'un contrat ou utilisés autrement devraient tous être visés par les contrôles de base (cyber.gc.ca).
- **Dossier des incidents.** Formulaire de triage, journal des décisions, modèles d'avis, registre des incidents et leçons tirées.

L'organisme fédéral de réglementation de la protection de la vie privée recommande de dresser l'inventaire des renseignements conservés, des raisons de leur conservation et de leur durée de conservation (priv.gc.ca). Le NIST recommande également de cartographier les données, de la collecte à l'élimination, et d'adopter des politiques officielles d'élimination (nist.gov) (nist.gov). Il s'agit de méthodes de mise en œuvre, et non de substituts à la loi québécoise.

Avis, consentement, conservation et demandes des personnes concernées

Rédiger l'avis à partir de la cartographie des données

Avant de recueillir des renseignements, confirmez un intérêt sérieux et légitime et déterminez les finalités. Ne recueillez que les renseignements nécessaires à ces finalités, par des moyens licites (legisquebec.gouv.qc.ca). Au moment de la collecte, expliquez les finalités et les moyens, les droits d'accès et de rectification, le retrait du consentement et, s'il y a lieu, la possibilité d'une communication à l'extérieur du Québec. Sur demande, les renseignements supplémentaires comprennent les catégories de personnes qui y ont accès à l'interne, la durée de conservation et les coordonnées du responsable de la protection des renseignements personnels.

Une entreprise qui recueille des renseignements par un moyen technologique doit publier ou diffuser autrement une politique de confidentialité rédigée en termes simples et clairs (legisquebec.gouv.qc.ca). Selon la CAI, cette politique devrait préciser les tiers concernés et les contextes de communication, les mesures de protection, les témoins de connexion s'il y a lieu, les droits, les recours et les modifications de la politique (cai.gouv.qc.ca). L'outil d'autoévaluation d'un organisme de réglementation considère aussi les durées de conservation comme un élément d'une politique écrite (oipc.bc.ca). Les personnes doivent être avisées lorsque cette politique est modifiée (cai.gouv.qc.ca).

Traiter le consentement comme une décision, et non comme une case à cocher

Un consentement valide doit être manifeste, libre, éclairé et lié à des finalités spécifiques. Il doit être demandé pour chacune des finalités en termes simples et clairs, et une demande écrite doit être présentée distinctement des autres renseignements (legisquebec.gouv.qc.ca). Un consentement exprès est requis pour l'utilisation ou la communication de renseignements personnels sensibles (legisquebec.gouv.qc.ca). La CAI recommande d'interpréter les exceptions au consentement de façon restrictive (cai.gouv.qc.ca).

Pour les listes de clients potentiels, ne considérez pas une interaction antérieure comme une autorisation illimitée. La prospection commerciale n'est pas une finalité secondaire compatible au sens de la loi sur le secteur privé (legisquebec.gouv.qc.ca). Les règles fédérales antipourriel peuvent aussi s'appliquer. Les lignes directrices fédérales indiquent qu'une demande de renseignements peut justifier un consentement tacite pendant seulement **six mois**, et que les demandes de désabonnement doivent être exécutées dans un délai de **10 jours ouvrables** (ised-isde.canada.ca) (ised-isde.canada.ca).

Gérer les demandes selon un calendrier

Utilisez une seule adresse de réception et consignez immédiatement la date d'échéance. Une demande d'accès ou de rectification doit être faite par écrit par une personne qui justifie son identité. Le responsable de la protection des renseignements personnels doit répondre par écrit au plus tard **30 jours** après la réception ; l'absence de réponse est considérée comme un refus (legisquebec.gouv.qc.ca). L'accès est gratuit, sous réserve de frais raisonnables de reproduction ou de transmission, et un refus doit être motivé et citer son fondement légal.

La portabilité vise les renseignements informatisés admissibles dans un format technologique structuré et couramment utilisé, sous réserve de difficultés pratiques sérieuses. Les renseignements créés ou inférés par l'entreprise et les renseignements obtenus auprès de tiers sont exclus (cai.gouv.qc.ca). La rectification s'applique aux renseignements inexacts, incomplets ou équivoques. La désindexation ou la cessation de la diffusion n'existe que dans des conditions précises ; il ne faut donc pas la présenter comme un droit inconditionnel à la suppression.

Une fois les finalités accomplies, détruisez les renseignements ou anonymisez-les pour les utiliser à des fins sérieuses et légitimes, sous réserve des lois applicables en matière de conservation (legisquebec.gouv.qc.ca). Un renseignement dépersonnalisé demeure un renseignement personnel, et la dépersonnalisation n'équivaut pas à la destruction (cai.gouv.qc.ca).

Liste de vérification des obligations selon les événements

Le *tableau 1* associe les événements courants d'une microentreprise à un responsable, à des preuves minimales et à un cycle de révision. L'« examen des éléments déclencheurs » signifie que le responsable de la protection des renseignements personnels détermine quelle obligation s'applique, plutôt que de présumer que chaque événement exige les mêmes documents.

Événement d'affaires	Obligation et mesure de contrôle immédiates	Responsable	Preuves et révision
Première liste de clients ou de clients potentiels	Confirmer un intérêt sérieux et légitime, définir chaque finalité, la nécessité et le fondement du consentement avant la collecte. Fournir l'avis au moment de la collecte.	Responsable de la protection des renseignements personnels et responsable des ventes	Entrée d'inventaire, version de l'avis, preuve de consentement ; réviser lorsque les champs ou les finalités changent.
Premier employé ou candidat	Inventorier les dossiers de recrutement, de paie, d'avantages sociaux et de rendement. Limiter l'accès aux personnes qui ont besoin des renseignements pour exercer leurs fonctions (cai.gouv.qc.ca).	Responsable de la protection des renseignements personnels et employeur	Matrice d'accès et calendrier de conservation ; réviser à l'embauche, lors d'un changement de rôle et au départ.
Nouvel outil CRM, SaaS, infonuagique ou d'IA	Suspendre l'acquisition pour déterminer si une EFVP est requise. Cartographier les entrées, les sorties, l'accès du fournisseur, l'utilisation des modèles, les lieux, la conservation, la suppression et la portabilité. L'examen du fournisseur devrait porter sur l'avis d'accès non autorisé, la destruction à la fin du contrat et l'emplacement du centre de données (cyber.gc.ca).	Responsable du projet et responsable de la protection des renseignements personnels	Note sur les éléments déclencheurs, EFVP, conditions d'approbation, contrat ; réexaminer lors d'un changement important.
Données transmises ou accessibles à l'extérieur du Québec	Réaliser l'EFVP relative au transfert transfrontalier avant la communication. Confirmer une protection adéquate et conclure une entente écrite.	Responsable de la protection des renseignements personnels et responsable du contrat	Cartographie des pays et des sous-traitants, évaluation du contexte juridique, mesures de protection, entente signée.

Événement d'affaires	Obligation et mesure de contrôle immédiates	Responsable	Preuves et révision
Nouveau formulaire Web, outil d'analyse ou témoins de connexion	Mettre à jour l'avis de collecte et la politique de confidentialité. Régler les paramètres de confidentialité au niveau le plus élevé par défaut lorsque la règle légale s'applique, en tenant compte de l'exception concernant les témoins de connexion du navigateur.	Responsable du produit ou du site Web	Captures d'écran, exportation des paramètres, version de la politique et avis de modification.
Bureau virtuel, boîte postale ou espace de travail partagé	Considérer la numérisation du courrier, les interactions avec les visiteurs, les bureaux partagés et les conversations en salle de réunion comme des points de traitement des renseignements. Définir les destinataires autorisés, les conversations privées, le verrouillage des écrans, le transport des documents papier et le rangement sécurisé.	Responsable de la protection des renseignements personnels et utilisateur de l'espace de travail	Liste de vérification de l'espace de travail et liste des noms autorisés ; réviser lors d'un changement de forfait, de personnel ou de traitement du courrier.
Incident de confidentialité	Circonscrire l'incident, préserver les faits, évaluer le préjudice sérieux, consigner chaque incident, aviser lorsque le seuil est atteint et suivre les mesures correctives.	Responsable de l'intervention et responsable de la protection des renseignements personnels	Registre des incidents, évaluation, avis, dossier des mesures correctives.
Demande d'accès, de rectification, de portabilité ou de désindexation admissible	Vérifier l'identité, déclencher le délai de 30 jours , effectuer des recherches dans les systèmes cartographiés, documenter les exceptions, approuver et transmettre de façon sécurisée.	Responsable de la protection des renseignements personnels	Réception, journal de recherche, décision, réponse et date de clôture.
Finalité accomplie ou compte fermé	Vérifier les obligations de conservation à des fins juridiques et les durées propres à chaque catégorie, puis détruire ou anonymiser correctement. Obtenir une preuve de suppression du fournisseur.	Responsable du système et responsable de la protection des renseignements personnels	Rapport de suppression, certificat ou décision d'anonymisation ; vérifier un échantillon chaque trimestre.

La matrice fait reposer le système de conformité d'une microentreprise sur les événements. Un même événement peut activer plusieurs lignes. L'ajout d'un CRM infonuagique, par exemple, peut modifier l'avis, la conception du consentement, le contrat du fournisseur, l'analyse concernant l'extérieur du Québec, la méthode de conservation et la procédure de recherche pour les demandes. Un bureau virtuel ne transfère pas l'imputabilité au fournisseur de l'espace de travail. Il ajoute des points de traitement physiques et des points de traitement par le fournisseur que l'entreprise doit contrôler. Les contrats devraient définir les exigences de sécurité et le traitement des données (priv.gc.ca).

EFVP, fournisseurs, infonuagique et transferts à l'extérieur du Québec

Reconnaître les trois éléments déclencheurs d'une EFVP

Les trois éléments déclencheurs opérationnels les plus pertinents ici sont les suivants :

- **Systèmes d'information et services électroniques.** L'acquisition, le développement ou la refonte qui implique la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels exige une EFVP. Un outil prêt à l'emploi n'est pas automatiquement exclu de cette obligation. La CAI indique qu'une EFVP est requise pour tout projet de système visé (cai.gouv.qc.ca).
- **Communication à l'extérieur du Québec.** Réalisez une EFVP avant la communication, y compris lorsqu'une personne ou un organisme à l'extérieur du Québec recueillera, utilisera, communiquera ou conservera des renseignements pour l'entreprise (legisquebec.gouv.qc.ca).
- **Communication à des fins de recherche sans consentement.** Une procédure distincte s'applique avant une communication sans consentement à des fins d'étude, de recherche ou de production de statistiques (cai.gouv.qc.ca).

Suivre une démarche simplifiée en six étapes

Le *tableau 2* présente une démarche d'EFVP justifiable pour une petite organisation. Sa profondeur est adaptée aux données et au projet, et non à un nombre fixe de pages.

Étape	Questions de décision	Preuves minimales
1. Décrire	Quels sont le résultat d'affaires, le changement de système et le cycle de vie des renseignements proposés ?	Description du projet sur une page, schéma de circulation des données et responsable du système.
2. Déterminer les éléments déclencheurs	S'agit-il d'une acquisition, d'un développement ou d'une refonte ? Les renseignements seront-ils communiqués ou traités à l'extérieur du Québec ? Une communication à des fins de recherche est-elle prévue ?	Décision datée sur les éléments déclencheurs, y compris les motifs si aucune EFVP n'est entreprise.
3. Nécessité et proportionnalité	Chaque champ est-il nécessaire ? La finalité, la sensibilité, la quantité, la circulation et le support de stockage sont-ils proportionnés ?	Examen de la nécessité de chaque champ et cote de risque.
4. Fournisseur et géographie	Qui peut accéder aux données, où, par l'intermédiaire de quels sous-traitants, pendant combien de temps et selon quel cadre juridique ?	Réponses du fournisseur, carte des lieux, liste des sous-traitants et lacunes contractuelles.
5. Mesures de contrôle et risque résiduel	Peut-on réduire la collecte ? L'accès, le chiffrement, la journalisation, l'exportation, la suppression, les avis d'incident et la continuité sont-ils adéquats ?	Responsable des mesures d'atténuation, échéance, vérification et décision sur le risque résiduel.
6. Approuver et réexaminer	Le responsable de la protection des renseignements personnels a-t-il participé dès le début ? Quelles conditions s'appliquent ? Quel changement exige une réévaluation ?	Décision signée, contrat, liste de vérification du lancement et élément déclencheur d'une révision.

Les facteurs légaux de proportionnalité comprennent la sensibilité, les finalités, la quantité, la répartition et le support des renseignements. Le responsable de la protection des renseignements personnels doit être consulté dès le début et peut recommander des mesures de contrôle du projet, l'attribution de responsabilités, des mesures de protection concernant la documentation et de la formation (legisquebec.gouv.qc.ca). La CAI

recommande de réexaminer l'EFVP lorsque le projet change, notamment en cas de modification d'une entente ou de refonte d'un système (cai.gouv.qc.ca). Les lignes directrices officielles britanniques recommandent également une vérification diligente de la sécurité du SaaS avant le déploiement (ncsc.gov.uk).

Intégrer les mesures de protection au contrat et à la configuration

Un mandat de service qui implique une communication nécessaire de renseignements doit être écrit. Le contrat devrait limiter l'utilisation à l'exécution du mandat, empêcher la conservation après son expiration, exiger un avis rapide de toute violation ou tentative de violation de la confidentialité et permettre au responsable de la protection des renseignements personnels de vérifier la conformité (legisquebec.gouv.qc.ca). Pour le traitement transfrontalier, consignez aussi dans l'entente écrite le droit applicable à destination, les mesures de protection contractuelles, la protection adéquate et toute mesure d'atténuation des risques.

La vérification diligente pratique devrait mettre le service à l'épreuve, et non simplement recueillir un lien vers une politique :

- **Identité et accès.** Exigez des comptes individuels, le principe du moindre privilège, l'authentification multifacteur pour les administrateurs et le retrait des accès en temps opportun lors des départs. Le Centre canadien pour la cybersécurité recommande l'authentification à deux facteurs pour les comptes d'administration infonuagique (cyber.gc.ca).
- **Administration centralisée.** Gérez le SaaS de façon centralisée et attribuez le bon niveau d'accès à chaque utilisateur (ncsc.gov.uk). Appliquez le principe du moindre privilège selon les rôles (ico.org.uk).
- **Emplacement des données.** Consignez les lieux de stockage principal, de sauvegarde, de soutien et de reprise après sinistre. Les lignes directrices canadiennes recommandent d'évaluer les territoires de compétence juridique où les fournisseurs externes stockent ou utilisent les renseignements sensibles (cyber.gc.ca).
- **Gestion des incidents.** Définissez les voies de notification, les délais, les faits minimaux à communiquer, la préservation des preuves et les obligations de collaboration. Traitez le fournisseur infonuagique comme un fournisseur dans la gestion de la chaîne d'approvisionnement (ised-isde.canada.ca).
- **Sortie et suppression.** Confirmez le format d'exportation, la restitution, les délais d'élimination des sauvegardes et les preuves de suppression. L'organisme fédéral de réglementation recommande l'élimination sécurisée des renseignements qui ne servent plus les besoins de l'entreprise (priv.gc.ca).
- **Sécurité opérationnelle.** Activez les correctifs automatiques lorsque cela convient, les sauvegardes chiffrées et les essais de restauration (cyber.gc.ca) (tsapps.nist.gov).

Pour un utilisateur d'un espace de coworking ou d'un bureau virtuel, ajoutez le rangement des documents papier sous clé, les conversations privées, le verrouillage des écrans et la remise contrôlée du courrier. L'accès physique aux lieux de stockage des renseignements personnels devrait être restreint (priv.gc.ca). Les lignes directrices officielles recommandent des espaces privés pour les conversations sensibles, une règle de bureau dégagé et le verrouillage de l'ordinateur lorsque l'on quitte son poste de travail (gov.uk) (gov.uk)

(gov.uk). Les lignes directrices sur le télétravail recommandent de n'emporter que les dossiers nécessaires pour une période limitée, de transporter les documents papier dans un sac verrouillé et de chiffrer les appareils portables (oipc.ab.ca) (oipc.ab.ca) (oipc.ab.ca). Les dossiers papier devraient demeurer dans des armoires verrouillées lorsqu'ils ne sont pas utilisés, et le courrier sensible peut être envoyé avec suivi lorsque cela convient (ico.org.uk) (ico.org.uk).

Intervention en cas d'incident et preuves

Un incident de confidentialité comprend l'accès, l'utilisation ou la communication non autorisés, la perte ou toute autre atteinte à la protection des renseignements. Lorsqu'il existe des motifs raisonnables de croire qu'un incident s'est produit, l'entreprise doit prendre des mesures raisonnables pour réduire le préjudice et prévenir une récurrence. L'évaluation du préjudice sérieux tient compte de la **sensibilité**, des **conséquences appréhendées** et de la **probabilité d'une utilisation préjudiciable**, en consultant le responsable de la protection des renseignements personnels (legisquebec.gouv.qc.ca). Si un préjudice sérieux est possible, avisez rapidement la CAI et les personnes concernées.

Le *tableau 3* est une grille d'évaluation de la gravité. Il structure les facteurs légaux sans inventer de seuil numérique de notification.

Facteur	Questions à consigner	Preuves
Sensibilité	Les renseignements concernent-ils les finances, les justificatifs d'identité, la santé, l'emploi, la localisation précise ou un autre contexte sensible ? Étaient-ils chiffrés ou autrement illisibles ?	Catégories de données, classification, exemples de dossiers et état des clés.
Conséquences appréhendées	L'utilisation pourrait-elle affecter les finances, l'identité, la dignité, l'emploi, la sécurité, la réputation ou l'accès aux services ? Quelles mesures de protection sont disponibles ?	Analyse des scénarios et options d'atténuation.
Probabilité d'une utilisation préjudiciable	Qui les a reçus ou pouvait y accéder ? L'accès a-t-il été confirmé ? Les renseignements peuvent-ils être récupérés, leur accès révoqué ou leur contenu effacé à distance ?	Journaux, confirmation du destinataire, état de l'appareil et résultats des mesures de confinement.
Décision globale	La combinaison de ces facteurs présente-t-elle un risque de préjudice sérieux ? Quels faits appuient la décision ?	Consultation du responsable, justification datée et approbation.

N'utilisez pas un pointage comme substitut automatique au jugement. Le registre doit comprendre tous les incidents, même ceux qui ne présentent pas de risque de préjudice sérieux. Les renseignements à consigner comprennent les circonstances et les dates, la date de découverte, le nombre estimatif de personnes concernées, les motifs de l'évaluation du préjudice sérieux, les dates des avis et les mesures correctives. Conservez et mettez à jour le registre pendant au moins **cinq ans** après avoir pris connaissance de l'incident.

La séquence d'intervention est la suivante :

- **Circonscrire.** Désactivez les accès, récupérez les dossiers, préservez les journaux et prévenez une récurrence.

- **Trier.** Identifiez les systèmes, les renseignements, les personnes, la période, les destinataires et les tiers.
- **Évaluer.** Appliquez les trois facteurs légaux et consultez le responsable de la protection des renseignements personnels.
- **Aviser.** Si le seuil de préjudice sérieux est atteint, avisez rapidement la CAI et les personnes concernées. Seules trois circonstances précises permettent un avis public plutôt qu'un avis direct (cai.gouv.qc.ca).
- **Consigner.** Inscrivez l'incident, quelle que soit la décision de notification, puis mettez le dossier à jour à mesure que les faits évoluent.
- **Améliorer.** Attribuez les mesures correctives, vérifiez leur réalisation et intégrez les changements à la formation, aux contrats et aux EFVP.

Un dossier de preuves concis devrait contenir la nomination ou la délégation, une capture d'écran des coordonnées publiques, le dossier de gouvernance approuvé, l'inventaire daté, les avis, les preuves de consentement, le registre des demandes, le registre des incidents, les EFVP, les contrats des fournisseurs, les présences aux formations, les révisions des accès et les preuves de suppression. Le cadre canadien de base organise la sécurité en **13 catégories de contrôles** (cyber.gc.ca). Le programme CyberSécuritaire Canada demande aussi aux candidats d'examiner et de mettre en œuvre **13 contrôles**, et sa marque de certification est valide pendant **deux ans** (ised-isde.canada.ca) (ised-isde.canada.ca). La norme ISO/IEC 27701:2025 décrit un système de management de la protection de la vie privée comme un système établi, mis en œuvre, tenu à jour et amélioré en continu (iso.org). Une microentreprise peut appliquer ce cycle sans chercher à obtenir une certification.

Analyse des données et éléments probants

Les petites entreprises ne sont pas un cas marginal. Le Québec comptait **228 622 petites entreprises employeuses de 1 à 99 employés** en décembre 2024 (ised-isde.canada.ca). Les microentreprises de 1 à 4 employés représentaient **59,1 %** des entreprises canadiennes, tandis que plus des trois quarts comptaient de 1 à 9 employés (ised-isde.canada.ca) (ised-isde.canada.ca). À l'échelle nationale, les entreprises de **1 à 19 employés représentaient 91,2 %** des entreprises employeuses et employaient **4,5 millions de personnes**, soit **24,4 %** de l'emploi, en 2024 (www150.statcan.gc.ca) (www150.statcan.gc.ca). La liste de vérification s'adresse donc au segment dominant selon la taille des employeurs, et non à un créneau.

L'adoption des technologies rend la décision de réaliser une EFVP importante sur le plan opérationnel. Au deuxième trimestre de 2026, **19,9 %** des entreprises canadiennes de 1 à 4 employés ont déclaré avoir utilisé l'IA pour produire des biens ou fournir des services au cours de l'année précédente (www150.statcan.gc.ca). Parmi ces microentreprises utilisant l'IA, **24,0 %** ont formé le personnel en place et **10,7 %** ont fait appel à des consultants ou à des fournisseurs externes (www150.statcan.gc.ca) (www150.statcan.gc.ca). Les données de l'OCDE indiquaient que **41 %** des petites entreprises avaient acquis des services infonuagiques en 2021 (oecd.org). Les différences de populations et de périodes empêchent une comparaison directe, mais les deux ensembles de données montrent que les changements de fournisseurs et de systèmes sont courants.

Les données sur la préparation révèlent une lacune documentaire. En 2023, **26 %** des entreprises canadiennes avaient des politiques écrites de cybersécurité. L'enquête de Statistique Canada reposait sur un échantillon final de **12 462 entreprises** et un **taux de réponse de 71 %**, ce qui donne à l'estimation un contexte national utile (www150.statcan.gc.ca) (www150.statcan.gc.ca). Dans un sondage distinct de BDC auprès de **484 répondants** en septembre 2024 (bdc.ca), **37 %** ont déclaré avoir un plan informel en cas de cyberincident, **52 %** ont déclaré n'avoir aucun plan et **76 %** effectuaient des sauvegardes régulières (bdc.ca) (bdc.ca). Ces études mesurent la cybersécurité, et non la conformité à la Loi 25, et ne devraient pas être considérées comme des estimations des taux d'atteinte à la sécurité ou de conformité. Elles appuient une conclusion plus limitée : on ne peut pas présumer que les petites entreprises disposent de procédures opérationnelles écrites et mises à l'essai.

Le cadre d'application de la loi a des conséquences importantes, mais ne devrait pas être transformé en affirmation sur la probabilité d'une sanction. Une sanction administrative pécuniaire imposée à une entreprise peut atteindre le plus élevé des montants suivants : **10 millions de \$ ou 2 % du chiffre d'affaires mondial** de l'exercice financier précédent (cai.gouv.qc.ca). Pour une entreprise, la fourchette des amendes pénales commence à **15 000 \$** et peut atteindre le plus élevé des montants suivants : **25 millions de \$ ou 4 % du chiffre d'affaires mondial** (cai.gouv.qc.ca). Les sanctions administratives s'appliquent à des manquements précis, et non automatiquement à chaque document imparfait. Aucune donnée disponible ne permet d'établir une probabilité de sanction propre aux microentreprises, et il ne faut pas en inventer une.

Plan de mise en œuvre sur 30/60/90 jours

La séquence ci-dessous donne la priorité à la visibilité, aux événements fréquents et aux preuves de fonctionnement.

Jours 1 à 30 : établir le contrôle

- **Nommer.** Confirmez la personne qui exerce la plus haute autorité ou signez une délégation écrite. Publiez le titre et les coordonnées du responsable.
- **Inventorier.** Interrogez chaque responsable de processus et cartographiez les données relatives aux clients, aux clients potentiels, aux employés, aux candidats, au site Web, au courrier, au contrôle des accès et aux fournisseurs.
- **Suspendre les acquisitions à l'aveugle.** Exigez une vérification des éléments déclencheurs en matière de protection des renseignements personnels avant d'activer un nouveau CRM, service infonuagique, outil d'IA ou service électronique.
- **Ouvrir les registres.** Créez des registres des demandes, des incidents, des fournisseurs et des EFVP, même s'ils sont vides au départ.
- **Réduire les risques d'exposition évidents.** Éliminez les comptes partagés, activez l'authentification multifacteur, restreignez les permissions des fichiers, mettez les documents papier sous clé et chiffrez les appareils portables.

- **Établir la direction.** Confiez la responsabilité de la sécurité informatique à une personne qui occupe un rôle de direction et reliez ce rôle au responsable de la protection des renseignements personnels (cyber.gc.ca).

Jours 31 à 60 : harmoniser les engagements publics et les opérations

- **Fixer la conservation.** Attribuez un événement déclencheur et une durée à chaque catégorie de l'inventaire. Consignez les exigences légales externes et définissez les preuves de destruction.
- **Réécrire les avis.** Faites correspondre chaque formulaire, scénario d'appel, processus de collecte à la conclusion d'un contrat et processus concernant les employés aux finalités et aux communications réelles.
- **Publier l'information sur la gouvernance.** Fournissez la politique en langage clair et la marche à suivre pour déposer une plainte, puis consignez la version et la date d'approbation.
- **Traiter les fournisseurs en attente.** Évaluez les fournisseurs actifs selon la sensibilité, la quantité, l'emplacement et l'accès. Commencez par la paie, le CRM, le courriel, le stockage infonuagique, l'analyse de données, l'IA et le traitement des renseignements au bureau virtuel.
- **Former selon les rôles.** Présentez de courts scénarios aux équipes de vente et des opérations, aux gestionnaires et aux administrateurs. L'outil d'autoévaluation d'un organisme de réglementation structure les directives au personnel autour des attentes concernant la collecte, l'utilisation et la communication (oipbc.bc.ca).

Jours 61 à 90 : mettre à l'essai et documenter les preuves

- **Simuler le traitement d'une demande.** Récupérez les données d'une personne choisie comme exemple dans le courriel, le CRM, le stockage de fichiers et auprès des fournisseurs ; mettez à l'essai l'exportation et la transmission sécurisée dans le délai de **30 jours**.
- **Mettre les sauvegardes à l'essai.** Vérifiez que les données de sauvegarde sont chiffrées, que l'accès est restreint et qu'une restauration fonctionne réellement (cyber.gc.ca).
- **Mettre la restauration à l'essai.** Le NIST recommande séparément des sauvegardes régulières et des essais de ces sauvegardes (tsapps.nist.gov).
- **Simuler un incident.** Mettez à l'essai la réception, le confinement, l'évaluation des facteurs, les listes de contacts, la préparation de l'avis à la CAI et la tenue du registre. Les lignes directrices canadiennes recommandent un plan écrit qui précise les personnes responsables (cyber.gc.ca).
- **Terminer les EFVP prioritaires.** Réglez les questions de mesures de protection et de modifications contractuelles avant les lancements à risque élevé ou les communications transfrontalières.
- **Supprimer un ensemble réel de données.** Appliquez le calendrier de conservation à une catégorie admissible et conservez les preuves de suppression.
- **Faire rapport au propriétaire.** Consignez les risques non résolus, les exceptions, les mesures en retard et la prochaine révision trimestrielle.

Au jour 90, le résultat devrait être un cycle de contrôle fonctionnel. Les révisions trimestrielles peuvent porter sur un échantillon de nouveaux systèmes, de listes d'accès, d'incidents, de demandes, de changements de fournisseurs et de suppressions. La révision annuelle devrait réapprouver la gouvernance, actualiser la formation et faire concorder la politique publique avec l'inventaire. Pour les appareils mobiles, le navigateur des CIS Controls précise un délai de verrouillage automatique ne dépassant pas **deux minutes** ([cisecurity.org](https://www.cisecurity.org)). Il s'agit d'un repère recommandé, et non d'un délai légal québécois.

Incidences et perspectives

La principale incidence pour la gestion est que le travail de protection des renseignements personnels devrait être rattaché à la gestion du changement. Les acquisitions, l'embauche, le marketing, les lancements de produits, les changements d'espace de travail et les départs constituent de meilleurs points de contrôle qu'une réécriture annuelle de la politique. Cela réduit le risque qu'un système soit lancé avant que son EFVP, son contrat, son avis et sa méthode de suppression soient compris.

L'adoption de l'IA rend la nécessité de chaque champ et la transparence des fournisseurs plus importantes. Une microentreprise devrait consigner si les requêtes contiennent des renseignements sur les clients ou les employés, si le fournisseur utilise les entrées pour améliorer les modèles, où le traitement a lieu, comment les administrateurs accèdent au contenu, quelles possibilités d'exportation sont offertes et comment la suppression s'applique aux sauvegardes. L'EFVP devrait distinguer une expérimentation interne de productivité d'un service électronique offert aux clients, mais ni l'une ni l'autre ne devrait contourner la décision sur les éléments déclencheurs. Le NIST décrit l'authentification multifacteur comme l'une des protections les plus rapides et les moins coûteuses disponibles (tsapps.nist.gov).

Les modèles infonuagiques et d'espaces de travail partagés renforcent aussi la responsabilité partagée. Les lignes directrices canadiennes sur l'infonuagique indiquent que l'imputabilité du client ne peut pas être déléguée au fournisseur et recommandent de traiter le fournisseur infonuagique comme un fournisseur (ised-isde.canada.ca) (ised-isde.canada.ca). Un fournisseur peut offrir des installations sécurisées ou des fonctions techniques, mais l'entreprise décide toujours de ce qu'elle recueille, des personnes qui peuvent y accéder, de ce qui apparaît dans les numérisations du courrier, du lieu où se tient une conversation avec un client et du moment où les données sont supprimées.

Enfin, la proportionnalité devrait servir à améliorer le jugement, et non à justifier l'absence des éléments de base. Un consultant indépendant peut avoir une courte politique et un inventaire dans un tableur ; une entreprise de vingt personnes qui traite des dossiers financiers ou des dossiers liés à la santé peut avoir besoin d'une journalisation des accès plus poussée, d'une séparation des données, d'essais et d'un examen spécialisé. Les deux devraient pouvoir montrer qui a décidé, quelles preuves ont été prises en compte, quelles mesures de contrôle ont été approuvées et quand la décision sera réexaminée.

Foire aux questions (FAQ)

Quelles sont les exigences de la Loi 25 du Québec pour les petites entreprises ?

Au minimum, identifiez le responsable de la protection des renseignements personnels et publiez ses coordonnées, mettez en œuvre des politiques de gouvernance proportionnées, dressez l'inventaire des renseignements personnels, fournissez des avis conformes, obtenez un consentement valide lorsqu'il est requis, contrôlez l'accès et les fournisseurs, gérez la conservation et la destruction, répondez aux demandes d'exercice des droits, évaluez les éléments déclencheurs d'une EFVP et maintenez une procédure et un registre des incidents. La petite taille modifie la proportionnalité, et non la nécessité de mesures de contrôle assorties d'une responsabilité claire.

Quelles sont les exigences de la Loi 25 concernant le responsable de la protection des renseignements personnels ?

La personne qui exerce la plus haute autorité est le responsable par défaut. La totalité ou une partie de la fonction peut être déléguée par écrit à toute personne, mais l'imputabilité demeure celle de la personne qui exerce la plus haute autorité. Publiez le titre et les coordonnées du responsable et fournissez des ressources suffisantes pour exercer cette fonction.

Chaque petite entreprise a-t-elle besoin d'une EFVP pour un SaaS ?

Pas simplement parce qu'un produit porte l'étiquette SaaS. La question clé est de savoir si l'initiative constitue un projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services qui implique des renseignements personnels. Un élément déclencheur distinct d'EFVP s'applique avant une communication à l'extérieur du Québec. Documentez la décision sur les éléments déclencheurs avant le déploiement.

Quelles sont les exigences de consentement de la Loi 25 du Québec ?

Le consentement doit être manifeste, libre, éclairé, compréhensible et lié à des finalités spécifiques. Demandez-le séparément pour chaque finalité et présentez une demande écrite de consentement distinctement des autres renseignements. Le consentement relatif aux renseignements sensibles doit être exprès. Demandez-vous d'abord si la collecte ou l'utilisation proposée est nécessaire et si une exception légale s'applique réellement.

Quelle est l'exigence d'intervention en cas d'atteinte à la sécurité des données au Québec ?

Le terme légal est « incident de confidentialité ». Circonscrivez l'incident, prévenez une récurrence, consultez le responsable de la protection des renseignements personnels et évaluez la sensibilité, les conséquences appréhendées et la probabilité d'une utilisation préjudiciable. Avisez rapidement la CAI et les personnes concernées si un préjudice sérieux est possible. Consignez chaque incident et conservez le registre pendant au moins cinq ans.

La conformité à la Loi 25 change-t-elle pour les bureaux virtuels ?

Les obligations applicables demeurent celles de l'entreprise. Un bureau virtuel ajoute des points de traitement, comme les destinataires autorisés du courrier, les images des enveloppes, les contenus numérisés, les vérifications d'identité à la cueillette et la conservation du courrier physique. Intégrez les exigences pertinentes à l'entente de service et aux procédures de l'entreprise. Ne présentez pas le fournisseur d'adresse comme le responsable de la protection des renseignements personnels, à moins qu'une délégation écrite valide ne le prévoie réellement.

Un modèle de politique de confidentialité suffit-il ?

Non. Le texte publié doit correspondre aux finalités, aux données, aux technologies, aux destinataires, aux lieux, à la conservation et aux droits des personnes réels. Les preuves de conformité comprennent aussi les documents de nomination, les inventaires, les approbations, les EFVP, les contrats, les révisions des accès, les dossiers d'incidents et de demandes, la formation et les preuves de destruction.

Conclusion

La réponse pratique à la **conformité à la Loi 25 pour les microentreprises** est un système opérationnel simple, et non une leçon d'histoire ou un classeur de modèles génériques. La responsabilité commence par la personne qui exerce la plus haute autorité, même lorsque la fonction de protection des renseignements personnels est déléguée. Le dossier minimal de gouvernance relie un inventaire de données à jour à la conservation, aux avis, au consentement, aux demandes d'exercice des droits, à l'examen des fournisseurs, aux décisions d'EFVP, à l'intervention en cas d'incident et aux preuves.

Les événements d'affaires devraient orienter le travail. La première liste de clients déclenche les questions de finalité et d'avis. Le premier employé ajoute des mesures de contrôle de l'accès et des dossiers d'emploi. Le déploiement d'un CRM, d'un service infonuagique ou d'un outil d'IA exige une décision sur les éléments déclencheurs d'une EFVP avant le lancement. L'accès à l'extérieur du Québec nécessite une évaluation transfrontalière et une entente écrite. Un incident de confidentialité déclenche le confinement, l'évaluation fondée sur les facteurs, l'analyse de notification et une inscription au registre à conserver pendant cinq ans. Une demande déclenche un délai de 30 jours.

Pour une entreprise québécoise de 1 à 20 personnes, la proportionnalité signifie des documents plus courts et des responsabilités plus claires, et non l'absence de mesures de contrôle. Le programme de 90 jours le plus solide est celui qui peut démontrer les décisions réelles : ce qui a été recueilli, pourquoi c'était nécessaire, qui y a accédé, où un fournisseur a traité les renseignements, quand une EFVP a été réalisée, comment une demande a été traitée et quand les données périmées ont été détruites. Ces preuves rendent la liste de vérification utile pendant la croissance, les acquisitions et les changements opérationnels, qui sont les moments où le risque pour la vie privée évolue réellement.

Liens vers les sources

Liens cités dans cet article, dans leur ordre de première apparition. Les adresses complètes sont fournies pour les lecteurs qui utilisent le texte extrait.

1. <https://www.legisquebec.gouv.qc.ca/en/pdf/cs/P-39.1.pdf>
2. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/champ-application-loi_entreprises
3. https://www.legisquebec.gouv.qc.ca/fr/version/lc/P-39.1?code=se%3A3_1&history=20240306&langCont=en
4. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/responsable-protection-renseignements-personnels-entreprise>
5. https://www.legisquebec.gouv.qc.ca/fr/version/lc/P-39.1?code=se%3A3_2&history=20231128&langCont=en
6. <https://www.legisquebec.gouv.qc.ca/fr/version/lc/p-39.1?code=se%3A17&history=20251023&langCont=en>
7. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/incidents-confidentialite-mesures-securite-entreprises>
8. <https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1%20>
9. https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_ECredits_2023-2024.pdf?v=1705585130
10. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/principaux-changements-loi-25>
11. <https://www.legisquebec.gouv.qc.ca/fr/version/lc/ccq-1991?code=se%3A1525&history=20251103&langCont=en>
12. <https://www.iso.org/standard/27701>
13. <https://www.quebec.ca/gouvernement/travailler-gouvernement/normes-gouvernance-pratiques-interne/protection-des-renseignements-personnels/activites-formation/formations-protection-renseignements-personnels-acces>
14. <https://www.oipc.bc.ca/documents/guidance-documents/2165?Lang=spa>
15. https://www.priv.gc.ca/en/privacy-topics/privacy-for-businesses/appropriate-handling-of-personal-information/gd_rd_201406/
16. <https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>
17. <https://www.nist.gov/system/files/documents/2021/01/13/Getting-Started-NIST-Privacy-Framework-Guide.pdf>
18. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/collecte-renseignements-personnels_entreprises
19. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/consentement-personnes-entreprises>
20. <https://ised-isde.canada.ca/site/loi-canadienne-anti-pourriel/fr/obtenir-consentement-pour-envoyer-courriels>
21. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/conservation-destruction-renseignements-personnels>
22. https://www.priv.gc.ca/en/privacy-topics/privacy-for-businesses/privacy-breaches-at-your-business/prevent_pb/?wbdisable=true
23. https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_EFVP.pdf?gt=obligation
24. <https://www.ncsc.gov.uk/guidance/understanding-software-service-saas-security>
25. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/encryption-and-data-protection/>
26. https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdi_crwg_publication_-_shared_responsibility_in_the_cloud_for_small_and_medium-sized-enterprises_0.pdf
27. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957322
28. https://www.priv.gc.ca/media/1966/pipeda_sa_tool_200807_e.pdf
29. <https://www.gov.uk/government/publications/data-protection-caseworker-guidance/data-protection-caseworker-guidance>

30. <https://oipc.ab.ca/resource/work-from-home-transitioning-records/>
31. <https://ico.org.uk/media2/migrated/4026547/disclosure-1-ico-outcome-to-psni-ic-250806-z1n6.pdf>
32. <https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035>
33. <https://ised-isde.canada.ca/site/cybersecure-canada/en/cybersecure-canada-information-sheet>
34. <https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2025>
35. <https://www150.statcan.gc.ca/n1/pub/11-621-m/11-621-m2026008-eng.htm>
36. <https://www150.statcan.gc.ca/n1/pub/11-621-m/11-621-m2026010-eng.htm>
37. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/09/sme-digitalisation-to-manage-shocks-and-transitions_735fc44d/eb4ec9ac-en.pdf
38. <https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm>
39. <https://www.bdc.ca/en/articles-tools/blog/cyberattacks-small-businesses-remain-denial>
40. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/sanctions-entreprises-poursuites>
41. <https://www.cisecurity.org/controls/cis-controls-navigator>

L'ÉDITEUR

À propos de 2727 Coworking

2727 Coworking is a Montreal workspace and business-address provider. We serve people who need a place to focus, meet, run a small business or establish a professional mailing presence. Our website offers English and French information about workspace options and services, alongside educational resources for operating a business in Canada.

A workspace that fits the day

Our workspace options include private offices, day passes and desks, and a conference room. These formats help individuals and teams compare a dedicated office with more flexible ways to work or hold a meeting. Prospective members can explore the virtual tour, review current pricing and book a visit before choosing a workspace.

Business addresses and mail

2727 Coworking provides business-address and virtual-mailbox services. Our resources explain the documents and practical questions involved, including guidance for people outside Canada. Service eligibility, included features, availability and access arrangements should be confirmed on the applicable service page or with our team.

Resources for Canadian small businesses

We publish guides, research and planning tools about workspace decisions, business addresses and starting a business in Canada. Our incorporation research includes information for people inside Canada and abroad, with jurisdiction-specific material to help readers identify the next questions to investigate. These educational resources complement our workspace and address services; they are not individualized legal, tax or immigration advice.

Visit or contact 2727 Coworking

Explore [private offices](#), [day passes and desks](#), [the conference room](#), [business addresses](#) and [virtual mailboxes](#). [Book a visit](#) or [contact the team](#) to discuss your needs.

A business address alone does not establish tax residence, immigration status, banking approval or eligibility for a government program.

Site Web : <https://2727coworking.com>

Cet article est de nature informative. Validez toute décision médicale, juridique, financière, réglementaire ou technique importante auprès de professionnels compétents et des sources primaires citées. Les services de l'entreprise sont décrits séparément des constats de recherche de l'article.