

LOI 25 · ARTICLES 3.3 ET 17, RLRQ C. P-39.1

Gabarit d'évaluation des facteurs relatifs à la vie privée (EFVP)

Un modèle prêt à remplir pour documenter les risques d'un projet qui touche des renseignements personnels, y compris les projets d'intelligence artificielle.

Quand ce gabarit est-il obligatoire?

La Loi sur la protection des renseignements personnels dans le secteur privé, telle que modifiée par la Loi 25, impose une EFVP dans deux situations :

- **Article 3.3** : 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. Déployer un outil d'IA qui traite des données de clients ou d'employés entre dans cette catégorie.
- **Article 17** : avant de communiquer des renseignements personnels à l'extérieur du Québec, notamment quand ton fournisseur d'IA ou d'infonuagique héberge ses serveurs aux États-Unis.

L'évaluation doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

Loi sur la protection des renseignements personnels dans le secteur privé, art. 3.3, RLRQ c. P-39.1

PRINCIPE DE PROPORTIONNALITÉ

Un petit projet avec peu de renseignements peu sensibles peut se contenter d'une EFVP courte. Un système biométrique, un outil de pointage de crédit ou un agent d'IA qui prend des décisions exige une analyse approfondie. Adapte la profondeur des sections qui suivent à ton projet.

Le responsable de la protection des renseignements personnels de l'entreprise doit être consulté **dès le début du projet**, pas une fois le contrat signé. Si tu n'as pas encore désigné ce responsable, utilise la lettre type de désignation disponible dans la même bibliothèque de ressources.

Section 1 : fiche du projet

Nom du projet

.....

Porteur du projet (nom, titre, service)

.....

Responsable de la protection des renseignements personnels consulté (nom et date de la première consultation)

.....

Description du projet (que fait le système, pour qui, avec quelles données; nomme les outils d'IA et les fournisseurs impliqués)

.....

.....

.....

Type de projet

☐ Acquisition d'un système ☐ Développement interne ☐ Refonte d'un système existant

☐ Prestation électronique de services

Date de mise en service visée

.....

Section 2 : inventaire des renseignements personnels

Liste chaque catégorie de renseignements que le projet recueille, utilise, communique, conserve ou détruit. Un renseignement est sensible s'il suscite un haut degré d'attente raisonnable en matière de vie privée : santé, finances, biométrie, origine ethnique, opinions, géolocalisation fine.

Catégorie de renseignements	Personnes concernées	Sensible?	Source de collecte	Support et localisation

Exemples de catégories : identité (nom, courriel), données RH (CV, évaluations), données financières, historique de navigation, contenu des conversations soumises à une IA.

Section 3 : finalités, nécessité et conservation

Finalité principale (à quoi serviront précisément ces renseignements)

.....

.....

Test de nécessité (le projet peut-il atteindre son objectif avec moins de renseignements, des données dépersonnalisées ou anonymisées? justifie)

.....

.....

Durée de conservation prévue et mode de destruction ou d'anonymisation

.....

.....

Consentement (comment le consentement est-il obtenu? est-il manifeste, libre, éclairé et donné à des fins spécifiques?)

Section 4 : flux de données et acteurs

Acteur	Rôle dans le traitement	Accès à quels renseignements	Encadrement contractuel

Inclus les équipes internes, les sous-traitants, les fournisseurs d'IA et d'hébergement. Un mandat confié à un tiers doit faire l'objet d'un contrat écrit qui protège les renseignements.

Les renseignements sortent-ils du Québec?

☐ Non ☐ Oui, remplir obligatoirement la section 6 ☐ À confirmer avec le fournisseur

Section 5 : analyse des risques

Évalue chaque risque selon sa probabilité (faible, moyenne, élevée) et la gravité de ses conséquences pour les personnes concernées. Risques typiques d'un projet d'IA : accès non autorisé, réidentification de données anonymisées, utilisation des données pour entraîner les modèles du fournisseur, dérive de finalité, décision automatisée sans transparence, fuite chez un sous-traitant.

Risque identifié	Probabilité	Gravité	Conséquences pour les personnes

Section 6 : communication à l'extérieur du Québec (article 17)

À remplir dès qu'un renseignement personnel est communiqué, hébergé ou accessible à l'extérieur du Québec. L'article 17 exige une évaluation qui tient compte des éléments suivants; la communication ne peut avoir lieu que si l'évaluation démontre que les renseignements bénéficieraient d'une protection adéquate, et elle doit être encadrée par une entente écrite.

Destination (pays, fournisseur, service précis)

.....

Sensibilité des renseignements communiqués

.....

Fins auxquelles les renseignements seront utilisés là-bas

Mesures de protection chez le destinataire (chiffrement, certifications, clauses contractuelles, engagement de non-entraînement des modèles)

Régime juridique de l'État de destination (les lois locales offrent-elles une protection comparable aux principes québécois? pense au CLOUD Act américain)

ALTERNATIVE SIMPLE

Si l'évaluation ne démontre pas une protection adéquate, la communication est interdite. L'option la plus directe reste de choisir un fournisseur qui héberge et traite les données au Canada. C'est l'approche de Kébek : hébergement exclusif au Canada, aucun entraînement des modèles sur tes données.

Section 7 : mesures d'atténuation

Mesure	Responsable	Échéance	Statut

Exemples : dépersonnalisation avant envoi à l'IA, restriction des accès par rôle, journalisation des requêtes, clause contractuelle de non-entraînement, formation des équipes, plan de réponse aux incidents.

Section 8 : conclusion et signatures

Avis du responsable de la protection des renseignements personnels

Décision

☐ Projet approuvé ☐ Approuvé avec conditions (voir section 7) ☐ Projet refusé ou reporté

Responsable de la protection des renseignements personnels : nom, signature, date

Porteur du projet : nom, signature, date

APRÈS L'EFVP

- Conserve ce document : la Commission d'accès à l'information peut demander à voir tes évaluations.
- Réévalue à chaque changement significatif du projet, du fournisseur ou des données traitées.
- Reporte les systèmes évalués dans ton registre des systèmes d'IA, disponible dans la même bibliothèque.

Avis : ce gabarit est un outil d'aide fourni gratuitement par Kébek IA. Il ne constitue pas un avis juridique et ne remplace pas les orientations de la Commission d'accès à l'information du Québec. Valide ta démarche avec un professionnel qualifié. Références : Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c. P-39.1, art. 3.1, 3.3 et 17. Document publié en juillet 2026 sur kebek.ai. Reproduction permise à l'interne de ton organisation.