

La Société et ses employés doivent protéger la vie privée des renseignements personnels des clients, en assurant leur confidentialité et leur sécurité. La collecte, l'utilisation, la conservation, la communication et la destruction des renseignements personnels doivent être effectuées conformément à la Loi 25 du Québec, qui modifie la Loi sur la protection des renseignements personnels dans le secteur privé.

Toute communication doit être conforme aux exigences légales et réglementaires, y compris les dispositions relatives au consentement, aux obligations légales ou à l'intérêt légitime. La Société a établi une « **Politique de confidentialité pour la collecte, l'utilisation, la conservation et la destruction des renseignements personnels** », qui est fournie aux clients lors du processus d'ouverture de compte ou avec la politique de placement.

Le Responsable de la protection de la vie privée (RPVP) est chargé de s'assurer que tous les employés et agents connaissent les politiques de confidentialité de la Société avant d'interagir avec les clients, et que tous les rôles et responsabilités tout au long du cycle de vie des renseignements personnels sont clairement définis et communiqués.

RÔLES ET RESPONSABILITÉS

Tout au long du cycle de vie des renseignements personnels, tous les employés sont responsables de leur protection:

- **Collecte** : Les employés doivent s'assurer que les renseignements personnels sont recueillis légalement et uniquement aux fins clairement identifiées auprès du client.
- **Utilisation** : Les renseignements ne peuvent être utilisés qu'aux fins prévues et doivent être traités avec une stricte confidentialité.
- **Conservation** : Les renseignements personnels ne doivent être conservés qu'aussi longtemps que nécessaire pour atteindre les fins pour lesquelles ils ont été recueillis, à moins que la loi n'en dispose autrement.

- **Destruction** : Une fois le délai de conservation expiré, les renseignements personnels doivent être détruits de manière sécurisée, en veillant à ce qu'aucune personne non autorisée ne puisse accéder aux données. Le processus de destruction suivra des procédures sécurisées, telles que le déchiquetage de documents ou la suppression de données numériques, conformément à la Loi 25.

Le RPVP supervisera ce processus et assurera la conformité à chaque étape du cycle de vie de l'information.

PROGRAMME DE FORMATION

1. Nouveaux employés ou agents :

Avant de traiter avec des clients, les nouveaux employés ou agents doivent consulter la politique. Une réunion aura lieu entre le RPVP et l'employé pour clarifier toute question. L'employé doit ensuite signer le certificat de l'employé dans le système de conformité.

2. Employés ou agents existants :

Annuellement, ou au besoin, chaque employé ou agent doit réviser la politique. Une réunion avec le RPVP suivra pour assurer la compréhension, et l'employé signera le certificat de l'employé.

Le RPVP veillera à ce que la politique de confidentialité de la Société soit respectée en vérifiant périodiquement qu'elle est affichée de manière bien visible, mise en œuvre et accessible. Les préoccupations ou les plaintes concernant le traitement des renseignements personnels doivent être adressées au RPVP, et la Société enquêtera sur toute plainte et la résoudra par le biais d'un processus de gestion des plaintes bien documenté.

PROCESSUS DE GESTION DES PLAINTES

Afin d'assurer la conformité à la Loi 25 et de répondre aux préoccupations concernant le traitement des renseignements personnels, la Société a établi un processus formel de traitement des plaintes relatives à la vie privée:

- **Dépôt d'une plainte** : Les clients ou les employés peuvent déposer une plainte relative à la vie privée en contactant le RPVP.
- **Enquête** : Dès réception d'une plainte, le RPVP mènera une enquête approfondie pour déterminer s'il y a eu une violation ou une mauvaise manipulation des renseignements personnels.
- **Accès et rectification** : L'officier désigné de la Société est responsable de répondre à toute demande d'accès ou de rectification des renseignements personnels d'un client dans les 30 jours suivant la réception de la demande.

- **Prolongation :** Si plus de temps est nécessaire, le client ou l'employé sera informé par écrit de la prolongation, tel que permis par les lois applicables.
- **Résolution :** La Société prendra des mesures correctives si nécessaire et communiquera la résolution au plaignant.
- **Signalement :** Si la loi l'exige, le RPVP avisera la Commission d'accès à l'information (CAI) et les autres autorités compétentes au Québec de toute violation importante.

PROTECTION DES RENSEIGNEMENTS PERSONNELS

Dans le cadre des activités de la Société, des renseignements personnels tels que l'identité (ex. : nom, date de naissance, citoyenneté), des détails financiers (ex. : revenus, état civil) et d'autres données pertinentes (ex. : numéro d'assurance sociale) peuvent être recueillis. Ces informations sont confidentielles et les employés doivent les protéger conformément à la Loi 25 du Québec. Les renseignements personnels ne peuvent être communiqués qu'avec le consentement écrit explicite du client ou une autorisation légale.

Les employés doivent s'assurer que les renseignements personnels sont utilisés uniquement aux fins prévues, telles que l'ouverture de comptes, le respect des obligations réglementaires ou l'application des droits légaux de la Société. L'accès, l'utilisation ou la communication non autorisés de renseignements personnels sont strictement interdits.

ACCÈS DES CLIENTS AUX RENSEIGNEMENTS PERSONNELS

Les clients ont le droit d'accéder à leurs renseignements personnels et de demander des corrections si nécessaire. Toutefois, l'accès peut être restreint dans les cas permis par la loi. Les clients peuvent demander l'accès ou s'informer sur les politiques de confidentialité de la Société en contactant le RPVP.

RÈGLES DE BASE POUR PROTÉGER LA CONFIDENTIALITÉ

1. Limiter la communication :

Les renseignements confidentiels ne doivent être partagés qu'avec des personnes ou entités ayant un besoin légitime de savoir ou avec le consentement explicite du client, conformément aux obligations légales de la Loi 25.

2. Empêcher l'accès non autorisé :

Les employés doivent prendre toutes les précautions nécessaires pour protéger les renseignements confidentiels, notamment:

- Éviter les discussions sur des renseignements confidentiels dans des lieux publics ou non sécurisés.
- Restreindre l'accès aux fichiers informatiques par des mesures de sécurité appropriées.
- S'assurer qu'aucune personne non autorisée, y compris le personnel temporaire, n'accède aux données confidentielles sans autorisation appropriée.

3. Élimination des documents :

Toute copie inutile de documents contenant des renseignements confidentiels doit être solidement déchiquetée ou détruite.

PROTECTION FORMATION CONTINUE DES EMPLOYÉS SUR LA PROTECTION DE LA VIE PRIVÉE

Les employés recevront une formation régulière sur la protection de la vie privée et sur l'importance de se conformer à la Loi 25. La formation couvrira tous les aspects du cycle de vie de l'information, y compris la collecte, l'utilisation, la conservation et la destruction sécurisée des renseignements personnels.

GESTION DES VIOLATIONS DE LA VIE PRIVÉE

Une violation de la vie privée se produit lorsqu'il y a un accès, une collecte ou une communication non autorisée de renseignements personnels. Toute violation doit être signalée immédiatement. Le RPVP dirigera les enquêtes et s'assurera que des mesures correctives sont prises, conformément aux obligations légales de la Loi 25, y compris la notification des personnes concernées et de la Commission d'accès à l'information (CAI).

Plan d'intervention en cas d'incident :

- **Confinement** : Contenir immédiatement la violation.
- **Enquête** : Le RPVP dirigera l'enquête et fera remonter l'information à l'interne ou à l'externe si nécessaire.
- **Évaluation des risques** : Déterminer la portée de la violation, y compris le type d'information impliquée et le nombre de personnes touchées.
- **Notification** : Si nécessaire, aviser les personnes touchées, les organismes de réglementation et les autres autorités compétentes telles que la CAI.
- **Prévention future** : Prendre les mesures nécessaires pour prévenir de nouvelles violations (mise à jour des politiques, renforcement de la sécurité, formation supplémentaire).

Communication aux fournisseurs externes et aux autorités

Evovest peut avoir besoin de partager des renseignements personnels avec des fournisseurs externes pour fournir des services ou gérer des relations d'affaires ou d'emploi. Avant de le faire, Evovest s'assure que ces fournisseurs disposent de mesures adéquates pour maintenir la confidentialité et la sécurité.

Dans certains cas, Evovest peut être légalement tenue de communiquer des renseignements personnels à des autorités gouvernementales ou des organismes de réglementation. Certains fournisseurs externes peuvent utiliser des technologies de traitement de données situées à l'extérieur du Québec ou du Canada.

DIX PRINCIPES DE CONFIDENTIALITÉ

Conformément à la Loi 25, la Société adhère aux principes suivants :

1. **Responsabilité** : La Société est responsable des renseignements personnels sous son contrôle.
2. **Détermination des fins** : Les fins de la collecte doivent être clairement communiquées avant la collecte.
3. **Consentement** : Les renseignements ne peuvent être recueillis, utilisés ou communiqués sans le consentement du client, sauf exception légale.
4. **Limitation de la collecte** : Seuls les renseignements nécessaires aux fins identifiées doivent être recueillis.
5. **Limitation de l'utilisation, de la communication et de la conservation** : Les renseignements ne doivent être utilisés qu'aux fins originales et conservés uniquement le temps nécessaire.
6. **Exactitude** : Les renseignements doivent être exacts, complets et à jour.
7. **Mesures de sécurité** : La Société doit protéger les renseignements par des mesures de sécurité appropriées.
8. **Transparence** : La Société doit être transparente quant à ses politiques et procédures.
9. **Accès individuel** : Les clients ont le droit d'accéder à leurs renseignements et de demander des corrections.
10. **Possibilité de porter plainte** : Les clients peuvent contester la conformité de la Société auprès du RPVP ou des autorités.

Évaluations des facteurs relatifs à la vie privée (EFVP)

Conformément à la Loi 25 et aux directives de la Commission d'accès à l'information du Québec (CAI), la Société s'engage à mener des (Évaluation des facteurs relatifs à la vie privée, EFVP) dans les conditions suivantes :

Quand une EFVP est requise

Une EFVP sera menée avant de mettre en œuvre tout projet, système ou technologie impliquant :

- La collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
- L'acquisition, le développement ou la refonte de systèmes d'information ou de systèmes de prestation de services électroniques traitant des renseignements personnels.

- Toute activité pouvant avoir un impact élevé sur la vie privée ou les droits des individus.

Objectifs de l'EFVP

EFVP a objet de:

- Identifier et évaluer les risques potentiels pour la vie privée.
- S'assurer que les renseignements sont traités dans le respect de la Loi 25.
- Recommander des mesures pour atténuer les risques identifiés.

Responsabilités

- **Responsable de la protection de la vie privée (RPVP)** : Supervise le processus d'EFVP, en veillant à ce qu'il soit mené efficacement et conformément aux exigences légales.
- **Chefs de projet** : Collaborent avec le RPVP pour fournir les informations nécessaires et mettre en œuvre les mesures recommandées.
- **Employés** : Participent à l'EFVP selon les besoins et respectent les mesures établies pour protéger les renseignements personnels.

Processus de l'EFVP

1. Initiation :

- **Identification du projet** : Toute nouvelle initiative impliquant des renseignements personnels doit être signalée au RPVP.
- **Analyse préliminaire** : Déterminer si une EFVP est nécessaire en fonction de la portée et de la nature du projet.

2. Évaluation :

- **Description de l'initiative** : Documentation détaillée des objectifs du projet, des processus et des technologies utilisées.
- **Analyse des renseignements personnels impliqués** : Type, sensibilité et volume des données personnelles collectées ou traitées.
- **Identification des risques** : Évaluer les risques potentiels pour la vie privée, y compris l'accès non autorisé, la perte ou l'utilisation abusive des données.
- **Vérification de la conformité légale** : S'assurer que toutes les activités sont conformes à la Loi 25 et aux autres réglementations applicables.

3. Mesures d'atténuation :

- **Recommandations** : Développer des stratégies pour atténuer les risques identifiés, comme le renforcement des mesures de sécurité ou la limitation de la collecte de données.
- **Plan de mise en œuvre** : Décrire les étapes pour mettre en œuvre les mesures recommandées.

4. Documentation :

- **Rapport d'EFVP** : Compiler toutes les conclusions, analyses et recommandations dans un rapport formel.
 - **Approbation** : Obtenir l'approbation signée du RPVP et de la haute direction concernée avant de procéder.
- 5. Consultation auprès de la CAI :**
- Si des risques résiduels élevés subsistent après les efforts d'atténuation, la Société consultera la CAI pour obtenir des conseils avant la mise en œuvre.
- 6. Surveillance et examen :**
- **Évaluation continue** : Surveiller continuellement le projet pour détecter de nouveaux risques ou des changements de portée.
 - **Mises à jour périodiques** : Examiner et mettre à jour l'EFVP au besoin, particulièrement en cas de modifications importantes du projet.

Tenue des dossiers et conservation

- Tous les rapports d'EFVP et les documents connexes seront stockés de manière sécurisée et conservés conformément aux politiques de conservation des données de la Société.
- L'accès aux documents d'EFVP est restreint au personnel autorisé afin de maintenir la confidentialité.

Formation et sensibilisation

- **Éducation des employés** : Les employés impliqués dans des projets nécessitant une EFVP recevront une formation sur le processus d'EFVP et leurs responsabilités.
- **Programmes de sensibilisation** : Des mises à jour régulières et des ressources seront fournies pour s'assurer que tout le personnel comprend l'importance des évaluations des facteurs relatifs à la vie privée.