POLITIQUE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Date d’entrée en vigueur : 20 mars 2025

Version	Statut	Date d’approbation
V1	En vigueur	20 mars 2025

Politique sur la protection des renseignements personnels

Table des matières

1. Objectif

1.1 La présente Politique (tel que ce terme est défini ci-dessous) a pour objectif de permettre à RGP (tel que ce terme est défini ci-dessous) d'informer les Clients (tel que ce terme est défini ci-dessous) du traitement de leurs Renseignements personnels en toute transparence, par exemple en leur expliquant clairement pourquoi et comment il collecte, utilise et divulgue leurs Renseignements personnels. Cette Politique vise également à assurer la protection et la sécurité des Renseignements personnels utilisés et conservés par RGP, conformément à la Loi.

1.2 Cette Politique sert de document-cadre à toutes les autres politiques, directives et normes associées. RGP peut, selon ses besoins commerciaux et ses exigences légales et de conformité, aller au-delà des exigences de protection sur les Renseignements personnels énoncées dans ce document. Toutefois, RGP atteindra, au minimum, les niveaux de sécurité requis dans cette Politique.

2. Champ d'application

Cette Politique s'applique aux renseignements personnels que RGP, ou ses fournisseurs agissant en son nom, recueillent, utilisent ou divulguent concernant les Clients. Elle couvre la gestion des renseignements personnels sous forme verbale, écrite ou électronique. L'objectif de cette Politique est d'informer les Clients sur la manière dont RGP collecte, utilise, divulgue, conserve et protège leurs renseignements personnels des Clients.

3. Définitions

3.1 **« Collecte »** signifie l'action de recueillir, d'acquérir ou d'obtenir des Renseignements personnels de quelque façon et par quelque moyen que ce soit, y compris auprès de Tiers.

3.2 **« Confidentialité »** signifie la garantie que les renseignements personnels sont protégés contre tout accès, Divulgation ou Utilisation non autorisés.

3.3 **« Consentement »** signifie un accord libre à la Collecte, à l'Utilisation ou à la Divulgation de Renseignements personnels aux fins déterminées par RGP. Le Consentement peut être explicite ou implicite et peut être donné directement par le Client ou par un mandataire autorisé. Le Consentement explicite peut être donné de vive voix, par des moyens électroniques ou par écrit. Toutefois, il doit toujours être manifeste, libre, éclairé et être donné à des fins spécifiques. Le Consentement implicite désigne un Consentement que l'on peut raisonnablement déduire d'un acte ou d'une omission de la part d'une personne.

3.4 **« Destruction »** signifie l'élimination définitive et irréversible des Renseignements personnels, de manière à ce qu'ils ne puissent plus être récupérés ou reconstitués.

3.5 **« Divulgation »** signifie l'action de révéler ou de communiquer des Renseignements personnels à un Tiers.

3.6 *«* **Loi** *»* désigne la *Loi sur la protection des renseignements personnels dans le secteur privé* (Québec).

3.7 **« Client(s) »** signifie tout client de RGP.

3.8 **« Politique »** signifie la présente politique sur la protection des Renseignements personnels, telle que modifiée de temps à autres.

3.9 **« Renseignement(s) personnel(s) »** signifie une information concernant une personne physique qui, seule ou combinée à d'autres données, permet de l'identifier directement ou indirectement, y compris ses noms, adresses postales, adresses courriel, date de naissance ou données de crédit.

3.10 **« Responsable de la protection des renseignements personnels »** signifie une ou plusieurs personnes nommées par RGP, conformément à l'article 4 de la Politique, pour assurer le respect et l'application de cette Politique ainsi que des lois en vigueur concernant la protection des Renseignements personnels.

3.11 **« RGP »** désigne REGAR Inc., ses divisions, filiales et sociétés affiliées, y compris R.E.G.A.R. Gestion Privée Inc. et le Programme Standop.

3.12 **« Site(s) »** signifie tous les site web, y compris les sites de commerce en ligne, médias sociaux, applications mobiles et autres plateformes appartenant à RGP.

3.13 **« Tiers »** signifie une personne autre que le Client, que RGP ou qu'un mandataire de cette dernière.

3.14 **« Utilisateur »** signifie quelqu'un qui accède et interagit avec le contenu et les fonctionnalités du Site. Cela peut inclure des actions comme naviguer entre les pages, cliquer sur des liens, remplir des formulaires, etc.

3.15 **« Utilisation »** signifie le traitement, la manipulation et la gestion de Renseignements personnels par RGP.

4. Responsable de la protection des renseignements personnels

4.1 Conformément à la Loi, RGP doit désigner la personne ayant la plus haute autorité pour veiller au respect et à la mise en œuvre des dispositions relatives à la Loi. Cette personne exerce la fonction de Responsable de la protection des renseignements personnels et peut déléguer cette fonction, en tout ou en partie, par écrit à toute personne de son choix.

4.2 Le titre et les coordonnées du Responsable de la protection des renseignements personnels sont publiés sur les Sites ou, à défaut, rendus accessibles par tout autre moyen approprié.

4.3 Les tâches du Responsable de la protection des renseignements personnels incluent, sans s'y limiter :

- coordonner l'approbation des politiques et des pratiques en matière de protection des renseignements personnels par le conseil d'administration de RGP;
- le traitement des demandes des Clients en matière de protection des Renseignements personnels;
- le Responsable de la protection des renseignements personnels joue un rôle clé en tant que répondante auprès des autorités règlementaires et veille à ce que les employés de RGP soient informés des modalités de la Politique;
- elle communique aux employés de RGP toutes les informations et le matériel nécessaires pour assurer le respect de la Politique; et
- elle supervise le processus en cas d'atteinte à la vie privée et traite également les demandes de renseignements et les plaintes des Clients, le tout en conformité avec la politique sur le traitement des plaintes.

5. Gestion des Renseignements personnels

5.1 Pour garantir la protection des Renseignements personnels, RGP doit mettre en œuvre des mesures appropriées, que ces informations soient sous forme papier ou électronique. Cette responsabilité couvre toutes les étapes, de la Collecte à la Destruction des Renseignements personnels, en passant par leur Utilisation, communication et conservation.

5.2 De plus, il est essentiel que RGP permette à tout Client d'accéder à ses Renseignements personnels à tout moment et de les mettre à jour s'ils sont erronés ou incomplets.

6. Consentement

6.1 RGP doit obtenir le Consentement du Client, pour l'Utilisation ou la Divulgation de leurs Renseignements personnels.

6.2 Si le Client retire son Consentement, RGP doit expliquer les répercussions sur la prestation des services, bien que certaines exigences légales ou contractuelles puissent empêcher ce retrait. En cas de refus de Collecte de certains renseignements, RGP pourrait ne pas être en mesure de fournir le service demandé.

7. Collecte des Renseignements personnels

7.1 RGP s'engage à définir les finalités de la Collecte des Renseignements personnels avant toute Collecte. Les objectifs de chaque Collecte sont clairement expliqués aux Clients conformément à ce qui est requis par la Loi.

7.2 RGP recueille les Renseignements personnels par l'une des manières suivantes :

- directement auprès du Client;
- lors de l'Utilisation des produits et services;
- de nos Sites;
- lors de l'embauche de tout nouvel employé; et
- par d'autres moyens.

8. Utilisation des Renseignements personnels

8.1 RGP doit expliquer les finalités de l'Utilisation des renseignements personnels recueillis auprès du Client. Si ces renseignements sont utilisés à des fins autres que celles initialement prévues, RGP doit obtenir le Consentement explicite du Client, sauf si cette Utilisation ou communication est requise ou permise par la Loi.

8.2 RGP doit utiliser les renseignements personnels uniquement aux fins prévues et informer les Clients des raisons de cette Collecte ainsi que de la manière dont ces renseignements seront utilisés.

9. Mesure de sécurité et de Confidentialité

9.1 RGP doit s'assurer que les personnes autorisées avec qui il divulgue ou échange des Renseignements personnels ont signé un engagement de Confidentialité. Il doit également obtenir un engagement de ses employés à protéger la Confidentialité et la non-divulgation des Renseignements personnels nécessaires à leurs fonctions.

9.2 RGP doit s'assurer que tous les fournisseurs de services et partenaires s'engagent contractuellement à respecter ses normes strictes en matière de protection et de Confidentialité des Renseignements personnels des Clients. Il ne doit leur confier que les Renseignements personnels nécessaires à l'accomplissement de leurs tâches, fonctions et obligations contractuelles.

9.3 En plus des obligations de Confidentialité, le personnel des fournisseurs ayant accès à des Renseignements personnels doit respecter rigoureusement les règles contractuelles. Enfin, les fournisseurs et partenaires doivent appliquer des mesures de sécurité physiques, informatiques et administratives conformes à la Loi.

10. Incidents de Confidentialité

10.1 Tout incident de Confidentialité doit être déclaré immédiatement au Responsable de la protection des renseignements personnels. Une évaluation des risques doit être effectuée pour déterminer les mesures correctives nécessaires. RGP doit informer les Clients si l'incident présente un risque de préjudice sérieux pour elles après avoir obtenu l'autorisation du Chef de la conformité.

10.2 Un incident de Confidentialité se produit notamment lorsqu'il y a un accès non autorisé à des Renseignements personnels ou si des Renseignements personnels font l'objet d'une Collecte, d'une Utilisation ou d'une Divulgation non autorisée par la règlementation. Ainsi, un incident appartient à l'une des catégories suivantes :

- accès non autorisé par la Loi à un Renseignement personnel;
- Utilisation non autorisée par la Loi d'un Renseignement personnel;
- Divulgation non autorisée par la Loi d'un Renseignement personnel; et
- perte d'un Renseignement personnel ou tout autre atteinte à la protection d'un tel renseignement.

10.3 Un incident de Confidentialité peut, par exemple, se produire lors du vol d'un ordinateur portable ou de l'envoi de Renseignements personnels au mauvais destinataire.

11. Conservation

11.1 RGP doit conserver tous les dossiers des Clients, qu'ils soient sur papier ou en format électronique, pendant une durée minimale de sept (7) ans après la fin de la relation d'affaires, afin de se conformer aux exigences règlementaires.

11.2 Pour la conservation physique des dossiers, il est nécessaire d'utiliser une méthode sécurisée, telle qu'un classeur verrouillé, afin de protéger les informations sensibles. Chaque dossier du Client doit être conservé individuellement, sauf si une autorisation écrite permet de regrouper les dossiers des conjoints, ce qui facilite la gestion des documents.

11.3 En ce qui concerne la conservation électronique, il faut également utiliser une méthode sécurisée en appliquant des mesures raisonnables, telles que l'Utilisation de mots de passe robustes, de pare-feu, d'antivirus, et de copies de sauvegarde régulières. Cette liste n'est pas exhaustive, mais elle illustre les bonnes pratiques à adopter pour garantir la sécurité des données.

12. Droits à l'égard des Renseignements personnels

12.1 Tout Client peut demander à RGP d'accéder aux informations détenues à son sujet, de rectifier toute information erronée, de cesser la diffusion de ses Renseignements personnels ou de transférer ses données.

12.2 RGP doit informer le Client de ces droits. Toute demande doit être faite par écrit et recevoir un accusé de réception dans les cinq (5) jours ouvrables. La demande doit être traitée dans un délai de 30 jours civils, avec une confirmation écrite envoyée une fois la demande exécutée. En cas de réception d'une demande, l'employé doit contacter la personne responsable de la conformité dans les deux (2) jours civils.

12.2.1 **Droit d'accès :** Permet au Client de consulter ou de demander une copie de ses Renseignements personnels.

12.2.2 **Droit de rectification :** Permet de corriger des informations inexactes, incomplètes ou ambigües.

12.2.3 **Droit de retrait du consentement** : Permet au Client de retirer son consentement à l'utilisation de ses Renseignements personnels à tout moment.

12.2.4 **Droit de désindexation :** Permet à tout Client de demander à RGP de cesser la diffusion de ses Renseignements personnels ou de désindexer de ses Sites tout hyperlien rattaché à son nom permettant d'accéder à ses Renseignements personnels par un moyen technologique.

12.2.5 **Droit à la portabilité :** Permet à toute personne qui en fait la demande d'obtenir les Renseignements personnels informatisés qu'elle a fournis à RGP dans un format technologique structuré et couramment utilisé.

12.3 Les demandes doivent être faites par écrit par le Client ou, dans certains cas, par une tierce personne bénéficiant d'une autorisation écrite du Client pour agir en son nom. Cela permet au demandeur de se prévaloir de ses recours auprès de la Commission d'accès à l'information du Québec ou d'autres autorités compétentes.

13. Destruction et anonymisation des Renseignements personnels

13.1 RGP doit détruire, de façon sécuritaire et en prenant des mesures raisonnables, tout document, que ce soit sur papier ou sur support électronique. Les Renseignements personnels doivent être détruits de manière sécurisée lorsqu'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés, de manière qu'ils ne puissent être reconstitués.

13.2 RGP doit supprimer ou anonymiser les Renseignements personnels dont la durée de conservation est arrivée à terme, soit sept (7) ans après la fin de la relation d'affaires. Alors que la Destruction est un processus d'élimination définitif, l'anonymisation signifie que les Renseignements personnels de tout client sont modifiés de façon à ne plus permettre l'identification directe ou indirecte, et ce, de façon irréversible.

14. Procédure de Destruction des Renseignements personnels

14.1 Afin de garantir la Confidentialité et la sécurité des Renseignements personnels, RGP a mis en place une procédure rigoureuse de Destruction des Renseignements personnels. Cette procédure détaille les étapes nécessaires pour identifier, détruire et anonymiser les documents contenant des Renseignements personnels. Tout employé de RGP doit suivre la procédure suivante :

14.1.1 **Identification des Renseignements personnels à détruire :** Inventaire des documents physiques et numériques contenant des Renseignements personnels et classification des documents selon leur type et leur sensibilité.

14.1.2 **Méthodes de Destruction pour les documents physiques:** Déchiquetage à l'aide de déchiqueteuses.

14.1.3 **Méthodes de Destructions pour les documents numériques :** Suppression sécurisée à l'aide de logiciels spécialisés et Destruction physique des disques durs et autres supports de stockage.

14.1.4 **Anonymisation :** Application de techniques d'anonymisation pour rendre les données non identifiables avant Destruction et vérification que les données anonymisées ne peuvent pas être réidentifiées.

14.1.5 **Documentation et suivi :** Tenue d'un journal de Destruction détaillé et réalisation d'audits réguliers pour vérifier la conformité.

14.1.6 **Communication et formation :** Publication des règles de Destruction sur les Sites et formation régulière du personnel sur les procédures de Destruction et les meilleures pratiques.

14.1.7 **Sécurité :** Limitation de l'accès aux documents à détruire aux personnes autorisées.

15. Utilisation des témoins de connexions

15.1 RGP pourrait utiliser des Cookies et des technologies similaires pour améliorer l'expérience des Utilisateurs visitant ses Sites.

15.2 **Types de Cookies :**

15.2.1 **Cookies essentiels :** Ces cookies sont indispensables au bon fonctionnement des Sites, ils permettent la navigation et l'Utilisation des fonctionnalités de base.

15.2.2 **Cookies de préférences :** Ces cookies mémorisent des informations modifiant l'apparence ou le comportement des Sites, comme la langue préférée ou la région de l'Utilisateur.

15.2.3 **Cookies de performance :** Ces cookies collectent des données sur l'Utilisation des sites, comme les pages les plus visitées, afin d'améliorer les sites et l'expérience de l'Utilisateur.

15.2.4 **Cookies de statistiques :** En recueillant et communiquant des informations de manière anonyme, ces cookies aident RGP à comprendre comment les Utilisateurs interagissent avec les Sites.

15.2.5 **Cookies de publicité (ou Marketing) :** RGP peut utiliser des cookies tiers pour diffuser des publicités personnalisées en fonction des intérêts des Utilisateurs.

15.3 **Contrôle des Cookies :**

15.3.1 Les Utilisateurs peuvent généralement configurer leur navigateur pour refuser les Cookies ou être avertis de leur envoi.

16. Révision annuelle

Cette Politique sera revue et mise à jour annuellement pour s'assurer qu'elle reste conforme aux lois et règlements en vigueur, ainsi qu'aux meilleures pratiques en matière de protection des Renseignements personnels.

17. Entrée en vigueur

La présente Politique peut être modifiée en tout temps à l'entière discrétion de RGP sans préavis. Toute modification entrera en vigueur lorsqu'elle sera approuvée par les membres du conseil d'administration de RGP et que sa version modifiée sera publiée sur le Site Web de RGP. La mention de la « date d'entrée en vigueur » au début de la présente Politique indique la date à laquelle elle a été mise à jour pour la dernière fois.