

POLITIQUE DE GESTION DES RENSEIGNEMENTS PERSONNELS (PGRP)

1. INTRODUCTION

La présente politique entend répondre aux exigences de la loi et au désir de notre organisation de respecter son personnel et d'inspirer confiance à ses partenaires. À cette fin, notre politique présente les mesures adéquates pour protéger les renseignements personnels (RP) contre l'accès non autorisé, le vol et l'altération indue et pour assurer leur intégrité, leur confidentialité et leur disponibilité auprès des personnes admissibles seulement.

2. OBJECTIFS

Dans le cadre de ses activités, notre organisation recueille, détient, utilise et communique des RP. Ces RP peuvent revêtir différents caractères (légal, administratif, financier, gestion de la clientèle, etc.) et sont essentiels à nos activités.

Les objectifs de cette politique visent à :

- Assurer la protection des RP recueillis, détenus et communiqués par notre organisation, par de bonnes pratiques de gestion des RP.
- Déployer des mesures de protection permettant de réduire les risques d'atteinte à la vie privée, tels que l'accès non autorisé aux RP, incluant notamment le vol d'informations.
- Préserver l'intégrité de l'information, tout au long de son cycle de vie.

3. PORTÉE

La présente politique s'adresse et s'applique à toute personne physique ou morale (partenaire régulier ou occasionnel) ayant accès aux RP, et ce, sans égard au statut d'emploi, y compris les propriétaires, dirigeants, employés permanents ou occasionnels, administrateurs et fournisseurs en relation avec notre organisation.

4. APPLICATION

Les employés sont informés de l'existence de la politique, et doivent la consulter périodiquement et se conformer aux exigences y étant énoncées. Qui plus est, les fournisseurs de services à qui des renseignements personnels sont confiés dans le cadre de nos activités respectent les principes énoncés dans la PGRP.

La direction générale, en collaboration avec le/les personnes responsables de la protection des renseignements personnels (RPRP), veille à l'application de la PGRP et s'assure d'instaurer une culture de sécurité des RP au sein de l'organisation.

5. RENSEIGNEMENTS CONCERNÉS

La présente politique concerne tout renseignement identifiant directement ou indirectement une personne, ou susceptible de procurer des informations privées (p. ex. statut matrimonial), voire intimes (p. ex. données médicales) sur une personne.

6. ÉTENDUE

6.1 Collecte

La présente politique autorise uniquement la collecte des RP nécessaires à l'exercice de nos activités, lesdits RP ne pouvant être obtenus qu'auprès des personnes autorisées, le tout à la connaissance et avec l'approbation de la personne à laquelle se rapportent les RP en cause, à moins d'exigences contraires (p. ex. légales). Dans toute la mesure du possible, l'organisation s'assure que les RP admissibles recueillis sont exacts, à jour, fiables et traçables.

6.2 Utilisation

La présente politique requiert de déterminer les fins de la collection avant de recueillir des RP. Elle permet la collecte, l'utilisation et la conservation des RP exclusivement aux fins pour lesquelles ils ont été demandés. Lesdits RP pourront être communiqués uniquement aux personnes physiques ou morales auxquelles il est requis de les communiquer dans le cadre de nos activités et, lorsque requis, seulement sur approbation de la personne concernée par ces RP. Il importe toutefois de noter que certains RP pourraient être divulgués sans l'autorisation de la personne visée dans les cas où la chose est prévue et imposée par la loi.

6.3 Protection

La présente politique prévoit que l'organisation prend les mesures requises pour que ses dirigeants et employés respectent la confidentialité des RP et les préserve de toute divulgation, tout accès ou toute utilisation non autorisée. Elle prévoit également que des ententes de confidentialité seront convenues avec tous les intervenants externes auxquels recourt notre organisation (fournisseurs, consultants, etc.). À cette fin, ont été mis au point :

- une catégorisation des RP permettant, notamment, de les protéger en fonction de leur valeur et des risques auxquels ils sont exposés, et de limiter la divulgation des RP aux personnes autorisées à les utiliser par nécessité, le tout afin d'assurer la confidentialité des RP tout au long de leur cycle de vie. Cela doit se faire en respectant les exigences légales et selon le niveau de sensibilité de ces RP;
- une procédure de traitement des plaintes concernant la protection des RP;
- des mesures ou contrôles permettant de prévenir les incidents de confidentialité (notamment la procédure de gestion des incidents de confidentialité et le registre afférent), la fraude, les fuites d'information ou d'exfiltration, les attaques informatiques, les erreurs accidentelles, les actions délibérées et l'atteinte à la vie privée;
- une méthode de sensibilisation des dirigeants/employés/intervenants aux risques, à la sécurité et à la protection des RP, notamment en offrant des formations adaptées sur la gestion des RP, sur leur rôle et responsabilités à l'égard des RP, et sur les éléments en place permettant de parer aux incidents de confidentialité;
- l'obligation de signaler sans tarder à l'autorité compétente (responsable de la protection des RP ou comité des RP) tout problème lié aux RP, tels que tout incident ou tout acte susceptible de représenter un incident de confidentialité ou un incident de sécurité tel que le vol, l'intrusion dans un réseau ou système, les dommages délibérés, l'utilisation abusive, la fraude, les tentatives d'accès non autorisés ou événements de même nature;
- une procédure permettant d'aviser la Commission sur l'accès à l'information si un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé.

6.4 Conservation

La présente politique vise aussi la conservation sécuritaire des RP. Ainsi, notre organisation dispose de méthodes uniformisées de classement et de dénomination des documents. La conservation sécuritaire implique aussi que nous conservons sous clé des documents physiques, s'il y en a, et la conservation sécurisée des RP détenus en format électronique, le cas échéant.

D'autre part, la conservation des RP durera uniquement le temps requis par leur utilisation justifiée, à moins d'obligation légale. À cet effet, un calendrier de conservation des RP a été défini.

6.5 Destruction

La présente politique prévoit que les RP devenus inutiles en fonction de l'usage qui leur était assigné seront détruits de façon sécuritaire dans le respect des politiques de l'organisation et des lois applicables. Une destruction sécuritaire implique ici que le support des RP doit être physiquement supprimé, selon le médium de conservation, en vue de rendre impossible la récupération desdits RP après qu'on en aura disposé. La présente disposition de destruction des RP s'applique aussi en cas de décès de la personne concernée.

6.6 Désindexation

La présente politique prévoit, dans les cas où la chose pourrait s'appliquer, de désindexer dans toute la mesure du possible les RP, en les extrayant par exemple des moteurs de recherche informatique et des sites web de l'organisation s'il y a lieu.

6.7 Droits de la personne concernée par les RP

La présente politique entend respecter rigoureusement le droit de la personne concernée d'exiger qu'on obtienne son consentement avant d'utiliser ses RP, de refuser de donner certains RP sous réserve des lois applicables, de corriger ou de compléter ses RP, d'accéder en tout temps à ses RP et d'obtenir des réponses aux questions qu'elle se pose à propos de ses RP.

7. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (EFVP)

Une EFVP est requise si votre organisation planifie un des quatre types de projets suivants (c.-à-d. que l'EFVP doit être faite avant ou au tout début du projet) :

- tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels;
- la communication des RP à l'extérieur du Québec;
- l'utilisation des données biométriques;
- la réalisation d'études et de recherche et la production de statistiques.

8. RÔLES ET RESPONSABILITÉS

- Mme Leidy Avila est responsable de l'application de la présente politique et la porte à l'attention de tous les dirigeants/employés/intervenants par une diffusion adéquate.

- Mme Arian Cueto-Bergner soutient Mme Leidy Avila en assurant la mise en place de mesures et de contrôles nécessaires à l'application de la présente politique.
- Dirigeants/employés/intervenants : Chaque dirigeant/employé/intervenant s'engage à respecter tous les éléments de la présente politique sous peine de sanction appropriée ou disciplinaire pouvant aller jusqu'au congédiement. Il s'engage également à signaler tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la sécurité et à la protection des RP.

9. CONTACT DU RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (RPRP)

Pour toute question, commentaire ou plainte à l'égard de la présente Politique ou à l'égard de la gestion des renseignements personnels, communiquez avec le responsable de la protection des renseignements personnels aux coordonnées suivants :

- Mme Leidy Avila et Mme Arian Cueto-Bergner, 514.366.29.70, info@lasallenhc.com

10. RÉVISION

La présente politique, ainsi que tout ce qui s'y rapporte, sera révisée et mise à jour lorsque les circonstances l'exigeront, tout comme les mesures de protection et de sécurité qui en découlent.