LA CHARPENTERIE

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, fournisseurs, etc. en relation avec notre organisation.

4. Application

Les employés sont informés de l'existence de la politique, 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 au sein de l'organisation, une culture de sécurité des RP.

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 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 de 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 recherches informatiques 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. 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;
- communiquer des RP à l'extérieur du Québec;
- utiliser des données biométriques;
- effectuer des études, de la recherche, de la production de statistiques.

8. Rôles et responsabilités

- Responsable de la protection des RP: 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.
- Comité des RP : Soutient le Responsable de la protection des RP en assurant la mise en place de mesures et 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. Révision

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

Responsable	Sonia Morneau
Approuvé par	Comité des RP
Date d'entrée en vigueur	1er septembre 2023

Annexe I - Définitions

Termes	Définitions
Comité d'accès à l'information et la protection des RP - LAI, Article 8.1	Au sein d'un organisme public, un comité d'accès à l'information et la protection des renseignements personnels est chargé de le soutenir dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la présente loi. Ce comité exerce aussi les fonctions qui lui sont confiées par la présente loi. Le comité relève de la personne ayant la plus haute autorité au sein de l'organisme ou, dans le cas d'un ministère, du sous-ministre et, dans le cas d'une municipalité, d'un ordre professionnel ou d'un centre de services scolaire, du directeur général. Il se compose de la personne responsable de l'accès aux documents, de celle responsable de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise, incluant, le cas échéant, le responsable de la sécurité de l'information et le responsable de la gestion documentaire. Un règlement du gouvernement peut exclure un organisme public de l'obligation de former ce comité ou modifier les obligations d'un organisme en fonction de critères qu'il définit.
Consentement - LP, Article 14, entrée en vigueur le 22 septembre 2023	Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé. Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur. Le consentement du mineur de 14 ans et plus est donné par le mineur, par le titulaire de l'autorité parentale ou par le tuteur. Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé. Un consentement qui n'est pas donné conformément à la présente loi est sans effet.
Détenteur des RP	Intervenant qui détient des RP et est responsable de leur traitement. Le détenteur est rarement les TI.

Droit à la portabilité - CAI	Si la personne concernée le demande, les organisations auront l'obligation de lui communiquer, dans un format technologique structuré et couramment utilisé, un renseignement personnel informatisé recueilli auprès d'elle. Cette communication pourra aussi se faire à une personne ou à un organisme autorisé à recueillir le renseignement, à la demande de la personne concernée.
Exactitude des RP - LP, Article 11, entrée en vigueur le 22 septembre 2023	Toute personne qui exploite une entreprise doit veiller à ce que les renseignements personnels qu'elle détient sur autrui soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée. Les renseignements utilisés pour prendre une telle décision sont conservés pendant au moins un an suivant la décision.
Incident de confidentialité - LP, Article 3.6, entrée en vigueur le 22 septembre 2023	Par incident de confidentialité, on entend : ➢ l'accès non autorisé par la loi à un renseignement personnel; ➢ l'utilisation non autorisée par la loi d'un renseignement personnel; ➢ la communication non autorisée par la loi d'un renseignement personnel; ➢ la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.
Profilage - LP, article 8.1, entrée en vigueur le 22 septembre 2023	Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.
Règles	Politiques, directives, guides, procédures, plans, etc.
Renseignement anonymisé - LP, article 23, entrée en vigueur le 22 septembre 2023	Un RP est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.
Renseignement dépersonnalisé - LP, article 12, entrée en vigueur le 22 septembre 2023	Un RP est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée.
RP - LP, Article 2, entrée en vigueur le 22 septembre 2023	Tout renseignement qui concerne une personne physique et permet de l'identifier directement ou indirectement.
Renseignement sensible - LP, article 12, entrée en vigueur le 22 septembre 2023	Un RP est considéré comme sensible lorsque, de par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

RPRP - CAI	Le RPRP désigné par la LP est la personne ayant la plus haute autorité dans l'organisation. Le RPRP veille à assurer le respect et la mise en œuvre de la LP. Cette fonction peut être déléguée par écrit, en tout ou en partie, à toute personne. Dans ce cas, il est recommandé de désigner une personne pouvant assumer efficacement ce rôle. Idéalement, celle-ci devrait avoir les compétences requises et un pouvoir décisionnel important. Il est également important d'appuyer la personne responsable de la protection des renseignements personnels avec les ressources humaines, techniques et financières nécessaires pour assurer la conformité à la Loi sur le privé. La loi confie des rôles spécifiques au RPRP. En cas d'incident de confidentialité impliquant un RP, notamment, il doit : • Enregistrer les communications effectuées à toute personne ou tout organisme susceptible de diminuer le risque pour la personne concernée suivant l'incident; • Prendre part à l'évaluation du préjudice causé par l'incident.
Traitement des RP	Collecte, conservation, utilisation, échange/transfert, destruction des RP.
Traitement automatisé des RP - LP, article 12.1, entrée en vigueur le 22 septembre 2023	Toute personne qui exploite une entreprise et qui utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci doit, au moment de la décision ou avant, en informer la personne concernée. Elle doit aussi, à la demande de la personne concernée, l'informer : 1. des renseignements personnels utilisés pour rendre la décision; 2. des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision; 3. de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision. Il doit être donné à la personne concernée l'occasion de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision.