

POLITIQUE DE GOUVERNANCE VISANT À ENCADRER LA DÉTENTION DES RENSEIGNEMENTS PERSONNELS (RP)

Afin d'assurer le respect par les intervenants de la Fondation Sainte-Croix/Heriot de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels dans le secteur privé*, aussi appelée Loi 25, voici les pratiques de l'organisation en la matière.

COLLECTE DES RENSEIGNEMENTS PERSONNELS ET OBTENTION DU CONSENTEMENT

L'organisation peut collecter des renseignements personnels pour la bonne gestion de ses relations et des services avec chaque personne concernée et limiter la collecte des informations à ce qui est requis à cette fin. Le consentement de la personne concernée est nécessaire pour pouvoir légalement utiliser les renseignements personnels qu'il transmet à l'organisation.

L'organisation a mis en place un processus d'obtention du consentement de chaque personne de façon à documenter à quel moment et comment ce consentement a été obtenu ou renouvelé. La base de données de l'organisation documente le consentement obtenu ou renouvelé.

CONSULTATION ET UTILISATION DES RENSEIGNEMENTS PERSONNELS

L'organisation s'assure de respecter les paramètres suivants :

- Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de l'entreprise lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions;
- Limiter l'utilisation des renseignements personnels : à moins d'une exception prévue par la loi, l'entreprise doit obtenir le consentement de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli.
- Mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.

COMMUNICATION DES RENSEIGNEMENTS

Les renseignements personnels que la Fondation Sainte-Croix/Heriot détient sur un individu doivent lui être transmis sur demande de sa part.

D'ailleurs, l'article 27 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (LP) prévoit le droit à la portabilité des renseignements personnels entrant en vigueur à compter du 22 septembre 2024. 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.

De plus, la loi prévoit que l'organisation puisse transmettre des renseignements personnels d'un individu sur demande d'un tiers ou d'une organisation gouvernementale :

- à son procureur;
- au directeur des poursuites criminelles et pénales si le renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec;
- à un organisme chargé, en vertu de la loi, de prévenir, détecter ou réprimer le crime ou les infractions aux lois, qui le requiert dans l'exercice de ses fonctions, si le renseignement est nécessaire pour la poursuite d'une infraction à une loi applicable au Québec;
- à une personne à qui il est nécessaire de communiquer le renseignement dans le cadre d'une loi applicable au Québec ou pour l'application d'une convention collective;
- à un organisme public au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements publics et sur la protection des renseignements personnels qui, par l'entremise d'un représentant, le recueille dans l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion;
- à une personne ou à un organisme ayant pouvoir de contraindre à leur communication et qui les requiert dans l'exercice de ses fonctions;
- à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;
- à des tiers en vue de prévenir un acte de violence, dont un suicide et lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence;
- à un service d'archives dans certaines conditions et/ou après un certain délai;
- à une personne qui peut utiliser ce renseignement à des fins d'étude, de recherche ou de statistique conformément à l'article 21 ou à une personne qui est autorisée conformément à l'article 21.1 de la LP;

- à une personne qui, en vertu de la loi, peut recouvrer des créances pour autrui et qui le requiert à cette fin dans l'exercice de ses fonctions;
- à une personne si le renseignement est nécessaire aux fins de recouvrer une créance de l'entreprise;
- à toute personne ou tout organisme susceptible de diminuer un risque suivant un incident de confidentialité impliquant un renseignement personnel, en ne lui communiquant que les renseignements personnels nécessaires à cette fin;
- à son conjoint ou à l'un de ses proches parents dans le cas d'une personne décédée si ce renseignement est susceptible d'aider cette personne dans son processus de deuil, à moins que la personne décédée n'ait consigné par écrit son refus d'accorder ce droit d'accès;
- au titulaire de l'autorité parentale ou du tuteur d'un mineur de moins de 14 ans, sauf lorsque cette collecte sera manifestement au bénéfice de ce mineur.

CONSERVATION DES RENSEIGNEMENTS PERSONNELS

La loi exige que l'organisation mette en place des règles applicables à la conservation et à la destruction des renseignements personnels.

Dossiers matériels

L'organisation documente où se retrouvent les dossiers matériels et papier contenant des informations personnelles et limite l'accès à ces dossiers aux personnes ayant besoin de disposer de ses renseignements.

Dossiers informatiques

L'organisation documente également où se retrouvent les dossiers informatiques contenant des informations personnelles et limite l'accès à ces dossiers aux personnes ayant besoin de disposer de ses renseignements. Généralement, les dossiers se retrouvent sur le réseau informatique de l'organisation.

La personne responsable des renseignements personnels de la Fondation définit à qui l'accès des différents dossiers informatiques est autorisé dans le cadre de leurs fonctions et la personne ou l'organisation qui paramètre matériellement l'accès aux différents dossiers.

Localisation du ou des serveurs informatiques

Le serveur informatique est localisé dans les locaux de l'organisation. La Fondation s'assure de limiter l'accès au local concerné aux personnes devant avoir accès aux renseignements personnels et au personnel informatique chargé de l'entretien du serveur.

Il est recommandé que :

- L'organisation se dote de mesures de sécurité encadrant l'accès aux serveurs informatiques;
- Le responsable du réseau informatique de l'organisation évalue les risques associés à l'accès aux renseignements personnels, à la sécurité du réseau et recommande toute mesure pour limiter et réduire tout accès non autorisé, notamment et sans limiter la généralité de ce qui précède, les tentatives d'intrusion externes, d'hameçonnage, etc.

DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

La Fondation Sainte-Croix/Heriot a défini les règles relatives à la destruction des renseignements personnels qu'elle détient sur un individu. Le consentement est également donné à des fins spécifiques et pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Comme les obligations d'un organisme de bienfaisance exigent de conserver les informations reliées à l'émission des reçus pour fins d'impôt de ses donateurs pour une période de minimum 6 ans, il est donc nécessaire de préserver ces renseignements personnels.

L'organisme conserve les renseignements personnels aussi longtemps que requis pour mener ses activités et sa mission, sous réserve de délais prévus à son calendrier de conservation. Lorsque sont atteintes les finalités pour lesquelles les renseignements personnels ont été collectés, ces renseignements sont détruits ou anonymisés, suivant les délais prévus au calendrier de conservation et aux règles de gestion des documents de la Fondation.

Rappelons que le consentement des donateurs et des intervenants dans le cadre des liens et transactions effectuées avec l'organisation peut être renouvelé et qu'il faut définir un mécanisme de documentation des consentements obtenus.

Les personnes pour lesquelles la Fondation détient des renseignements personnels peuvent demander en tout temps que leurs renseignements personnels soient détruits, désindexés (art 28.1 de la LP) ou anonymisés (à l'exception des informations requises précédemment figurant aux reçus d'impôt pour une période de 6 ans).

ENGAGEMENTS DE CONFIDENTIALITÉ DES INTERVENANTS AYANT ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Engagement de confidentialité de la part du personnel, d'un contractuel et des bénévoles ayant accès à des renseignements personnels

Il est désormais requis que toute personne pouvant avoir accès aux renseignements personnels d'un individu détenu par l'organisation signe un engagement de confidentialité avec l'organisation.

Dernière mise à jour : 13 septembre 2023