POLITIQUE DE GOUVERNANCE SUR LES MEILLEURES PRATIQUES VISANT À ENCADRER LA DÉTENTION DES RENSEIGNEMENTS PERSONNELS (RP) PAR L'ORGANISATION

Afin d'assurer le respect par les intervenants de la Fondation À Notre Santé de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels dans le secteur privé, aussi appelée Loi 25, nous vous proposons de valider et d'adapter au besoin les pratiques de l'organisation en la matière. La Loi 25 apporte ainsi des modifications significatives aux dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé (LP)* à laquelle les organisations à but non lucratif au Québec étaient déjà assujetties.

Nous tenons à rappeler que **les renseignements concernant les corporations de même que les coordonnées professionnelles des individus ne représentent pas des RP soumis à la Loi.**

DÉFINITION D'UN RENSEIGNEMENT PERSONNEL :

Voici ce qui constitue un renseignement personnel :

- le nom, la race, l'origine ethnique, la religion, l'état matrimonial et le niveau d'instruction;
- l'adresse électronique, les messages de courriel et l'adresse IP (protocole Internet-cookie);
- l'âge, la taille, le poids, les dossiers médicaux, le groupe sanguin, l'ADN, les empreintes digitales et la signature vocale;
- les revenus, les achats, les habitudes de consommation, les renseignements bancaires, les données sur les cartes de crédit ou de débit, les rapports de prêt ou de solvabilité et les déclarations de revenus;
- le numéro d'assurance sociale (NAS) ou d'autres numéros d'identification.

Voici donc certains éléments à considérer et à mettre en pratique pour favoriser le respect des dispositions législatives dont la plupart entreront en vigueur en septembre 2023.

Cycle de vie d'un renseignement personnel :

1. 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 également nécessaire pour pouvoir légalement utiliser les renseignements personnels qu'il transmet à l'organisation.

L'organisation doit ainsi mettre 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 devrait donc prévoir et documenter le consentement obtenu ou renouvelé.

2. Consultation et utilisation des renseignements personnels

L'organisation doit s'assurer 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.

3. Communication des renseignements

Les renseignements personnels que la Fondation À Notre Santé détient sur un individu doivent lui être transmis sur demande de sa part. Cette information doit d'ailleurs figurer au site web de la Fondation À Notre Santé.

D'ailleurs, l'article 27 de la LP prévoit le droit à la portabilité des RP 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 la Fondation À Notre Santé 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 le 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.

4. 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 doit donc documenter où se retrouvent les dossiers matériels et papier contenant des informations personnels et limiter l'accès à ces dossiers aux personnes ayant besoin de disposer de ces renseignements. Par exemple, l'organisation pourrait réunir tous les dossiers comportant des renseignements personnels et les placer dans un ou plusieurs classeurs localisés dans une pièce à accès restreint et/ou barrés avec une serrure dont les seules personnes ayant besoin de les consulter peuvent disposer de la clé.

EXEMPLE :

TYPE DE RENSEIGNEMENTS PERSONNELS	LOCALISATION DES RP	PERSONNES AYANT ACCÈS AUX RP	JUSTIFICATION DE L'ACCÈS	SÉCURITÉ DES RP
Adresses et coordonnées des donateurs à l'événement x	Classeur no. 1 dans le bureau 102 utilisé par la direction du développement	Direction générale, Direction du développement, préposée à l'émission des reçus pour fins d'impôt	Pour les fins de sollicitation, d'émission et consultation des reçus	Bureau fermé à clé en dehors des heures de bureau, classeur barré à clé à accès limité aux personnes mentionnées précédemment
Liste des participants à l'événement x et leurs coordonnées	Liste remise aux membres du comité de l'événement X	Direction du développement et membres du comité de l'événement X		Engagement de confidentialité et de destruction des listes signé par chaque membre du comité de l'événement X
Dossiers RH : CV des postulants à un poste, dossier personnel et contrat des membres du personnel, dossier d'information sur les bénévoles, etc.				

Dossiers informatiques :

L'organisation doit également documenter où se retrouvent les dossiers informatiques contenant des informations personnelles et limiter l'accès à ces dossiers aux personnes ayant besoin de disposer de ces renseignements. Généralement, les dossiers se retrouvent au réseau informatique de l'organisation.

Il faut alors définir qui autorise les permissions d'accès aux différents dossiers informatiques et qui paramètre matériellement l'accès aux différents dossiers.

Il faut ensuite effectuer l'inventaire des dossiers informatiques dans lesquels peuvent se retrouver des RP, redéfinir s'il y a lieu l'arborescence des dossiers informatiques et limiter l'accès aux dossiers informatiques dans lesquels se retrouvent des RP aux seules personnes ayant besoin d'accéder ou consulter ces informations dans le cadre de leurs fonctions.

EXEMPLE :
Personne autorisant les permissions d'accès ou les paramètres de permissions d'accès : _____ Substitut en cas d'absence :_____

Personne paramétrant les permissions d'accès :
_____ Substitut en cas d'absence :_____

TYPE DE RENSEIGNEMENTS PERSONNELS	LOCALISATION DES RP	PERSONNES AYANT ACCÈS AUX RP	JUSTIFICATION DE L'ACCÈS	SÉCURITÉ DES RP
Base de données Prodon : historique de l'ensemble des donateurs ou personnes sollicitées par l'organisation	Base de données externe ou infonuagique	Direction de l'organisation, Direction du développement, préposé à la gestion de la base de données, coordination aux communications	Historique des transactions et communications, informations sur le donateur	Sauvegarde des données chaque semaine (quand), copie disponible auprès de Logilys à ses serveurs localisés à (endroit)
Liste des participants à l'événement x et leurs coordonnées	Liste remise aux membres du comité de l'événement X	Direction du développement et membres du comité de l'événement X		Engagement de confidentialité et de destruction des listes signé par chaque membre du comité de l'événement X
Dossiers RH : CV des postulants à un poste, dossier personnel et contrat des membres du personnel, dossier d'information sur les bénévoles, etc.				
Autre				

Localisation du ou des serveurs informatiques :

Si le serveur informatique est localisé dans les locaux de l'organisation, les locaux d'une organisation à laquelle il est affilié ou d'une entreprise informatique externe, l'organisation doit s'assurer de limiter l'accès au local concerné aux personnes devant avoir accès aux RP ou au personnel informatique chargé de l'entretien du serveur.

Il serait 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 RP, 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.

La loi exige par ailleurs que l'organisation réalise une évaluation des facteurs relatifs à la vie privée (ÉFVP), notamment avant de communiquer des renseignements personnels à l'extérieur du Québec, ce qui peut survenir si les serveurs informatiques et/ou la base de données de l'organisation sont situés hors Québec. Le responsable du réseau informatique de l'organisation ou un consultant externe pourrait se voir confier cette évaluation.

5. Destruction des renseignements personnels

La Fondation À Notre Santé doit définir 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 6 ans, il est donc nécessaire de préserver ces renseignements personnels. Voici un rappel des renseignements devant se trouver au reçu pour fins d'impôt émis par un organisme de bienfaisance comportant certains renseignements personnels :

Les reçus officiels de dons émis aux fins de l'impôt sur le revenu doivent contenir les éléments suivants :

- Un énoncé précisant qu'il s'agit d'un reçu officiel aux fins de l'impôt sur le revenu;
- Le nom et l'adresse de l'organisme de bienfaisance enregistré auprès de l'Agence du revenu du Canada (ARC);
- Le numéro d'enregistrement de l'organisme de bienfaisance;
- Le numéro de série du reçu;
- Le lieu ou la région où le reçu a été remis;
- La date ou l'année où le don a été reçu;

- La date de remise du reçu si elle est différente de la date où le don a été reçu;
- Le nom et l'adresse du donateur, y compris son prénom et son initiale;
- Le montant du don;
- La valeur et la description de tout avantage reçu par le donateur;
- Le montant admissible du don;
- La signature d'une personne qui a été autorisée par l'organisme de bienfaisance à reconnaître les dons;
- Le nom et l'adresse du site Web de l'ARC.

Chaque organisme doit donc définir la durée nécessaire du consentement obtenu de ses donateurs et intervenants selon la fin pour laquelle les RP ont été obtenus. L'organisme considère qu'il conservera les RP obtenus de ses donateurs pour une durée maximale de 7 ans suivant la date de son dernier don ou son dernier consentement à l'utilisation de ses renseignements personnels, la date la plus récente ayant préséance.

Rappelons que ce consentement peut être renouvelé par les donateurs et les intervenants dans le cadre des liens et transactions effectuées avec la Fondation À Notre Santé et qu'il faut définir un mécanisme de documentation des consentements obtenus.

Les personnes pour lesquelles la Fondation À Notre Santé détient des RP 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).

6. Engagements de confidentialité des intervenants ayant accès aux RP

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

Il serait 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.

L'engagement suivant pourrait être souscrit par les intervenants de l'organisation :

« Pendant la durée de mon implication auprès de la FONDATION À NOTRE SANTÉ et suite à la fin de mon implication, auprès de la FONDATION À NOTRE SANTÉ, je m'engage et m'oblige à ne pas dévoiler ou divulguer à qui que ce soit, directement ou indirectement, tout renseignement personnel d'un individu détenu par la FONDATION À NOTRE SANTÉ et auquel je pourrais avoir accès. Un renseignement personnel représente notamment et sans limiter la généralité de ce qui précède :

- le nom, la race, l'origine ethnique, la religion, l'état matrimonial et le niveau d'instruction;
- l'adresse électronique, les messages de courriel et l'adresse IP (protocole Internet-cookie);
- l'âge, la taille, le poids, les dossiers médicaux, le groupe sanguin, l'ADN, les empreintes digitales et la signature vocale;
- les revenus, les achats, les habitudes de consommation, les renseignements bancaires, les données sur les cartes de crédit ou de débit, les rapports de prêt ou

de solvabilité et les déclarations de revenus;
- le numéro d'assurance sociale (NAS) ou d'autres numéros d'identification.

Je m'engage également à ne pas utiliser tout renseignement personnel pour des fins personnelles ou pour des fins autres que l'implication qui m'est requise par la FONDATION À NOTRE SANTÉ.

Nonobstant toute autre disposition du présent engagement, je ne serai pas en défaut ou en contravention en raison d'une divulgation de renseignement personnel, si je suis contraint par la loi de divulguer cette information pour autant que j'ai fait les meilleurs efforts pour aviser la FONDATION À NOTRE SANTÉ en temps opportun pour que la FONDATION À NOTRE SANTÉ puisse prendre les mesures appropriées afin d'empêcher cette divulgation s'il y avait lieu. »

Engagement de confidentialité de la part d'un tiers contractant ayant accès à des renseignements personnels

L'engagement suivant pourrait être souscrit par les intervenants de l'organisation (voir aussi le modèle d'accord avec un tiers) :

« Étant donné que l'organisation a décidé de confier le mandat de (description du mandat) à (nom) et que l'exécution de ce contrat nécessite le transfert et/ou l'accès par (nom), son personnel ou tout sous-traitant qu'elle mandate, à des renseignements personnels détenus par l'organisation,

Étant donné que (nom) s'engage à prendre toutes les mesures requises pour assurer la protection et la confidentialité des renseignements personnels détenus par l'organisation,

Il est convenu que le préambule fait partie intégrante du présent engagement.

Il est convenu que pendant la durée de mon contrat auprès de la FONDATION À NOTRE SANTÉ et suite à la fin de mon implication, auprès de la FONDATION À NOTRE SANTÉ, je m'engage et m'oblige à ne pas dévoiler ou divulguer à qui que ce soit, directement ou indirectement, tout renseignement personnel d'un individu détenu par la FONDATION À NOTRE SANTÉ et auquel je pourrais avoir accès. Un renseignement personnel représente notamment et sans limiter la généralité de ce qui précède :

- le nom, la race, l'origine ethnique, la religion, l'état matrimonial et le niveau d'instruction;
- l'adresse électronique, les messages de courriel et l'adresse IP (protocole Internet-cookie);
- l'âge, la taille, le poids, les dossiers médicaux, le groupe sanguin, l'ADN, les empreintes digitales et la signature vocale;
- les revenus, les achats, les habitudes de consommation, les renseignements bancaires, les données sur les cartes de crédit ou de débit, les rapports de prêt ou de solvabilité et les déclarations de revenus;
- le numéro d'assurance sociale (NAS) ou d'autres numéros d'identification.

Je m'engage également à ne pas utiliser tout renseignement personnel pour des fins personnelles ou pour des fins autres que l'implication qui m'est requise par la

FONDATION À NOTRE SANTÉ.

Nonobstant toute autre disposition du présent engagement, je ne serai pas en défaut ou en contravention en raison d'une divulgation de renseignement personnel, si je suis contraint par la loi de divulguer cette information pour autant que j'ai fait les meilleurs efforts pour aviser la FONDATION À NOTRE SANTÉ en temps opportun pour que la FONDATION À NOTRE SANTÉ puisse prendre les mesures appropriées afin d'empêcher cette divulgation s'il y avait lieu.

Par ailleurs, je m'engage à ce que tout membre de mon personnel intervenant dans le cadre de ce contrat adhère au présent engagement. Cet engagement lie toute corporation et toute personne liée à XXXX ayant accès aux renseignements personnels transmis par l'organisation.

À la fin du contrat, je m'engage à ce que les renseignements personnels transmis par l'organisation et traités par moi et mon personnel soient retournés à l'organisation et soient ensuite détruits sans copie de sauvegarde. »