Protection des renseignements personnels		
La Loi 25 modifie principalement la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé*.		
Vérification	**Oui/Non**	**À planifier/ Responsable.s**
Politique Avez-vous une politique sur la protection des renseignements personnels? Et est-ce que votre politique est adaptée à la réalité de votre organisation?		
Le responsable a été désigné et s'est adjoint d'une équipe au besoin Souvent la direction générale est la mieux placée pour être imputable, mais elle peut quand même solliciter de l'aide de ses employés en fonction de leurs aptitudes particulières ou de leur poste qui peuvent être centraux.		
Communication de la politique et sensibilisation du personnel Est-ce que la politique a été présentée et expliquée aux employés et aux bénévoles et est facilement accessible? Il est important de sensibiliser les employés et les bénévoles qu'une erreur (même faite de bonne foi) pourrait coûter très cher à l'organisation ainsi que causer un préjudice aux personnes concernées. **Source** : https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/sanctions-entreprises-poursuites		
Formation Est-ce que la personne responsable et les autres employés de l'entreprise ont suivi une formation en matière de protection des renseignements personnels qui est pertinente à l'exercice de leurs fonctions?		
Télétravail Les employés doivent être sensibilisés à l'importance de ne pas laisser trainer des dossiers clients dans leur salon par exemple. Il faut également faire attention à l'utilisation d'un ordinateur personnel pour des fins professionnelles (et vice versa). Utilisation d'un VPN pour se protéger? Les employés doivent être avisés qu'il peut y avoir des conséquences disciplinaires à ne pas respecter les directives de l'entreprise en matière de protection des renseignements personnels pouvant aller jusqu'au congédiement en cas de non-respect selon votre politique interne.		
Qui a accès à quoi? Seules les personnes qui ont besoin de traiter des renseignements personnels en question dans le cadre de leur travail devraient y avoir accès. Chaque accès doit être justifié par le poste et les responsabilités.		
Avez-vous un moyen de répertorier TOUS les renseignements personnels que vous détenez? Cela vaut autant à l'égard de vos membres, employés, clients, bénévoles, utilisateurs, donateurs, conseil d'administration.		

Il serait idéal d'avoir un **fichier maitre** qui vous permet d'avoir une cartographie d'où tout se trouve et ensuite, vous pourrez vérifier si vous mettez en place les mesures requises pour maximiser la protection des renseignements personnels. Cela permet d'éviter les pertes, oublis et doublons.		
Liste de tous les appareils ayant accès au réseau Parfois, on perd le fil de tous les gens qui ont accès à nos documents. Il est important de responsabiliser les personnes détenant le matériel informatique de l'organisation. Il sera également plus facile de retracer qui était fautif en cas de fuite par exemple.		
Fournisseurs Votre entente avec eux comprend-elle un engagement à la confidentialité des renseignements personnels?		
Protocole RH Avez-vous un protocole qui fait état des accès à retirer lors du départ d'un employé?		
Plan de communication Le conseil d'administration est-il avisé de ce qu'il se passe? Ceci vaut autant pour ce qui est des incidents que des mesures de protection prises pour protéger les renseignements personnels que pour leur compréhension de leurs obligations en la matière.		
Utilisation du courriel La règle à retenir pour préserver la confidentialité et respecter la loi sur la protection des renseignements personnels en lien avec l'envoi de courriel est : *« Si vous envoyez un courriel à la mauvaise personne, est-ce que cette personne a accès à des informations confidentielles ou des données personnelles? »* Par exemple : Vous pouvez ne pas utiliser les noms, vous pouvez utiliser seulement des initiales. Si le risque est présent d'identifier la personne avec les initiales, vous pouvez utiliser un PDF avec mot de passe et le mot de passe est envoyé dans un autre courriel ou par un autre moyen tel qu'un texto ou donné verbalement. Ou vous pouvez procéder à la création d'un dossier partagé dans OneDrive qui autorise que les personnes dont vous avez inscrit le courriel dans OneDrive à accéder au contenu.		
Calendrier de conservation Savez-vous pendant combien de temps que vous devez détenir tous les renseignements personnels en votre possession? Un calendrier ou un guide de conservation des renseignements personnels vous permettrait de surveiller ce qui n'est plus utile/pertinent/requis de conserver dans vos fichiers inutilement.		
Accès aux données personnelles par les personnes concernées. Si quelqu'un souhaite avoir une copie des renseignements personnels qui le concerne, pouvez-vous les fournir de façon adéquate et sécuritaire?		

Fréquence de changement des mots de passe Chaque mois, chaque trimestre, chaque six mois, jamais? Il est idéal de planifier un délai ou les mots de passe peuvent être renouvelés.		
Révision des formulaires Tout document devant être rempli pour pouvoir avoir accès à vos biens/services devrait être conforme à la loi et aux bonnes pratiques. Par exemple, sur un formulaire de prise de référence pour du recrutement, le genre « Homme ou femme » n'est pas un renseignement nécessaire.		
Registre d'incidents de confidentialité Avez-vous un document (Word, Excel ou autre) pour vous permettre de noter les incidents qui inclut? ▪ La date à laquelle a eu lieu l'incident; ▪ Le contexte de l'incident; ▪ Les renseignements personnels concernés par l'incident; ▪ La date à laquelle l'organisation a pris connaissance de l'incident; ▪ Le nombre de personnes concernées par l'incident; ▪ Le niveau du préjudice : faible, moyen ou sérieux; ▪ Est-ce que les personnes qui doivent être avisées l'ont été (C.A., responsable de la loi 25, RH …)? ▪ Les mesures prises par l'entreprise après l'incident : Politique, clarification de la politique, Rencontre, mesures de soutien, mesure disciplinaire, travail sur une meilleure communication de la politique, etc… **Exemple de bris de confidentialité :** envoyer un courriel avec plusieurs personnes en copie conforme. Puisque leur adresse courriel personnelle est visible, il s'agit d'une communication non autorisée par la *Loi sur la protection des renseignements personnels dans le secteur privé* parce que les personnes n'ont pas donné leur accord pour partager leur adresse courriel à un tiers. **Dans le cas d'un préjudice sérieux –** la personne responsable devra communiquer l'incident en question aux personnes concernées ainsi qu'à la Commission d'accès à l'information du Québec. Exemple : Informations qui peuvent permettre un vol d'identité.		
Plan de sauvegarde en cas de sinistre? Si vos locaux passent au feu, est-ce que vos dossiers ont des copies de sauvegarde dans un autre endroit (physique ou numérique) qui n'est pas affecté par le feu et qui est sécuritaire pour les données?		
Prestataire de services infonuagiques & transmission de renseignements personnels hors Québec Est-ce que les clauses au contrat assurent une protection adéquate des renseignements personnels hébergés? Avez-vous procédé à une évaluation des facteurs relatifs à la vie privée (ÉFVP) avant de communiquer les renseignements personnels/signer le contrat? Avez-vous vérifié la législation applicable dans la juridiction du fournisseur?		
Données biométriques collectées? Si oui, assurez-vous de respecter les obligations particulières en la matière.		

Authentification multifactorielle Lorsque des gens peuvent créer un profil sur votre site web ou procéder à un achat, avez-vous mis en place une façon de valider leur identité et prévenir la fraude?		
Avez-vous une couverture d'assurance en cas d'incident de confidentialité? Les frais de consultation, pertes de revenus et compensation du préjudice causé aux tiers devraient être considérés.		
Caméras de surveillance? Après combien de temps les images sont supprimées? L'utilisation est-elle justifiée?		
Soutien TI et juridique? Que ce soit pour désindexer des liens relatifs à l'existence d'une personne, obtenir des conseils en cas de questions ou incidents de confidentialité, ou pour assurer un audit de vos systèmes de cybersécurité, vous pourriez vous adjoindre d'experts dans le domaine.		