L'ASSOCIATION DES BARREAUX DE PROVINCE

Loi sur la protection des renseignements personnels dans le secteur privé

(Informations extraites de la Loi et/ou recueillies auprès de la Commission d'accès à l'information et du Barreau du Québec)

Ce document n'est qu'un résumé et n'a pas de valeur légale

1ère phase : Mise en œuvre depuis ***septembre 2022***

1) Personne Responsable

Désigner une personne responsable de la protection des renseignements personnels; Par défaut, la loi désigne la personne ayant la plus haute autorité dans l'entreprise.

- publier le titre et les coordonnées du responsable sur le site Internet de l'entreprise,

ou, si elle n'a pas de site internet :

- les rendre accessibles par tout autre moyen approprié.

2) En cas d'incident de confidentialité impliquant un renseignement personnel :

a. prendre les **mesures raisonnables** pour **diminuer les risques** qu'un préjudice soit causé aux personnes concernées et éviter que de nouveaux incidents de même nature ne se produisent;

b. **aviser la Commission** et la **personne concernée** si l'incident **présente un risque de préjudice sérieux**;

c. **tenir un registre des incidents** dont une copie devra être transmise à la Commission à sa demande;

2ième phase : *Mise en œuvre le 22 septembre 2023*

1) **Politiques et des pratiques de l'entreprise**

   Avoir établi des **politiques et des pratiques encadrant la gouvernance** des renseignements personnels;

   - Publier de l'information détaillée sur celles-ci en **termes simples et clairs** sur le site Internet de l'entreprise

     ou,

   - si elle n'a pas de site internet, par tout autre moyen approprié;

2) Réaliser une **évaluation des facteurs relatifs à la vie privée** (ÉFVP) lorsque la Loi l'exige, par exemple avant de communiquer des renseignements personnels à l'extérieur du Québec;

3) **Détruire** les renseignements personnels lorsque la finalité de leur collecte est accomplie, ou les **anonymiser** pour les utiliser à des fins sérieuses et légitimes, sous réserve des conditions et d'un délai de conservation prévus par une loi;

4) Respecter les nouvelles règles de communication des renseignements personnels à l'extérieur du Québec;

5) Prévoir, par défaut, les **paramètres assurant le plus haut niveau de confidentialité** du produit ou du service technologique offert au public;

6) Respecter les nouvelles règles entourant la collecte de renseignements personnels concernant un mineur;

7) Respecter les nouvelles règles de communication des renseignements personnels facilitant le processus de deuil.

Barreau du Québec

LISTE DE CONTRÔLE

LISTE DE CONTRÔLE

Principe	Contrôle	Disposition
Gouvernance		
Personne responsable de la protection des renseignements personnels (ou « responsable de la PRP »)	Tout cabinet d'avocats doit nommer un responsable de la PRP. Ce rôle revient par défaut à la personne ayant la plus haute autorité au sein du cabinet. ☐ Établir une description des rôles et des responsabilités du responsable de la PRP. ☐ Si nécessaire, désigner par écrit une personne à titre de responsable de la PRP. ☐ Publier les coordonnées du responsable de la PRP sur le site Web du cabinet.	Art. 3.1 de la *Loi sur le privé*
Règles de gouvernance à l'égard des renseignements personnels	Tout cabinet d'avocats doit avoir des politiques et des pratiques en matière de gouvernance et de protection des renseignements personnels. ☐ S'assurer que les politiques et pratiques respectent les obligations des membres en matière de secret professionnel, de confidentialité et de conservation, eu égard à la réglementation déontologique et des normes professionnelles. ☐ Adopter des politiques et pratiques prévoyant l'encadrement applicable à : **2.** la collecte, l'utilisation, le transfert, la conservation et la destruction des renseignements personnels ; **3.** les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels (de la collecte à la destruction) ; **4.** un processus de traitement des plaintes relatives à la protection des renseignements personnels ; **5.** la gestion des témoins de connexion (*cookies*).	Art. 3.2 (1) de la *Loi sur le privé*

Principe	Contrôle	Disposition
Gouvernance		
	☐ Publier des informations détaillées au sujet de ces politiques, en termes simples et clairs, sur le site Web du cabinet. ☐ Mettre à jour ou établir les politiques et procédures suivantes : **3.** politique de conservation et de destruction des données et calendrier de conservation (pour plus d'information sur les normes de gestion documentaire, consulter la ressource Conservation, destruction et numérisation de dossiers) ; **4.** directives et procédures relatives à la réception et au traitement de plaintes et de demandes des personnes concernées souhaitant exercer leurs droits ; **5.** politiques et procédures relatives à la sécurité de l'information ; **6.** politique de gestion des incidents de confidentialité et processus de réponse aux incidents.	
Consentement		
Formulaires de consentement	La *Loi 25* introduit certaines précisions par rapport à la forme et aux critères de validité du consentement. ☐ Effectuer une cartographie (*data mapping*) des renseignements personnels recueillis (clients et employés) afin de déterminer ceux qui sont de nature sensible, ceux appartenant à des mineurs, le cas échéant, et ceux qui sont exclus du champ d'application de la *Loi sur le privé* (p. ex. : les coordonnées d'affaires). ☐ Effectuer un inventaire des formulaires de consentement ou autres documents utilisés pour obtenir le consentement des individus concernés (clients ou employés) et les réviser afin de s'assurer que les consentements obtenus respectent les nouvelles exigences de la *Loi sur le privé*. Les éléments suivants doivent notamment s'y retrouver : • fins auxquelles les renseignements personnels sont collectés et moyens par lesquels ils sont collectés; • droits d'accès, de rectification et de retrait du consentement ; • le cas échéant : • nom du tiers pour qui la collecte est faite ; • catégories des fournisseurs de services ayant accès aux renseignements personnels ; • transfert des renseignements à l'extérieur du Québec. ☐ S'assurer qu'un consentement explicite est obtenu des individus concernés lorsque des renseignements personnels sensibles sont collectés.	Arts. 6, 8, 12, 13, 14, 15 et 18 de la *Loi sur le privé*

Principe	Contrôle	Disposition
Fournisseurs de services		
Ententes écrites	La *Loi 25* exige que le traitement des renseignements personnels par un fournisseur de services soit sujet à un contrat écrit devant comprendre les mesures que le fournisseur de services doit prendre pour assurer la protection du caractère confidentiel du renseignement personnel communiqué et pour que ce renseignement ne soit utilisé que dans le cadre de l'exécution du contrat. ☐ Recenser les fournisseurs de services traitant des renseignements personnels pour le cabinet d'avocats et déterminer si un contrat écrit conforme aux exigences légales a bien été conclu avec chacun d'eux. • Il est recommandé de faire faire affaire avec un fournisseur de services québécois qui héberge les données au Québec. • Si le fournisseur de services se trouve en dehors du Québec, il se pourrait que vous ayez à effectuer une évaluation des facteurs relatifs à la vie (« **EFVP** ») relative au transfert des données. Voir la section au sujet des EFVP ici-bas. ☐ Si nécessaire, mettre à jour les contrats existants et préparer un modèle de clauses de traitement des renseignements personnels contenant les éléments prévus par la loi.	Art. 18.3 de la *Loi sur le privé*
Transferts hors Québec		
Évaluation des facteurs relatifs à la vie privée	Toute personne qui souhaite communiquer des renseignements personnels à l'extérieur du Québec ou confier à un tiers situé à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte des renseignements personnels est tenue d'effectuer une EFVP. Pour plus d'information sur les responsabilités et obligations des entreprises, nous vous invitons à consulter l'Aide-mémoire sur les nouvelles responsabilités des entreprises, les pistes d'action et les bonnes pratiques développé par la Commission d'accès à l'information (« **CAI** »). ☐ Déterminer si des renseignements personnels détenus par le cabinet sont transférés en dehors du Québec (incluant lorsque les fournisseurs de service du cabinet font affaire avec des sous-traitants situés dans d'autres juridictions que le Québec) ; ☐ Le cas échéant, développer ou adopter un modèle d'EFVP qui tient compte des facteurs suivants : • la sensibilité des renseignements ; • la finalité de leur utilisation ; • les mesures de protection, y compris contractuelles, qui s'y appliqueront, et ; • le régime juridique applicable dans l'État de réception, notamment les principes de protection des renseignements personnels qui y sont applicables. ☐ Le cas échéant, mener une EFVP pour les activités de traitement impliquant la communication de renseignements personnels en dehors du Québec. ☐ Adapter le modèle de clauses contractuelles relatives au traitement des renseignements personnels pour prendre en compte les exigences liées aux fournisseurs de services situés hors du Québec.	Art. 17 de la *Loi sur le privé*

Principe	Contrôle	Disposition
Employés		
Politique de confidentialité	☐ Adopter ou mettre à jour une politique de confidentialité visant les employés du cabinet. ☐ Réviser les modèles de contrats de travail existants pour les employés du cabinet, notamment les clauses de confidentialité, afin de tenir compte des nouvelles exigences en matière de protection de la vie privée.	Art. 10 de la *Loi sur le privé*
Sensibilisation et formation	☐ Développer un programme de formation sur les règles relatives à la protection des renseignements personnels pour les employés qui traitent ou qui ont accès à des renseignements personnels. ☐ Organiser des séances de formation annuelles sur les meilleures pratiques en matière de cybersécurité et de protection des données pour tous les membres du personnel du cabinet.	Art. 10 de la *Loi sur le privé*
Cybersécurité		
Mesures de sécurité	Les cabinets d'avocats ont une obligation générale de prendre les mesures de sécurité appropriées et raisonnables pour protéger les renseignements personnels qu'ils détiennent. ☐ Mettre à jour le plan de réponse aux incidents de sécurité du cabinet et faire tester et approuver ce plan par des experts en cybersécurité. ☐ Revoir la police d'assurance responsabilité du cabinet pour déterminer si les incidents de sécurité sont couverts. À défaut, souscrire à une police d'assurance couvrant ces risques. • Rappelons que les cyberrisques ne sont pas couverts par la police émise par le FARPBQ (*Praeventio*, février 2022). Vous pouvez consulter la police d'assurance responsabilité professionnelle sur le site Web du FARPBQ. ☐ Élaborer un programme de formation à la cybersécurité à l'intention des membres du cabinet.	Art. 10 de la *Loi sur le privé*
Incidents de confidentialité	La *Loi 25* rend obligatoire la notification d'incidents de confidentialité à la CAI si le cabinet détermine que l'incident présente un risque de préjudice sérieux pour les individus concernés. ☐ Établir une grille ou un document similaire qui fournira les critères permettant de déterminer si un incident de confidentialité présente un risque de préjudice sérieux pour les personnes concernées, auquel cas il devra être notifié à la CAI et aux personnes concernées par l'incident. Les facteurs à considérer sont : • la sensibilité des renseignements en cause ; • les conséquences appréhendées de leur utilisation, et ; • la probabilité qu'ils soient utilisés à des fins préjudiciables. ☐ Créer un registre pour le cabinet de tout incident de confidentialité, et ce, même s'il ne comporte pas de risque de préjudice sérieux. • Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident ; • Le registre doit être communiqué à la CAI sur demande.	Arts. 3.5 à 3.8 de la *Loi sur le privé* Voir aussi le *Règlement sur le incidents de confidentialité*

Principe	Contrôle	Disposition
Autres		
Technologie d'identification, de localisation et de profilage	La *Loi 25* prévoit que lorsqu'une entreprise collecte des informations personnelles à l'aide d'une technologie incluant des fonctionnalités d'identification, de localisation ou de profilage d'un individu, elle doit informer préalablement cet individu de l'utilisation de cette technologie et des moyens disponibles pour activer ces fonctions. ☐ Déterminer si le cabinet recueille des renseignements personnels en utilisant des technologies ayant des fonctions permettant de profiler, de localiser ou d'identifier un individu (p. ex. : par l'entremise de témoins de connexion sur le site Web du cabinet). ☐ Le cas échéant, s'assurer que les individus sont informés, au moment de la collecte, de l'utilisation de la technologie et des moyens d'activer la fonction.	Art. 8.1 de la *Loi sur le privé*
Confidentialité par défaut	La *Loi 25* stipule que les entreprises qui collectent des informations personnelles en offrant au public un produit ou un service technologique doté de paramètres de confidentialité doivent garantir que ces paramètres par défaut offrent le niveau de confidentialité le plus élevé possible, sans que l'utilisateur ait à intervenir. Cette exigence ne s'applique pas aux témoins de connexion. ☐ Déterminer si le cabinet a des produits ou services technologiques offerts au public qui recueillent des renseignements personnels et qui disposent de paramètres de confidentialité. ☐ Le cas échéant, s'assurer que les paramètres de confidentialité de ces produits ou services sont ajustés pour être conformes à la nouvelle exigence de confidentialité par défaut.	Art. 9.1 de la *Loi sur le privé*

Biométrie	La *Loi 25* rend obligatoire la notification d'incidents de confidentialité à la CAI, si le cabinet détermine que l'incident présente un risque de préjudice sérieux pour les individus concernés. ☐ Si nécessaire, établir des lignes directrices internes sur l'utilisation des systèmes biométriques en tenant compte des nouvelles exigences en matière de protection de la vie privée. ☐ Établir un modèle d'évaluation des incidences sur la vie privée pour tout projet futur impliquant des données biométriques.	Arts. 44 et 45 de la *Loi concernant le cadre juridique des technologies de l'information*