Guide pratique
pour la protection des renseignements personnels par l'avocat et son équipe

Loi sur la protection des renseignements personnels dans le secteur privé

Barreau du Québec

CONTEXTE

La pratique du droit peut poser des défis uniques en matière de protection des renseignements personnels. En plus d'assumer leur rôle de conseiller juridique, les avocats et les avocates travaillant notamment en solo, en cabinet ou en entreprise peuvent aussi agir comme gestionnaires d'entreprise et, par ce fait même, comme responsables de la protection et de la sécurité des données sans nécessairement avoir accès à des ressources spécialisées ou à une expertise technique dans le domaine.

Or, la protection des renseignements personnels prend de plus en plus d'importance pour tous les clients et les clientes. Ainsi, les avocats et les avocates doivent s'adapter pour répondre à ces exigences. Cela est d'autant plus vrai au Québec alors que la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ c. P-39.1) (ci-après la « ***Loi sur le secteur privé*** ») applicable aux cabinets d'avocats prévoit des obligations notamment en ce qui a trait à la cueillette, à l'utilisation et à la communication de renseignements personnels.

Le Barreau du Québec propose ce guide pratique qui vise à sensibiliser les avocats et les avocates aux obligations en matière de protection des renseignements personnels au Québec et à leur fournir des conseils pratiques pour s'y conformer. À cet effet, chaque thème comporte des actions simples que peuvent accomplir tous les avocats et les avocates pour les aider à ce que leur pratique soit conforme aux nouvelles exigences de la *Loi sur le secteur privé*.

TEST ÉCLAIR DE CONFORMITÉ

Répondez aux questions suivantes au meilleur de vos connaissances. Si vous répondez NON ou si vous ignorez la réponse, consultez la liste de contrôle ci-dessous.

	Dans votre cabinet ou votre organisation…	**Oui**	**Non**	**Ne sais pas**	**Pour plus d'information**
1.	Avez-vous nommé un ou une responsable de la protection des renseignements personnels ?				Responsable de la protection des renseignements personnels
2.	Avez-vous publié une politique de confidentialité sur votre site Internet ?				Gouvernance
3.	Avez-vous publié des conditions d'utilisation sur votre site Internet relativement aux services que vous offrez ?				Gouvernance
4.	Avez-vous adopté une politique de conservation des données de vos client(e)s et/ou de vos employé(e)s ?				Gouvernance
5.	Avez-vous des politiques ou des procédures existantes pour le traitement des demandes de client(e)s ou d'employé(e)s relatives aux données ?				Règles de gouvernance à l'égard des renseignements personnels

---

Ce document a été préparé en collaboration avec Me Antoine Guilmain.

6.	Avez-vous mis en place une procédure pour l'évaluation des facteurs relatifs à la vie privée (EFVP) ?				Évaluation des facteurs relatifs à la vie privée
7.	Avez-vous communiqué avec vos fournisseurs de services qui traitent des renseignements personnels (p. ex. : hébergement de données) afin de vous assurer que ceux-ci, notamment ceux se trouvant en dehors du Québec, sont conformes aux exigences de la *Loi sur le secteur privé* ?				Fournisseurs de services
8.	Avez-vous révisé vos formulaires de consentement pour vous assurer qu'ils sont conformes aux exigences de la *Loi sur le secteur privé* ?				Consentement
9.	Avez-vous mis en place une procédure en cas d'incident de sécurité ?				Mesures de sécurité
10.	Avez-vous mis en place une procédure à suivre en cas d'incident de confidentialité ?				Incidents de confidentialité
11.	Avez-vous révisé votre assurance responsabilité civile pour vous assurer qu'elle couvre vos dommages et les dommages de vos clients et clientes qui découlent des incidents de sécurité ?				Cybersécurité
12.	Avez-vous créé un registre pour les incidents de confidentialité ?				Cybersécurité

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 Internet du cabinet.	Art. 3.1 de la *Loi sur le secteur 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 : • la collecte, l'utilisation, le transfert, la conservation et la destruction des renseignements personnels ; • la collecte de renseignements personnels concernant un mineur (le cas échéant) ; • 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) ; • un processus de traitement des plaintes relatives à la protection des renseignements personnels ; • la gestion des témoins de connexion (*cookies*).	Art. 3.2 de la *Loi sur le secteur privé* Pour plus d'information, voir le guide de la CAI : *Guide explicatif pour les entreprises : rédiger une politique de confidentialité.*

Principe	Contrôle	Disposition
Gouvernance		
	☐ Publier des informations détaillées au sujet de ces politiques, en termes simples et clairs, sur le site Internet du cabinet. ☐ Mettre à jour ou établir les politiques et procédures suivantes : • 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) ; • directives et procédures relatives à la réception et au traitement de plaintes et de demandes des personnes concernées souhaitant exercer leurs droits ; • politiques et procédures relatives à la sécurité de l'information ; • politique de gestion des incidents de confidentialité et processus de réponse aux incidents.	
Consentement		
Formulaires de consentement	La *Loi sur le secteur privé* prévoit certaines exigences concernant la forme et les 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 de certaines parties de la *Loi sur le secteur 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 exigences de la *Loi sur le secteur 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 secteur privé*

Portabilité des données	La *Loi sur le secteur privé* reconnaît le droit d'obtenir et de transférer des renseignements personnels d'une organisation à une autre dans un format structuré et couramment utilisé (droit à la portabilité des données). Ces renseignements doivent être communiqués sous la forme d'une transcription écrite et intelligible. ☐ Déterminer si votre cabinet collecte des renseignements personnels informatisés auprès d'individus, qui pourraient faire l'objet d'une demande de portabilité. ☐ Le cas échéant, établir une procédure permettant au cabinet de recevoir les demandes de portabilité et y répondre en fournissant, sur demande, des renseignements personnels informatisés à un individu, à une personne ou une entreprise autorisée par la loi à recueillir de tels renseignements, dans un format technologique structuré et couramment utilisé ; il faut également tenir compte des règles propres au transfert de dossiers clients en vertu des règles déontologiques.	Art. 27 de la *Loi sur le secteur privé*
Principe	**Contrôle**	**Disposition**
Fournisseurs de services		
Ententes écrites	La *Loi sur le secteur privé* 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 secteur 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 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 secteur privé* Pour plus d'information, voir le guide de la CAI sur les EFVP : *Réaliser une évaluation des facteurs relatifs à la vie privée.*
Principe	**Contrôle**	**Disposition**
Employés		
Politique de protection des renseignements personnels	☐ Adopter ou mettre à jour une politique de protection des renseignements personnels 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 exigences en matière de protection de la vie privée.	Arts. 3.2 et 10 de la *Loi sur le secteur 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 secteur 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, évaluer 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 Internet du FARPBQ. ☐ Élaborer un programme de formation à la cybersécurité à l'intention des membres du cabinet.	Art. 10 de la *Loi sur le secteur privé*
Incidents de confidentialité	La *Loi sur le secteur privé* 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 secteur privé* Voir aussi le *Règlement sur les incidents de confidentialité*
Principe	**Contrôle**	**Disposition**
Autres		
Technologie d'identification, de localisation et de profilage	La *Loi sur le secteur privé* prévoit que lorsqu'une entreprise collecte des renseignements personnels 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 Internet 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 secteur privé*

Confidentialité par défaut	La *Loi sur le secteur privé* prévoit que les entreprises qui collectent des renseignements personnels 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 l'exigence de confidentialité par défaut.	Art. 9.1 de la *Loi sur le secteur privé*
Biométrie	En vertu du droit québécois, toute organisation voulant utiliser un système biométrique ou un procédé permettant de saisir des caractéristiques ou des mesures biométriques pour vérifier ou confirmer l'identité d'une ou de plusieurs personnes doit préalablement en notifier la CAI. Si une entreprise veut créer une banque de caractéristiques ou de mesures biométriques, une déclaration doit être faite à la CAI au moins 60 jours avant la mise en service de la banque. La CAI rend disponible un formulaire de déclaration à cet effet sur son site Internet (disponible ici). ☐ Déterminer si votre cabinet utilise ou a l'intention de mettre en place un système (ou procédé) biométrique pour vérifier ou confirmer l'identité de personnes. ☐ Le cas échéant, remplir et transmettre le formulaire de la CAI à cet effet. ☐ Si nécessaire, établir des lignes directrices internes sur l'utilisation des systèmes biométriques en tenant compte des exigences en matière de protection des données.	Arts. 44 et 45 de la *Loi concernant le cadre juridique des technologies de l'information* Pour plus d'information, voir le guide de la CAI sur la biométrie : *Biométrie : principes à respecter et obligations légales des organisations.*