

Protection des renseignements personnels par l'avocat et son équipe

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 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 en matière de cybersécurité.

Or, la protection des renseignements personnels prend de plus en plus d'importance pour les clients. Ainsi, les avocats 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) (« **Loi sur le privé** ») applicable aux cabinets d'avocats a récemment été modifiée de manière importante par la [Loi modernisant des dispositions législatives en matière de protection des renseignements personnels](#) (LQ 2021, c. 25), aussi connue sous le nom de projet de loi 64 ou **Loi 25**.

Le Barreau du Québec propose cet aide-mémoire qui vise à sensibiliser les avocats aux nouvelles 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 pour que leur pratique soit conforme aux nouvelles exigences de la *Loi sur le privé*. Cet outil s'ajoute au [Guide des TI - Gestion et sécurité des technologies de l'information pour l'avocat et son équipe](#) disponible sur le site Web du Barreau du Québec.

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 Web?				Gouvernance
3.	Avez-vous publié des conditions d'utilisation sur votre site Web relativement aux services que vous offrez?				Gouvernance
4.	Avez-vous adopté une politique de conservation des données de vos clients et/ou de vos employés?				Gouvernance
5.	Avez-vous des politiques ou des procédures existantes pour le traitement des demandes de clients ou d'employés relatives à la vie privée?				Règles de gouvernance à l'égard des renseignements personnels

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 nouvelles exigences de la <i>Loi sur le privé</i> ?				Fournisseurs de services
8.	Avez-vous révisé vos formulaires de consentement pour vous assurer qu'ils sont conformes aux nouvelles exigences de la <i>Loi sur le privé</i> ?				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 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 »)	<p>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.</p> <p><input type="checkbox"/> Établir une description des rôles et des responsabilités du responsable de la PRP.</p> <p><input type="checkbox"/> Si nécessaire, désigner par écrit une personne à titre de responsable de la PRP.</p> <p><input type="checkbox"/> Publier les coordonnées du responsable de la PRP sur le site Web du cabinet.</p>	Art. 3.1 de la Loi sur le privé
Règles de gouvernance à l'égard des renseignements personnels	<p>Tout cabinet d'avocats doit avoir des politiques et des pratiques en matière de gouvernance et de protection des renseignements personnels.</p> <p><input type="checkbox"/> 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.</p> <p><input type="checkbox"/> Adopter des politiques et pratiques prévoyant l'encadrement applicable à :</p> <ul style="list-style-type: none"> • la collecte, l'utilisation, le transfert, la conservation et la destruction des renseignements personnels; • 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 (<i>cookies</i>). 	Art. 3.2 (1) de la Loi sur le privé

Principe	Contrôle	Disposition
Gouvernance		
	<input type="checkbox"/> Publier des informations détaillées au sujet de ces politiques, en termes simples et clairs, sur le site Web du cabinet. <input type="checkbox"/> Mettre à jour ou établir les politiques et procédures suivantes : <ul style="list-style-type: none"> • 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	<p>La <i>Loi 25</i> introduit certaines précisions par rapport à la forme et aux critères de validité du consentement.</p> <input type="checkbox"/> Effectuer une cartographie (<i>data mapping</i>) 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 <i>Loi sur le privé</i> (p. ex. : les coordonnées d'affaires). <input type="checkbox"/> 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 <i>Loi sur le privé</i> . Les éléments suivants doivent notamment s'y retrouver : <ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • 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. <input type="checkbox"/> 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	<p>La <i>Loi 25</i> 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.</p> <p><input type="checkbox"/> 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.</p> <ul style="list-style-type: none"> • Il est recommandé de 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. <p><input type="checkbox"/> 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.</p>	Art. 18.3 de la Loi sur le privé
Transferts hors Québec		
Évaluation des facteurs relatifs à la vie privée	<p>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.</p> <p>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»).</p> <p><input type="checkbox"/> 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);</p> <p><input type="checkbox"/> Le cas échéant, développer ou adopter un modèle d'EFVP qui tient compte des facteurs suivants :</p> <ul style="list-style-type: none"> • 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. <p><input type="checkbox"/> Le cas échéant, mener une EFVP pour les activités de traitement impliquant la communication de renseignements personnels en dehors du Québec.</p> <p><input type="checkbox"/> 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.</p>	Art. 17 de la Loi sur le privé

Principe	Contrôle	Disposition
Employés		
Politique de confidentialité	<input type="checkbox"/> Adopter ou mettre à jour une politique de confidentialité visant les employés du cabinet. <input type="checkbox"/> 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	<input type="checkbox"/> 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. <input type="checkbox"/> 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	<p>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.</p> <input type="checkbox"/> 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. <input type="checkbox"/> 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. <ul style="list-style-type: none"> • 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. <input type="checkbox"/> 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	<p>La <i>Loi 25</i> 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.</p> <input type="checkbox"/> 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 : <ul style="list-style-type: none"> • la sensibilité des renseignements en cause; • les conséquences appréhendées de leur utilisation, et; • la probabilité qu'ils soient utilisés à des fins préjudiciables. <input type="checkbox"/> Créer un registre pour le cabinet de tout incident de confidentialité, et ce, même s'il ne comporte pas de risque de préjudice sérieux. <ul style="list-style-type: none"> • 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 les incidents de confidentialité

Principe	Contrôle	Disposition
Autres		
Technologie d'identification, de localisation et de profilage	<p>La <i>Loi 25</i> 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.</p> <ul style="list-style-type: none"> <input type="checkbox"/> 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). <input type="checkbox"/> 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	<p>La <i>Loi 25</i> 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.</p> <ul style="list-style-type: none"> <input type="checkbox"/> 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. <input type="checkbox"/> 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	<p>La <i>Loi 25</i> 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.</p> <ul style="list-style-type: none"> <input type="checkbox"/> 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. <input type="checkbox"/> 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