Politique de Neolegal Inc. sur la protection des renseignements personnels

La présente politique est élaborée afin de se conformer à *la Loi sur la protection des renseignements personnels* ainsi que de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Dans le cadre des services rendus par Neolegal Inc., nous sommes tenus de recueillir des renseignements personnels de nos Client(e)s que nous nous engageons à protéger.

Neolegal s'engage à remettre au client, à sa demande, une copie de toutes ses informations confidentielles recueillies par l'entreprise dans un format lisible par des logiciels d'usage courant.

Neolegal Inc. consent à agir au nom du Client(e) exclusivement aux fins de la fourniture de Services précédemment limités par le programme (forfait) spécifique souscrit.

Neolegal Inc. déclare être lié en son nom et en celui des avocats qui le compose par le *Code de déontologie des avocats*, les règles du Barreau du Québec, et par toutes les autres lois ou règlements trouvant à s'appliquer dans la relation contractuelle présente.

Neolegal Inc. en son nom et en celui de ses représentants s'engage à agir avec loyauté et en toute transparence, dans l'intérêt de son Client(e) et en accord avec les coutumes et usages de la profession d'avocat.

En cas de souscription d'un Service, Neolegal Inc. conservera le dossier des Client(e)s selon ses règles internes et de concert avec les lois en place, ainsi que toutes les informations transmises, dans ses serveurs tel qu'utilisés à l'interne et ce tout le long de la relation contractuelle entre les Parties.

Neolegal Inc. s'engage à demander le consentement express à la collecte de tous renseignements personnels des Clients. Tous les renseignements ainsi obtenus ne pourront être utilisés ou communiquer sans ledit consentement express des Clients.

Neolegal Inc. ne détiendra ou ne demandera pas de document original de la part des Client(e)s. Le ou la Client(e) est responsable de l'ensemble des documents originaux qui compose son dossier juridique.

Neolegal Inc. s'engage à respecter la nature privée et confidentielle de tous les renseignements personnels des Client(e)s. Toutes les conversations entre le ou la Client(e) et un(e) représentant(e) de Neolegal Inc. peut être enregistrée pour fins de contrôle qualité et afin de répondre au Code de déontologie des avocats. Les conversations sont conservées de manière hautement sécuritaire et seul les personnes autorisées de Neolegal Inc. peuvent y avoir accès.

Neolegal Inc. ne conserve aucun renseignement lié au paiement de ses client(e)s, ainsi que les données nécessaires à l'achat. Ces données sont encryptées et détruites après l'utilisation selon les normes édictées en ce sens.

Neolegal Inc. s'assure aussi que ses fournisseurs de paiement respectent eux aussi les plus hauts standards de l'industrie.

Neolegal Inc. se doit de recueillir des renseignements personnels aux fins d'indentification des clients en vertu de l'article 14 du *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats.* Les renseignements ainsi recueillis permettent aussi à Neolegal Inc. de s'assurer, notamment, qu'il n'existe aucun conflit d'intérêts ou apparence de conflit d'intérêt.

Les processus généraux et anonymisation des données

La personne responsable de la protection des renseignements personnels au sein de Neolegal est le ou la VP, juridique en place. Me Catherine Fugère-Lamarre assume ce rôle et détient, supportée par le comité de cybersécurité, dont M. Sid Benachenhou, à titre de CTO, les responsabilités qui s'y rattachent.

Ses coordonnées sont les suivantes :

Courriel : confidentialite@neolegal.ca
Adresse : 420, rue Notre-Dame Ouest, Bureau 601
H2Y 1V3
Téléphone : 514-390-0367

Les données touchant les renseignements personnels des Client(e)s sont sécurisées par des logins et une authentification à deux facteurs. Ces données sont entreposées au Canada.

Des backups sont faits quotidiennement et un calendrier d'exercice de simulation est établit.

Les formations sur la cybersécurité sont offertes à tous les employés de Neolegal Inc. de manière régulière.

Un calendrier d'audit interne est aussi établi afin d'analyser régulièrement les procédés et les processus mis en place.

En vertu des articles 9 et 18 in fine du *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats,* Neolegal est tenu de conserver pendant une durée de 7 ans les dossiers des clients après la fermeture de ces derniers.

À la suite de cette période, les données sont encryptées et anonymisées en vertu des normes édictées par la Loi.

Après la fermeture d'un dossier et pour la durée de 7 ans, les renseignements personnels sont accessibles uniquement par les personnes autorisées. Il est en de même pour les dossiers ouverts.

La formation d'un Comité en Cybersécurité

Afin de s'assurer du maintien et du respect de cette politique, un comité formé du CTO, CLO, ainsi que la personne responsable des finances est mis en place dès l'adoption de cette politique.

Ce comité a pour tâche d'analyser les demandes d'informations, les plaintes, analyser l'ensemble des processus de cybersécurité et de la conservation des données.

Le comité veillera à se rencontrer de manière trimestrielle.

Ce comité aura aussi la responsabilité d'évaluer dans son ensemble tout risque de chaque projet informatique.

Processus pour les demandes d'informations ou les plaintes

Lorsque le ou la Client(e) désire obtenir des informations en lien avec cette politique, iel pourra le faire à l'adresse suivante : confidentialite@neolegal.ca ou privacy@neolegal.ca.

Si le ou la Client (e) désire souligner un incident de confidentialité ou porter plainte, iel devra respecter les étapes suivantes :

a. Écrire à l'adresse suivante : confidentialite@neolegal.ca ou privacy@neolegal.ca;
b. Écrire les motifs et la nature de la plainte;
c. Le comité fera une analyse de la plainte ou de l'incident;
d. Lors de la réception de la plainte, des délais seront stipulés afin de traiter adéquatement les informations;
e. Le plaignant sera avisé de l'avancement du dossier et si des renseignements additionnels sont nécessaires, une demande sera faite en ce sens;
f. Après décision du comité, une réponse sera envoyée au plaignant;
g. Si la plainte est justifiée, des actions claires et précises devront être mis en place le plus rapidement possible et le plaignant sera avisé desdites actions;
h. Si la plainte est non-justifiée, une réponse en ce sens sera envoyée aussi au plaignant et le dossier sera clos;
i. Advenant qu'un incident de confidentialité/sécurité ait eu lieu, le processus de divulgation auprès des autorités des compétentes, ainsi que des parties prenantes sera mise en place et suivie.

L'accès des employés aux renseignements personnels des Clients de Neolegal Inc.

Seuls les employé(e)s autorisé(e)s à chaque stade du mandat ont accès au dossier du Client(e).

Tous/toutes les employé(e)s de Neolegal Inc. sont tenu(e)s par le secret professionnel des avocat(e)s et ne peuvent en aucun cas divulguer de quelque manière que ce soit les informations ainsi perçues.

Aucun renseignement personnel ne pourra être écrite de manière manuscrite et si tel est le cas, l'employé(e) devra s'assurer de détruire de manière adéquate les renseignements ainsi écrits;

Le processus établit lors d'un incident de sécurité

Lors d'un incident de sécurité impliquant des renseignements personnels, les étapes suivantes seront suivies :

a) Le Comité se réunira afin de comprendre la situation;
b) Le CTO devra mettre en place les actions technologiques afin de rectifier rapidement la situation selon la nature;

c) Une évaluation sera faite pour savoir qui a été touché, ainsi que les risques pour la société et les risques de récidives;
d) CLO avisera la commission d'accès à l'information;
e) Un plan sera fait afin d'aviser les clients touchés, les partenaires, les employés, le conseil d'administration, les actionnaires et tous les dirigeants selon les besoins;
f) Un audit sera fait par la suite pour s'assurer que les données des clients sont bien protégées des suites de l'incident.

Les informations que le registre des incidents doit contenir :

a) Date de l'incident;
b) Le nom des personnes affectées et leur lien avec Neolegal inc.;
c) Nature de l'incident;
d) Impact de l'incident (ie. L'évaluation du risque);
e) Stratégie de communication auprès des personnes impliquées (voir la liste au point précédent);
f) Actions à prendre et prise pour résoudre l'incident;
g) Actions à prendre pour bloquer ce type d'incident dans le futur et la mise en place de solutions adéquates et durables.

La Commission d'accès à l'information devra aussi être mise au courant de tout risque au même titre que les incidents survenus et si ce potentiel d'incident engendre des risques sérieux.

La sécurité des renseignements personnels auprès de nos partenaires

Neolegal Inc. dans le cadre de ses fonctions fait affaire avec différents partenaires, soit et de manière non-exhaustive, des fournisseurs de services, des contractuels de services juridiques ainsi que des partenaires d'affaires de manière plus générale qui peuvent œuvrer dans différents secteurs, soit et non-exhaustivement, tel que le secteur juridique, des assurances ou autres.

Neolegal Inc. s'assure que chaque Partenaire respecte les plus hauts standards de l'industrie, ainsi que toutes les normes et les politiques édictées par *la Loi sur les renseignements personnels*.

Tous transferts de renseignements personnels auprès de partenaires d'affaires devront se faire de manière sécuritaire, de concert avec le département des technologies et le CTO.

Tous renseignements personnels des client(e)s ne pourra être transmis à un partenaire d'affaires sans l'obtention du consentement express du ou de la Client(e) et ne pourra se faire que sous les termes et conditions préalablement établis.

Neolegal Inc. s'assure que les transferts de renseignements personnels se fassent de manière sécuritaire à l'aide des technologies de l'information.