IA générative : votre liste de contrôle rapide

L'intelligence artificielle générative (IA) offre aux avocat(e)s et parajuristes d'immenses possibilités pour élargir leur pratique et améliorer leur prestation de services aux client(e)s. Mais comment les titulaires de permis peuvent-ils maitriser l'IA de manière responsable et conformément à leurs obligations professionnelles? La présente liste de contrôle fournit un guide précis, proposant des mesures concrètes et des recommandations pour intégrer l'IA dans les flux de travail juridique. Que vous exploriez le potentiel de l'IA générative, que vous l'utilisiez déjà ou que vous cherchiez à en optimiser l'utilisation, cette liste de contrôle propose une approche structurée allant de l'analyse initiale à la mise en œuvre d'outils d'IA générative. En suivant ces recommandations, vous pouvez gérer efficacement les risques, protéger les intérêts de vos clients et assurer l'intégration de manière responsable de l'IA générative dans votre pratique de droit ou de services juridiques.

Remarque : Selon les risques et les protections associés aux différents outils d'IA générative, vous n'avez pas à suivre toutes les recommandations indiquées. Les titulaires de permis doivent faire preuve de discernement pour déterminer les mesures à prendre dans les circonstances propres à chaque situation.

AVANT D'UTILISER L'IA

☐ Faire preuve de diligence raisonnable à l'égard des fournisseurs

- Évaluez l'expérience, la réputation, la fiabilité, la stabilité financière et le respect des normes juridiques des fournisseurs d'IA, y compris les lois sur la sécurité des données et la protection de la vie privée.
- Envisagez de créer ou d'utiliser une liste de contrôle ou un questionnaire* pour recueillir les renseignements essentiels au cours de votre processus d'évaluation.

☐ Examiner les conditions d'utilisation

- Examinez attentivement les conditions d'utilisation de l'outil d'IA et évaluez les conflits potentiels avec vos obligations professionnelles.
- Comprenez les responsabilités du fournisseur en cas de violation de données, de cyberattaque ou d'autres risques de divulgation involontaire.

☐ Connaitre les limites et les capacités

- Effectuez des recherches approfondies et expérimentez l'outil d'IA pour bien comprendre ses capacités et ses limites.
- Vérifiez la facilité avec laquelle l'outil d'IA s'intègre à vos systèmes ou logiciels existants.

☐ Évaluer la compétence et établir des lignes directrices

- Évaluez vos connaissances et vos compétences dans l'utilisation de l'outil d'IA, ainsi que votre compréhension de ses avantages et des risques qu'elle pose.
- Établissez des lignes directrices pour l'utilisation de l'outil d'IA, en vous assurant que vous et vos employé(e)s avez les compétences et les renseignements nécessaires pour bien utiliser l'outil dans le respect de l'éthique.

☐ Élaborer des protocoles de communication

- Trouvez des scénarios dans lesquels une communication transparente sur l'utilisation de l'outil d'IA avec un client est requise pour gérer les attentes et atténuer les risques. Précisez les cas où il convient d'obtenir le consentement éclairé du client.
- Établissez des protocoles de communication clairs et bien définis pour discuter de l'utilisation de l'IA avec les clients.

☐ Mettre en œuvre des mesures de protection des données

- Comprenez comment les données que vous saisissez dans l'outil d'IA sont traitées, stockées et protégées.
- Déterminez les mesures de sécurité mises en place par le fournisseur pour protéger l'outil d'IA contre un accès non autorisé.
- Au besoin, établissez des protocoles additionnels pour protéger les renseignements confidentiels des clients contre la divulgation involontaire.

☐ **Procéder aux essais et à la validation**

- Déterminez comment l'outil d'IA a été formé* (p. ex., demandez au fournisseur des renseignements concernant la source de l'ensemble des données, la manière dont les données ont été étiquetées et validées, et les algorithmes utilisés pour former l'outil d'IA).
- Utilisez ces renseignements pour reconnaitre et atténuer les biais des données et les autres risques.

☐ **Évaluer les pratiques de facturation pour l'utilisation de l'IA**

- Déterminez s'il convient de transférer aux clients les frais liés à l'utilisation de l'IA. Le cas échéant, assurez-vous que les frais facturés sont justes et raisonnables, et qu'ils sont communiqués sans délai aux clients.
- Toute disposition visant à transférer les frais d'utilisation de l'IA doit être clairement consignée par écrit et expliquée aux clients.

QUAND UTILISER L'IA

☐ **Incorporer un processus de vérification humaine**

- Intégrez un système ou un processus* de vérification humaine pour examiner les résultats générés par l'IA et assurer leur exactitude et leur fiabilité.
- Précisez les tâches ou les processus juridiques pour lesquels le jugement humain est essentiel et pour lesquels l'outil d'IA ne doit **pas** être utilisé.

☐ **Maintenir un historique de vérification**

- Établissez un processus systématique pour enregistrer toutes les invites et les données d'entrée que vous ou vos employés versez dans l'outil d'IA.
- Examinez régulièrement l'historique de vérification pour reconnaitre les risques, les anomalies ou d'autres problèmes, et prenez des mesures proactives pour les atténuer.

☐ **Donner la priorité à la confidentialité des clients**

- Demandez aux utilisateurs de l'IA de ne pas saisir d'invites susceptibles d'identifier des clients ou des affaires juridiques spécifiques.
- Établissez des protocoles clairs pour anonymiser ou supprimer les données sensibles utilisées comme invites.

☐ **Fournir une formation continue et solliciter une rétroaction**

- Proposez une formation continue aux utilisateurs de l'IA pour vous assurer qu'ils utilisent l'outil en conformité avec vos obligations professionnelles et légales.
- Recueillez régulièrement des commentaires sur le rendement des outils d'IA, leur convivialité et les aspects nécessitant des améliorations.

☐ **Superviser l'utilisation de l'IA par les employés**

- Formez les utilisateurs de l'IA aux invites appropriées, en précisant notamment celles qu'il convient d'éviter. Insistez sur l'importance du respect de la confidentialité dans toutes les interactions avec l'outil d'IA.
- Contrôlez régulièrement l'utilisation de l'IA par les employés et envisagez de mettre en place des autorisations d'utilisateur et des contrôles d'accès pour limiter l'entrée de données.

☐ **Éviter la violation des droits d'auteur**

- Demandez au fournisseur de l'IA si l'outil a été formé avec un contenu protégé par le droit d'auteur et, le cas échéant, vérifiez les conditions d'utilisation de ce contenu.
- Faites preuve de discernement lorsque vous traitez des contenus générés par l'IA, et veillez à y apporter votre propre expertise et vos propres idées.

APRÈS L'UTILISATION DE L'IA

☐ **Évaluer le rendement et l'efficacité**

- En fonction de l'utilisation, des essais et des commentaires, évaluez les effets de l'outil d'IA sur l'efficacité, la précision et la productivité.

☐ **Mener des contrôles de la conformité**

- Effectuez périodiquement des contrôles de conformité, d'éthique et de sécurité afin de repérer et

de corriger toute vulnérabilité et de garantir le respect continu de vos obligations légales et professionnelles.

☐ **Documenter les résultats générés par l'IA**

- Conservez un registre des résultats générés par l'outil d'IA en veillant à consigner les cas où les recommandations de l'IA reposaient sur des informations fantaisistes ou sur des données inventées ou fausses.

☐ **Se tenir au courant des développements en matière d'IA**

- Suivez les derniers développements en matière d'IA afin de garantir la conformité avec les règlementations juridiques, les responsabilités éthiques, les lignes directrices et les normes en constante évolution.

***Remarque :** Les ressources tierces mentionnées dans le présent document sont fournies à titre d'information seulement et ne constituent pas une approbation ou une recommandation de la part du Barreau de l'Ontario. Le Barreau ne contrôle ni ne garantit l'exactitude, la pertinence ou la qualité du contenu des ressources tierces.