1. INFORMATIONS GÉNÉRALES

- **Technologie de signature** : Le concepteur doit décrire le type de technologie de signature offert aux clients finaux — numérique ou électronique.
  - Détails : Décrire sommairement le processus de signature ainsi que les avantages de la technologie proposée.
- **Sécurité de la technologie :** Le concepteur doit aussi renseigner les mécanismes de sécurité appliqués pour assurer la prévention des menaces internes et externes de sécurité informatique (comme des politiques, procédures, outils de sécurité, etc.).
  - Détails **:** Est-ce que le concepteur répond aux diverses exigences de sécurité nécessaires pour respecter les lois applicables comme la Loi sur la protection des renseignements personnels dans le secteur privé du Québec, la loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE), et les normes de sécurité comme ISO 3200 et ISO 27001 et autres ?
- **Hébergement** : L'OACIQ privilégie l'hébergement au Québec et au Canada puisque les normes en matière de protection des renseignements personnels y sont reconnues et sûres. À noter que la loi exige qu'une évaluation des facteurs relatifs à la vie privée (EFVP) soit réalisée par l'entreprise en cas de communication et d'entreposage à l'extérieur du Québec des informations incluant les renseignements personnels.
- **Hébergement de la solution** : Le concepteur doit indiquer le ou les lieux d'hébergement de la solution, ainsi que les sites de relève.
- **Hébergement des formulaires signés** : Le concepteur doit indiquer le ou les lieux d'hébergement du stockage des données, ainsi que les sites de relève. Dans le cas d'un intégrateur de technologie de signature, il est important de mentionner le lieu d'incorporation du fournisseur de la technologie de signature.
- **Système de redondance** : Le concepteur doit indiquer la stratégie de redondance mise en place pour assurer la haute disponibilité.
  - Détails : Si aucune stratégie/système de redondance n'est en place, le concepteur doit indiquer :
    - la période maximale pendant laquelle il peut y avoir perte d'information en relation avec la stratégie de sauvegarde ;
    - le processus qu'il entend mettre en place pour se prémunir contre la perte d'information advenant un bris d'équipement entre deux sauvegardes.

2. GESTION DES FORMULAIRES OACIQ

- **Format des fichiers pour le chargement des formulaires à signer** : Le concepteur doit indiquer les divers formats de fichiers autorisés sur lesquels l'utilisateur pourra apposer sa signature.
- **Personnalisation des zones de signature** : Le concepteur doit indiquer le type d'usager qui est autorisé à personnaliser les diverses zones de signature. Il doit indiquer également le nombre maximal de signatures par formulaire.

- **Sauvegarde des zones de signature sous forme de gabarit** : Le concepteur doit indiquer si la solution permet de sauvegarder des gabarits de formulaires avec les zones de signature préétablies, et de constituer une librairie de formulaires à signer.
    - Détails : Ce faisant, lorsque l'utilisateur voudra faire signer un formulaire existant, il ne lui sera pas nécessaire de définir les zones de signature, car elles auront été sauvegardées au préalable.
- **Stockage des formulaires prédéfinis sur le site du fournisseur** : Le concepteur doit indiquer s'il est possible de conserver une librairie de formulaires prédéfinis, préciser la limite de formulaires pouvant être conservés ainsi que le format des fichiers.
- **Jumelage automatique du formulaire chargé avec un gabarit prédéfini** : Le concepteur doit indiquer si le système permet de jumeler automatiquement un formulaire chargé par l'utilisateur avec un formulaire prédéfini contenu dans la librairie de formulaires.
- **Interface multilingue — anglais et français** : Obtenir du concepteur une copie des interfaces de gestion des formulaires afin d'en valider la qualité.
- **Personnalisation de l'interface** : Le concepteur doit indiquer si l'interface de gestion des formulaires peut être personnalisée aux couleurs/logos d'un courtier.
    - Détails : Il devra fournir un exemple de personnalisation.

3. GESTION DES SIGNATAIRES, SÉCURITÉ DES ACCÈS

- **Gestion de multiples signataires** : Le concepteur doit indiquer si le système permet la gestion de multiples signataires, tant pour l'acquéreur que le vendeur, et indiquer le nombre maximal de signataires.
- **Gestion du flux/séquence des signataires** : Le concepteur doit décrire le processus de gestion des signataires.
    - Détails : Il devra décrire comment l'utilisateur peut contrôler le flux de signature des signataires selon l'une des deux options suivantes :
        - ✓ *Processus en série/séquence* : Sous-entend qu'un ensemble de formulaires à signer ne pourra être transmis au prochain signataire que lorsque le premier signataire aura achevé avec succès la signature de l'ensemble des formulaires ;
        - ✓ *Processus en parallèle* : Sous-entend qu'un ensemble de formulaires à signer peut-être transmis à tous les signataires simultanément et indépendamment de l'état d'achèvement.
    - Dans le cas où les signataires sont représentés par différents intervenants, le système de signature électronique ou numérique doit permettre un processus d'affaires.
- **Personnalisation des courriels à l'ensemble des signataires** : Le concepteur devra fournir un exemple de personnalisation des courriels acheminés aux signataires.

- Détails : Si aucune personnalisation n'est permise, le concepteur devra fournir un exemple du message qui sera transmis aux signataires.

- **Personnalisation de la langue du courriel par le signataire** : Le concepteur devra indiquer si l'on peut personnaliser la langue du courriel qui sera acheminé pour chacun des signataires.
- **Niveaux de sécurité (Vérification de l'identité du signataire) :** Le concepteur devra décrire le processus et les différentes méthodes qui permettront de s'assurer de l'identité numérique du signataire avant de pouvoir accéder au site contenant les formulaires à signer.
  Détails : La validation de l'identité du signataire doit se faire en combinant au moins (2) deux des méthodes détaillées ci-après :
  - ✓ Une **preuve de l'identité** avec une validation à travers des documents officiels, comme la carte d'assurance maladie, le passeport, le permis de conduire, etc.
  - ✓ Une **confirmation basée sur les connaissances** qui peut être statique (utilisation de renseignements personnels recueillis antérieurement ou établis à un moment précis dans le temps) ou dynamique (utilisation de renseignements personnels recueillis ou générés au fil du temps).
  - ✓ Une **confirmation des caractéristiques biologiques ou comportementales** (comparaison des traits faciaux, comparaison de l'iris, comparaison des empreintes digitales, comparaison de la voix, analyse des données, etc.).
  - ✓ Une **confirmation par un arbitre de confiance** (Répondant, Notaire, Agent agréé)
  - ✓ Une **confirmation par un élément connu de l'utilisateur** (par exemple des jetons à secret mémorisé ou des jetons à renseignement préenregistré), par un **élément que l'utilisateur possède** (par exemple un jeton à secret matriciel, un jeton hors bande, un dispositif de mot de passe à usage unique et à un seul facteur ou un dispositif cryptographique à un seul facteur) ou par un **élément que l'utilisateur produit ou qui le caractérise** (comme les données biométriques telles que l'empreinte digitale, le balayage rétinien et la reconnaissance faciale).

    La confirmation peut comporter une interaction sécurisée avec un processus de validation physique ou électronique comme une une notification push sur un dispositif hors bande comme un téléphone intelligent.

  La méthode de vérification d'identité (avec pièce valide avec photo délivrée par un gouvernement) devrait être privilégiée, car elle représente un risque moins élevé en comparaison avec les autres méthodes.
- **Sécurité des transactions :** Le concepteur doit fournir des garanties sur la sécurité des signatures électroniques.
  Pour cela, il doit :
  - ✓ **Garantir l'intégrité du document signé**

  Le concepteur doit démontrer qu'un document signé ne pourra être altéré. Il devra décrire le processus de certification des documents PDF utilisés afin d'en assurer l'authenticité.

- Détails : Une fois le processus de signature terminé, les documents doivent être scellés électroniquement via un sceau numérique inviolable généré depuis une infrastructure à clé publique (ICP). Ce sceau confirme la validité de la signature et garantit que le document électronique n'a subi aucune altération ou modification depuis sa date de signature.
  Si le concepteur n'utilise pas de signature numérique, il doit démontrer que le processus utilisé garantit le caractère authentique des documents signés.

✓ **Délivrer un certificat d'achèvement**

Ce certificat électronique renforce la sécurité de la signature digitale en fournissant des informations détaillées sur chaque signataire. Ces informations doivent inclure la déclaration du consommateur confirmant l'accord du signataire à utiliser la signature sous forme électronique, l'image de cette signature, les horodatages associés aux événements clés, l'adresse IP du signataire et d'autres données d'identification. Ces éléments contribuent à valider et authentifier la signature électronique du signataire.

- **Journalisation des transactions :** Le concepteur doit démontrer la procédure de suivi des transactions faites dans le système. Il doit, pour se faire, fournir pour chaque transaction, une piste d'audit qui va agir comme un enregistrement électronique de toutes les actions effectuées sur le document numérique. Cette piste d'audit doit détailler l'historique et l'horodatage (qui lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données et qui doit être fondé sur une horloge exacte liée au temps universel coordonné), y compris quand le document a été ouvert, consulté et signé. En cas de contestation ou de doute sur une signature électronique, cette piste d'audit, accessible à tous les participants à la transaction, permet d'apporter des preuves et de résoudre les objections.
  - Details: Le concepteur devra fournir une copie du journal des transactions.

- **Considérations pour une validation à long terme :** Le concepteur doit démontrer que tous les renseignements nécessaires pour valider la signature électronique vont être disponibles tant que l'enregistrement doit être conservé. La signature électronique doit pouvoir être vérifiée et confirmée au fil du temps.

- **Attribution des accès :** Le concepteur doit indiquer les outils de gestion des accès. Il doit indiquer quel groupe d'individus ou quel individu autorise quels individus, ainsi que les mécanismes garantissant la confidentialité d'accès des individus (modification des mots de passe).
  - Details: Étant donné que l'utilisateur peut utiliser le système de signature sans être membre d'une chambre immobilière, il sera important de savoir si le concepteur exige que l'OACIQ soit l'unique responsable de l'attribution des accès. Si tel était le cas, cette solution ne serait pas souhaitable et viable.

- **Groupe d'utilisateurs :** Le concepteur doit indiquer les groupes d'utilisateurs qui ont accès au système. Cette description doit définir qui sont les utilisateurs faisant partie de ces groupes, leurs droits et leurs privilèges — administrateur, utilisateur, signataire, etc. Cette gestion des accès doit respecter les principes du « moindre privilège » (un concept de sécurité dans lequel on accorde à un utilisateur le niveau d'accès [ou les permissions] minimum requis pour accomplir son travail) et du « besoin de savoir » (principe selon lequel l'accès à un fichier doit être donné qu'à des utilisateurs dûment autorisés et authentifiés) pour minimiser le risque d'exposition des données.

- **Maintien de la confidentialité d'accès :** Le concepteur doit indiquer les mécanismes permettant d'assurer le maintien de la confidentialité d'accès des utilisateurs, particulièrement lorsque l'application est accessible par les clients et qu'une authentification électronique est requise. Des mécanismes comme une authentification multiple sont attendus.

- **Résiliation des droits d'accès :**

Le concepteur doit décrire les processus permettant d'interrompre l'accès au système à ceux qui n'ont plus les privilèges d'accès, quelle qu'en soit la raison : changement d'agence, fin de l'abonnement au service, etc. Le processus doit permettre de reconnaître à temps la résiliation de l'accès et d'interrompre immédiatement l'accès.

4. GESTION DU FLUX DES SIGNATAIRES

- **Saisie d'une date d'expiration — délai de signature pour le flux de signataires** : Le concepteur doit indiquer si le système permet d'appliquer un délai de signature, soit une date de fin ou un délai en heures ou en jours.
- **Gestion du délai des rappels aux signataires** : Le système devra permettre un mécanisme de suivi et de rappel auprès des signataires, les avisant qu'un document ou une série de documents sont prêts à être signés. Le concepteur devra fournir un exemple de ce rappel afin de s'assurer que le rappel soit disponible en français.
- **Alerte automatique au gestionnaire du processus — courriel** : Le système devra permettre d'aviser automatiquement par courriel l'utilisateur/gestionnaire afin de connaitre l'état d'avancement du processus de signature. Tous les signataires doivent recevoir la confirmation que le processus est complété. Chacun pourra télécharger et sauvegarder le document.
- **Visualisation de l'état d'avancement du processus de signature** : Le système devra permettre de visualiser à l'écran l'état d'avancement du processus de signature.

5. PROCESSUS DE SIGNATURE DES FORMULAIRES

- **Interface multilingue — anglais et français** : Le concepteur doit s'assurer que toutes les interfaces qui seront affichées aux signataires soient en anglais et en français.
- **Accessibilité par un navigateur – IE, Safari, Firefox, Chrome** : Le concepteur devra fournir la liste de tous les navigateurs autorisés ainsi que leurs numéros de version.
- **Application Android, iPhone, iPad** : Il s'agit de déterminer si la solution de signature est accessible, à l'aide d'une application spécifique, par les téléphones intelligents ou les tablettes numériques. Le concepteur devra fournir une liste des plateformes autorisées.
- **Affichage et acceptation d'un consentement avant de débuter le processus de signature** : Le concepteur doit permettre d'afficher et d'exiger que le signataire accepte le consentement avant de démarrer le processus de signature.
    - Détails : Le concepteur devra permettre de personnaliser le formulaire de consentement en anglais et en français.
- **Plateforme acceptée pour le processus de signature** : Le concepteur doit spécifier les plateformes disponibles qui pourraient être utilisées par les signataires durant le processus de signature.
- **Option de signature** : Le concepteur doit décrire les diverses options de signature offertes aux signataires. L'utilisation du clavier avec sélection du type de calligraphie serait une option de base minimale.
- **Navigation assistée aux zones de signature** : Le concepteur doit permettre au signataire de naviguer rapidement entre les zones de signature, et l'informer du pourcentage ou du stade d'achèvement du processus de signature.
- **Zones de signature bien identifiées** : Le système doit clairement indiquer les zones précises où les signatures ou les initiales devront être apposées par le signataire.
- **Sauvegarde du formulaire signé** : Le système doit permettre de sauvegarder le formulaire signé sur la plateforme du signataire, ainsi que d'héberger et de stocker les formulaires sur le ou les serveurs du concepteur/fournisseur de la solution.
- **Capacité d'exporter un ensemble de documents signé**s : Le concepteur doit permettre au gestionnaire du processus de signature d'avoir la capacité de sélectionner et d'exporter un ensemble de documents signés en format PDF.

6. INCLUSIONS OBLIGATOIRES OU ÉQUIVALENTES AU CONTRAT LIANT LE FOURNISSEUR ET LES CLIENTS

- Les clauses contractuelles énoncées ci-dessous ou des clauses équivalentes devront obligatoirement être incluses dans tout contrat liant le fournisseur à un client, en anglais ou en français, en fonction de la langue du contrat.
- Le fournisseur devra fournir, en vue de son accréditation par l'OACIQ, copie du contrat qu'il entend utiliser dans le cadre de sa relation d'affaires avec les clients.

- Lorsque les clauses énoncées ci-dessous ne seront pas reproduites intégralement au contrat, des frais supplémentaires seront exigés pour fin d'approbation des équivalences.

Préambule	ATTENDU QUE le Client est un courtier/une agence au sens de la Loi sur le courtage immobilier et ses règlements qu'il/elle est assujetti(e) au pouvoir de surveillance et de contrôle de l'Organisme d'autoréglementation du courtage immobilier du Québec (« OACIQ ») ainsi qu'aux pouvoirs du syndic de l'OACIQ ;
Préambule	ATTENDU QUE le Client détient des données, des applications, des renseignements, des documents et informations confidentielles, incluant des renseignements personnels (ci-après l'"actif informationnel") dont la cueillette, la conservation, l'utilisation, la communication et la destruction sont sujettes aux règlements adoptés en vertu de la *Loi sur le courtage immobilier* (c. C-73.2) et aux dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé* (c. P-39.1) (ci-après la "Loi sur le secteur privé");
Préambule	ATTENDU QUE, conformément à ses obligations légales, le Client est tenu de protéger les renseignements personnels qu'il recueille, utilise, conserve, communique et détruit et qu'il est, entre autres, tenu d'aviser les personnes concernées du nom du tiers pour qui la collecte des renseignements personnels est faite, du nom du tiers à qui il est nécessaire de communiquer les renseignements personnels recueillis et de la possibilité que ces renseignements soient communiqués à l'extérieur du Québec;
Préambule	ATTENDU QUE, conformément à ses obligations légales, le Client doit réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) en cas de communication et d'entreposage à l'extérieur du Québec des renseignements personnels qu'il détient;
Préambule	ATTENDU que le Client, doit, s'il a des motifs raisonnables de croire que s'est produit un *incident de confidentialité* au sens de la Loi sur le secteur privé et que cet incident implique un renseignement personnel qu'il détient, prendre des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature se produisent et qu'il doit aussi, si l'incident présente un risque sérieux de préjudice, en aviser les personnes concernées et les autorités compétentes;
Préambule	ATTENDU QUE le Client et le Fournisseur souhaitent, conformément aux obligations légales leur incombant, convenir des obligations et mesures destinées à assurer en tout temps le caractère confidentiel de l'actif informationnel du Client, dont notamment des renseignements personnels reçus, utilisés, conservés ou communiqués dans le cadre de l'exécution de ce contrat;

Protection de l'actif informationnel	Le Fournisseur reconnait qu'il est responsable en tout temps d'assurer la protection et le caractère confidentiel de l'actif informationnel, dont notamment des renseignements personnels, qu'il reçoit dans le cadre du présent contrat et ce, lors de sa communication, son utilisation, sa détention, sa conservation et sa destruction.
Sous-traitants	Le Fournisseur doit encadrer les activités et obtenir des engagements contractuels de ses sous-traitants afin de s'assurer qu'ils respectent les obligations stipulées à ce contrat, notamment celles relatives à la communication, l'utilisation, la conservation, la destruction et la protection des renseignements personnels. Le Fournisseur est garant envers le Client de la pleine exécution de ces obligations. Nonobstant les termes des ententes susceptibles d'intervenir entre le Fournisseur et ses sous-traitants, le Fournisseur est responsable de l'entièreté des obligations souscrites dans le présent contrat en regard des services, ainsi que du maintien de la confidentialité de l'actif informationnel, et il est garant envers le Client de la pleine exécution de ces obligations.
Cloisonnement des Actifs informationnels	Le Fournisseur s'engage à fournir les services et à conserver l'actif informationnel du Client de façon à en assurer le cloisonnement logique. Les parties reconnaissent que cela n'exclut pas le recours aux installations d'hébergement d'un tiers agissant comme sous-traitant du Fournisseur.
Équipements dédiés	*Note : Dans la mesure où la sensibilité de l'information le commande et justifie des coûts plus élevés, certains fournisseurs offrent des équipements dédiés. Le cas échéant, la clause suivante peut être utilisée* : Le Fournisseur s'engage à recourir à l'utilisation d'équipements dédiés à la prestation des services afin d'assurer le cloisonnement de l'actif informationnel du client. Les parties reconnaissent que cela n'exclut pas le recours aux installations d'hébergement d'un tiers agissant comme sous-traitant du Fournisseur.
Restriction à localisation géographique	Le Fournisseur s'engage à aviser le Client de l'emplacement géographique des installations, équipements et systèmes utilisés dans le cadre de l'exécution du contrat et sur lesquels seront hébergés l'actif informationnel du Client. Le Fournisseur s'engage à n'utiliser que des installations ou équipements situés à l'intérieur des limites territoriales du Canada, de préférence au Québec. Le Fournisseur s'engage à aviser le Client sans délai et chaque fois lorsque lui ou un sous-traitant dans le cadre du présent contrat a recours aux installations d'hébergement se situant à l'extérieur du Québec.
Avis et coopération en cas de demande ou ordonnance	Lorsque le Fournisseur ou l'un de ses sous-traitants reçoit une ordonnance émise par un tribunal, une assignation (subpoena), ou toute autre requête d'une autorité compétente exigeant la communication de l'actif informationnel, le Fournisseur s'engage à en aviser immédiatement, et dans un délai maximal de quatre (4) heures, le Client. Les obligations du Fournisseur en vertu de ce paragraphe s'appliquent à l'égard

d'accès par des autorités	de toute demande entraînant l'accès ou la communication de l'actif informationnel du Client, indépendamment du fait que l'ordonnance, l'assignation, ou toute autre requête d'une autorité compétente porte spécifiquement ou non sur ceux-ci. Le Fournisseur s'engage, dans la mesure permise par les lois du Québec, à vérifier la légalité de la procédure d'émission ou d'obtention de l'ordonnance, de l'assignation ou de toute autre requête d'une autorité compétente. À moins qu'il ne s'agisse d'une requête de tout type provenant de l'OACIQ, le Fournisseur s'engage à s'opposer à l'ordonnance, à l'assignation ou à toute autre requête d'une autorité compétente ou requérir une remise de son exécution, afin de permettre au Client de réviser l'objet de celles-ci et faire valoir, le cas échéant, ses droits ou ceux de ses clients. Dans l'éventualité où le Fournisseur ne peut aviser le Client en temps opportun, ou s'il ne peut légalement l'informer de l'ordonnance, de l'assignation ou de toute autre requête d'une autorité compétente en temps opportun, le Fournisseur s'engage à informer le Client dès qu'il sera légalement autorisé à le faire. Le Fournisseur maintiendra, dans la mesure permise par les lois du Québec, un registre des demandes.
Confidentialité sécurité	Le Fournisseur s'engage à prendre et à appliquer les mesures de sécurité adéquates et à assurer la protection et le maintien de la confidentialité, de l'intégrité et de l'accessibilité de l'actif informationnel du Client, par un mécanisme de chiffrement des documents et des données au moment de leur transmission et pendant leur conservation, mais aussi aux centres où l'actif informationnel est entreposé et conservé. Le Fournisseur s'engage aussi à prendre et à appliquer les mesures relatives au contrôle d'accès, à l'authentification des utilisateurs et à la continuité des opérations qui sont raisonnables compte tenu, notamment, de la sensibilité de l'actif informationnel reçu et/ou communiqué dans le cadre du présent contrat, de la finalité de son utilisation, de sa quantité et de son support. Les processus en place doivent également viser à empêcher les *incidents de confidentialité* au sens de la Loi sur dans le secteur privé, les atteintes à la sécurité, les erreurs (comme les modifications non encadrées des systèmes), la malveillance, ainsi que la divulgation ou la destruction de l'actif informationnel sans autorisation. Le Fournisseur s'engage à se doter d'un mécanisme d'identification et de gestion des risques auxquels le Fournisseur fait face, d'audit ou de vérification permettant d'attester du respect des règles et processus en place.
Confidentialité sécurité	Le Fournisseur reconnaît qu'il se verra communiqué, et aura accès à l'actif informationnel confidentiel recueilli et conservé par le Client dans le cadre de ses activités. Le Fournisseur reconnaît que l'actif informationnel demeure la propriété exclusive du Client ou que celui-ci en est le détenteur au sens de la Loi sur le secteur privé ; qu'il peut ainsi revendiquer l'actif informationnel, et que toute divulgation non autorisée de l'actif informationnel, dont notamment les renseignements personnels, lui causerait des préjudices importants.

Confidentialité sécurité	Le Fournisseur s'engage à préserver le caractère confidentiel de l'actif informationnel dans le cadre de l'exécution du présent contrat et à prendre, à chacune des étapes de l'exécution du contrat, toutes les mesures appropriées à cette fin : • Préserver la confidentialité des codes d'utilisateur, mots de passe et clés de chiffrement selon les meilleures pratiques de l'industrie ; • Faire signer au préalable, à toute personne affectée par le Fournisseur à la manipulation ou au traitement de l'actif informationnel, un engagement de confidentialité et un engagement relatif au respect des mesures de sécurité, restreindre l'accès, la communication ou la divulgation de l'actif informationnel à ces seules personnes, et effectuer une vérification préalable des antécédents avant le recrutement de celles-ci. • Utiliser l'actif informationnel, dont notamment les renseignements personnels, uniquement aux fins pour lesquelles il a été communiqué ; • Ne pas communiquer l'actif informationnel du Client, dont notamment les renseignements personnels reçus et/ou communiqué dans le cadre du présent contrat à des tiers, sauf dans la mesure où cela est nécessaire pour l'exécution du présent contrat. Collaborer avec le Client, et ses clients le cas échéant, afin de permettre aux personnes visées d'exercer leur droit d'accès et de rectification de leurs renseignements personnels ; • Collaborer avec le Client afin de procéder à la destruction des renseignements personnels et des profils d'utilisateur en conformité avec le calendrier de conservation applicable ; • Ne pas reproduire l'actif informationnel du Client, dont notamment les renseignements personnels reçus et/ou communiqués dans le cadre du présent contrat, à moins qu'une telle reproduction ne soit requise dans le cadre de l'exécution du présent contrat. • Collaborer à toute enquête ou vérification concernant le respect de la confidentialité de l'actif informationnel, dont notamment des renseignements personnels.
Droit de vérification	Le Fournisseur reconnaît au Client le droit de s'assurer, en tout temps, du respect des obligations souscrites ci-dessus, de la conformité à la Loi sur le secteur privé et à la Loi sur le courtage immobilier incluant, si nécessaire, l'accès à ses installations. Le Fournisseur s'engage, au même titre que le Client, à collaborer à toute enquête ou vérification faite par les autorités compétentes incluant l'OACIQ.

Avis et coopération en cas de violation de la confidentialité des renseignements personnels et/ou d'atteinte à la sécurité	Le Fournisseur s'engage à aviser sans délai, et dans un délai maximal de quatre (4) heures le Client de toute violation ou tentative de violation par toute personne des obligations relatives à la confidentialité des renseignements personnels communiqués dans le cadre du présent contrat, de tout incident de confidentialité au sens de la Loi sur le secteur privé, de tout accès ou tentative d'accès non autorisé ou de toute atteinte au caractère confidentiel de l'actif informationnel du Client. Le Fournisseur s'engage au surplus à poser sans délai les actes nécessaires afin de pallier le risque d'atteinte continue, à procéder à une enquête afin d'identifier toute vulnérabilité et à apporter les correctifs nécessaires afin d'éviter toute répétition d'un tel incident. Le Fournisseur s'engage à permettre au Client ou à toute personne désignée par lui d'effectuer toute vérification relative à la confidentialité des renseignements personnels. À cet effet, le Fournisseur permettra au Client ou à toute personne désignée par lui à avoir accès à tout lieu, matériel, document ou équipement en lien avec toute violation ou tentative de violation des obligations relatives à la confidentialité des renseignements personnels. Les parties procéderont conjointement à l'analyse et à la gestion de la situation afin de minimiser les risques et d'identifier les intervenants appropriés en fonction du risque. Le Fournisseur s'engage à prendre toute mesure demandée par le Client pour diminuer le risque qu'un préjudice soit causé.
Assurance	Le Fournisseur doit souscrire et maintenir en vigueur pendant la durée du contrat à ses frais et auprès de compagnies d'assurance reconnues, une police d'assurance responsabilité professionnelle d'un minimum de cinq cent mille dollars (500 000 $ en dollars canadiens) par évènement, avec une franchise n'excédant pas 10 000 $ couvrant, sans s'y limiter, les pertes et dommages qui résultent d'erreurs ou omissions dans l'exécution du contrat. Cette police d'assurance professionnelle devra également comprendre la même couverture relativement aux pirates informatiques (hackers) qui pourraient accéder par effraction à l'actif informationnel du Client, à une erreur ou une omission attribuable au Client, et inclure l'avenant contre la destruction, la modification, la perte ou autres cas similaires relativement aux données informations, incluant les renseignements personnels, et documents du Client.
Terminaison, résiliation, annulation	Le Fournisseur doit, dans un délai de 30 jours suivant la date de la terminaison, de la résiliation ou de l'annulation du contrat, remettre au Client l'ensemble de l'actif informationnel reçu et/ou communiqué dans le cadre du présent contrat, et ce, quel que soit la nature des renseignements, documents ou informations ou le support sur lequel ils sont contenus. À compter de la date de la terminaison, de la résiliation ou de l'annulation du contrat, le Fournisseur s'engage à ne pas conserver copie et à ne plus utiliser l'actif informationnel, dont notamment les renseignements personnels reçus et/ou

	communiqués dans le cadre du présent contrat. À la demande écrite expresse du Client, le Fournisseur s'engage à lui fournir une preuve à cet effet, jugée acceptable par le Client. Les obligations du Fournisseur relatives à la confidentialité des renseignements personnels reçus et/ou communiqués dans le cadre du présent contrat survivent à sa terminaison, à sa résiliation ou à son annulation.