# Bonnes pratiques en matière de protection des renseignements personnels pour courtiers immobiliers

## 1 – Gestion des documents (papier et numérique)

- Ne pas conserver de copies de transactions sur un ordinateur personnel non sécurisé.
- Détruire systématiquement les documents papier sensibles avec une déchiqueteuse à coupe croisée.
- Ne jamais jeter de documents contenant des données privées à la poubelle ou au recyclage sans les rendre illisibles.
- Ranger les dossiers clients dans une armoire verrouillée, jamais sur un bureau accessible.
- Éviter de transporter des dossiers papier dans sa voiture sans coffre verrouillé.
- Numériser les documents uniquement sur un appareil protégé par mot de passe.
- Ne pas laisser traîner de contrats ou formulaires dans une salle de réunion après un rendez-vous.
- Définir un calendrier de conservation et destruction des dossiers (ex. 30 jours après l'acte de vente puis destruction des documents physiques).
- Ne pas conserver de copies de NAS ou pièces d'identité dans des fichiers non protégés.
- Éviter de photocopier inutilement des documents sensibles.
- Ne pas mélanger les dossiers personnels et professionnels dans un même classeur.
- Utiliser des enveloppes opaques pour transmettre des documents sensibles.
- Ne jamais laisser un dossier client dans une salle d'attente.

## 2 – Sécurité numérique

- Utiliser un ordinateur professionnel distinct de l'ordinateur personnel.
- Activer la double authentification sur les plateformes de courtage et CRM.
- Ne pas envoyer de documents sensibles par courriel sans chiffrement ou mot de passe.
- Éviter de stocker des copies de contrats sur des clés USB non protégées.
- Mettre à jour régulièrement les logiciels et antivirus.
- Ne jamais partager ses accès CRM ou courriel avec un collègue.
- Utiliser un réseau Wi-Fi sécurisé, éviter les connexions publiques.
- Sauvegarder les données sur un serveur ou cloud conforme aux lois québécoises.

- Ne pas conserver de copies de documents sensibles dans des applications de messagerie instantanée (SMS, WhatsApp).
- Éviter d'utiliser une adresse courriel personnelle pour les communications professionnelles.
- Ne pas utiliser de mots de passe simples (ex. "1234" ou "maison").
- Changer ses mots de passe tous les 6 mois.
- Ne pas laisser son ordinateur ouvert et accessible lors de rendez-vous.
- Activer le verrouillage automatique de l'écran après quelques minutes d'inactivité.
- Ne pas utiliser de services gratuits de stockage en ligne sans vérifier leur conformité.
- Ne pas envoyer de photos de documents par Messenger ou réseaux sociaux.

## 3 – Relation client

- Informer clairement les clients de la manière dont leurs données seront utilisées.
- Obtenir un consentement écrit avant de collecter des renseignements sensibles.
- Ne pas demander plus d'informations que nécessaire pour une transaction.
- Fournir aux clients un moyen simple de retirer leur consentement pour toutes les communications commerciales électroniques.
- Remettre aux clients une copie numérique lisible de leurs données si demandé.
- Éviter de discuter de dossiers clients dans des lieux publics.
- Ne pas laisser un client signer un document sans lui expliquer l'usage des données.
- Ne pas conserver de copies de pièces d'identité après vérification (sauf si la procédure de la vérification d'identité utilisée l'exige expressément dans les normes de conformité de CANAFE).
- Ne pas utiliser les coordonnées d'un client pour des fins de prospection sans consentement.
- Ne pas partager les informations d'un client avec un autre courtier sans autorisation.
- Prévenir le client si ses données doivent être transmises à un fournisseur externe.
- Ne pas utiliser les données d'un client pour des sondages internes sans consentement.
- Ne pas conserver les photos de propriétés avec des données personnelles visibles (ex. factures sur une table).
- Ne pas publier sur les réseaux sociaux des documents ou extraits contenant des données privées.

## Chapitre 4 – Fournisseurs et partenaires

- Vérifier que les fournisseurs (signature électronique, hébergement, CRM) respectent la Loi 25.
- Signer des ententes écrites avec les sous-traitants confirmant la protection des données.
- Ne pas transmettre de documents sensibles à un fournisseur sans chiffrement.
- Vérifier régulièrement la conformité des outils utilisés (CRM, plateformes de transaction).
- Ne pas partager les données clients avec des partenaires commerciaux sans consentement.
- Exiger des fournisseurs un engagement écrit sur la confidentialité.

- Ne pas stocker les données sur des serveurs hors Québec sans évaluation des facteurs relatifs à la vie privé (ÉFVP).
- Ne pas utiliser de services de traduction automatique pour des documents sensibles.
- Ne pas transmettre de données par fax non sécurisé.
- Ne pas confier la destruction des documents à un tiers sans contrat écrit.

## Chapitre 5 – Prévention et gestion des incidents

- Tenir un registre des incidents de confidentialité et le mettre à jour en cas de problème (délégué à l'agence).
- Préparer un modèle de communication pour informer rapidement un client en cas de fuite de données (délégué à l'agence).
- Tester régulièrement le plan de réponse aux incidents (simulation de perte ou piratage).
- Former les collaborateurs à reconnaître les tentatives de phishing.
- Ne pas minimiser une perte de document, la consigner dans le registre.
- Ne pas attendre pour informer un client si ses données sont compromises.
- Ne pas conserver un incident confidentiel "sous silence" : obligation de déclaration.
- Ne pas utiliser un ordinateur infecté sans l'avoir nettoyé.
- Ne pas réutiliser un mot de passe compromis.
- Ne pas remettre en circulation un document détruit de manière incomplète.
- Ne pas négliger les sauvegardes régulières pour éviter la perte de données.
- Ne pas ignorer les mises à jour de sécurité des logiciels.
- Ne pas laisser un stagiaire ou collaborateur non formé manipuler des données sensibles.
- Ne pas oublier de consigner les mesures correctives prises après un incident.