TI ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est un enjeu de conformité particulièrement important lors de l'utilisation des technologies de l'information (TI). Vous devez donc prendre les mesures nécessaires pour éviter l'accès indu aux données de vos clients. Certaines relèvent de vous, d'autres des gestionnaires de votre cabinet ou courtier ou du responsable des services informatiques, le cas échéant, auquel vous devriez vous adresser au besoin.

MESURES

MESURES PHYSIQUES

- Verrouillez les portes où se trouvent les ordinateurs, appareils informatiques et serveurs. Verrouillez les classeurs et sécurisez l'accès à tous les médias (CD, clé USB, cassettes de sauvegarde, etc.).

MESURES TECHNOLOGIQUES

- Éteignez les postes de travail ou activez la mise en veille automatique.
- Utilisez un mot de passe pour les ordinateurs, cellulaires, tablettes, portables et clés USB.
- Programmez la déconnexion des séances inactives.
- Utilisez un antivirus mis à jour automatiquement sur une base régulière.
- Utilisez un pare-feu.
- Programmez la mise à jour automatique des logiciels pour vous assurer d'avoir les dernières versions et de bénéficier des mises à jour de sécurité.
- Assurez-vous que les connexions Bluetooth sont désactivées.
- N'ouvrez pas les pièces jointes de courriels qui vous semblent louches ou dont vous ignorez l'identité de l'émetteur. Même si vous avez un antivirus à jour, il y a un risque qu'un nouveau virus se cache dans une pièce jointe. Supprimez-les.
- Évitez tout partage (DVD, CD, partage d'écran, de fichiers, d'imprimantes, de session ou gestion à distance, par Internet ou par Bluetooth). Ne cochez pas la case « Partage » pour ces services, à moins de nécessité précise. Dans ce dernier

cas, décochez la case aussitôt le partage fait. Les pirates informatiques entrent généralement dans les systèmes de cette manière.

CHIFFREMENT

- Chiffrez les données confidentielles sur les ordinateurs, les portables et les médias amovibles, telles les clés USB. À ce sujet, notez que les données des iPhone et iPad sont chiffrées, de même que celles des appareils Android récents. Le chiffrement sur les appareils plus anciens doit toutefois être programmé. Les ordinateurs Mac offrent des fonctionnalités de chiffrement des données sur le disque.
- Programmez vos appareils pour utiliser une connexion SSL (un protocole de sécurisation des échanges Internet).
- Programmez sur vos appareils le chiffrement des données avant l'envoi.

DANS LES DÉPLACEMENTS

- Ne discutez pas d'une affaire d'un client au téléphone dans un endroit public.
- Ne prêtez votre matériel informatique, utilisé pour des fins professionnelles, qu'à des personnes autorisées.
- Ne laissez pas votre portable, tablette ou téléphone cellulaire sans surveillance, dans une voiture ou dans un lieu public.
- Évitez d'utiliser un ordinateur public ou celui d'un tiers. Et si vous devez le faire :
    - Utilisez une connexion VPN pour vous connecter de façon sécuritaire à votre ordinateur professionnel à distance.
    - Effacez vos traces : documents téléchargés (incluant les documents imprimés, qui sont nécessairement téléchargés), fichiers Internet temporaires, mots de passe, etc.

L'INFONUAGIQUE

- Privilégiez les nuages composés de serveurs situés uniquement en sol canadien et sous le contrôle d'entités canadiennes. Notez qu'en ce qui concerne les renseignements confidentiels hébergés sur des sites infonuagiques étrangers, le problème tient au fait qu'ils sont soumis à la juridiction du pays hôte plutôt qu'aux lois québécoises et pourraient ainsi s'en trouver moins bien protégés.
- À défaut de faire affaire avec une entité canadienne, chiffrez les données à la source.

- Procédez régulièrement à des sauvegardes automatiques des données et conservez une copie de sauvegarde de toute information hébergée dans le nuage afin d'assurer la disponibilité de cette information en cas de panne ou de différend avec le fournisseur de services infonuagiques.

Pour des informations et des conseils sur le bureau à distance et l'infonuagique, consultez les fiches d'informations suivantes publiées par la Commission d'accès à l'information :

- L'infonuagique (ou « cloud computing »)
- La destruction des documents contenant des renseignements personnels

AU SUJET DE LA NUMÉRISATION

- Conservez l'information numérisée des clients de façon sécuritaire.
- Ne partagez pas votre mot de passe avec qui que ce soit.
- Il est préférable de faire affaire avec des salariés ou des contractuels pour effectuer la numérisation de vos dossiers clients et de leur faire signer au préalable un engagement de confidentialité.
- Vous pouvez également faire appel à une firme spécialisée en numérisation documentaire et en gestion de la clientèle dont les serveurs sont idéalement situés au Québec.
- Pour chaque document numérisé, conservez certaines informations sur papier ou sous forme de métadonnées ajoutées automatiquement au fichier lors de la numérisation, si votre numériseur le permet. Ces informations doivent être conservées tout au long du cycle de vie du document.
    - Identification de l'appareil ayant servi à la numérisation.
    - Identification du logiciel ayant servi à la numérisation.
    - Identification du serveur où ont été transférées les données.
    - Les garanties du fabricant quant à la préservation de l'intégrité des données lors du transfert entre le document source et le document numérique.

ENTENTES AVEC LES FOURNISSEURS

- Révisez attentivement les ententes signées avec les fournisseurs de services informatiques (photocopieurs, télécopieurs, services d'hébergement des données, accès Internet, services infonuagiques, etc.), car comme représentant, vous êtes responsable de l'information personnelle que vous leur transmettez.
- Ne permettez pas à des tiers ou à des fournisseurs de services d'accéder aux informations de vos systèmes informatiques sans vérifier leur probité, et sans

leur faire signer au préalable une entente de confidentialité portant sur les renseignements personnels.
- Envisagez la possibilité d'avoir recours à des solutions clé en main conçues pour les professionnels des services financiers si vous n'avez pas les connaissances requises pour mettre vous-même en place les mesures de protection appropriées de vos dossiers clients. Vous pourriez profiter d'économies d'échelle à cet égard.

LORS D'UN RISQUE RÉEL DE PRÉJUDICE

En présence d'un risque réel de préjudice, vous devrez peut-être aviser les victimes, la police, la Commission d'accès à l'information (CAI) et d'autres intervenants, si nécessaire. Tout d'abord, consultez le département de conformité de votre cabinet ou courtier, le cas échéant. Ceux-ci ont sans doute mis en place des politiques et procédures à cet égard. Si vous n'avez pas accès à un tel service, vous devez tout de même mettre de l'avant certaines mesures. À cet effet, n'hésitez pas à consulter les guides et directives de la CAI :

- Pour informer la Commission, utilisez le Rapport de déclaration d'un incident de sécurité portant atteinte à des renseignements personnels.
- Vous pouvez également consulter l'aide-mémoire à l'intention des organismes et des entreprises – Que faire en cas de perte ou de vol de renseignements personnels? publié par la Commission d'accès à l'information.
- Pour soutenir vos clients victimes d'une perte ou d'un vol de renseignements personnels, recommandez-leur de consulter l'aide-mémoire à l'intention de citoyens Perte ou vol de renseignements personnels : comment réagir? publié par la Commission d'accès à l'information.