Plan de gestion des incidents de confidentialité

Table des matières

Procédure de conservation, de destruction et d'anonymisation des renseignements personnels.....2

Procédure de demande d'accès aux renseignements personnels et de traitement des plaintes.....3

Procédure de demande de désindexation et de suppression des renseignements personnels.....6

Procédure de gestion des incidents de sécurité et violations des renseignements personnels.....8

Liste de bonnes pratiques et outils en ligne pour la protection des renseignements personnels.....10

Procédure de conservation, de destruction et d'anonymisation des renseignements personnels

Durée de conservation des dossiers clients : 7 ans

Méthodes de stockage sécurisé

Les renseignements personnels se trouvent aux endroits suivants :

Programme Psylio, messagerie Proton Mail, ordinateur personnel d'Audrey-Anne Lamarre, T.S.

Le degré de sensibilité de chacun de ces lieux de stockage a été établi.

Ces lieux de stockage, qu'ils soient papier ou numérique, sont adéquatement sécurisés.

L'accès à ces lieux de stockage a été restreint à Audrey-Anne Lamarre, T.S..

Destruction des renseignements personnels

Pour les renseignements personnels sur papier, ils devront être totalement déchiquetés.

Pour les renseignements personnels numériques, ils devront être totalement supprimés des appareils (ordinateurs, téléphone, tablette, disque dur externe), des serveurs et des outils infonuagiques.

Un calendrier de destruction en fonction de la durée de conservation a été établi pour chaque catégorie de renseignements personnels.

Il faudra s'assurer que la destruction est réalisée de manière à ce que les renseignements personnels ne puissent pas être récupérés ou reconstitués.

Anonymisation des renseignements personnels

L'anonymisation des renseignements personnels ne devrait se faire que si l'organisation souhaite les conserver et les utiliser à des fins sérieuses et légitimes.

La méthode d'anonymisation des renseignements personnels choisit est la suivante : effacer toute trace permettant d'identifier le client.

Il faudra s'assurer que l'information restante ne permettre plus de façon irréversible l'identification directe ou indirecte des individus concernés et s'assurer d'évaluer régulièrement le risque de réidentification des données anonymisées en effectuant des tests et des analyses pour garantir leur efficacité.

Attention, à la date de rédaction du présent gabarit, l'anonymisation des renseignements personnels à des fins sérieuses et légitimes n'est pas possible. Un règlement du gouvernement doit être adopté pour déterminer les critères et les modalités.

Procédure de demande d’accès aux renseignements personnels et de traitement des plaintes

Soumission de la demande

L'individu qui souhaite accéder à ses renseignements personnels doit soumettre une demande écrite à Audrey-Anne Lamarre, T.S.. La demande peut être envoyée par courriel ou par courrier postal.

La demande doit clairement indiquer qu'il s'agit d'une demande d'accès aux renseignements personnels, et fournir des informations suffisantes pour identifier l'individu et les renseignements recherchés.

Ces informations peuvent inclure le nom, l'adresse ainsi que toute autre information pertinente pour identifier de manière fiable l'individu qui effectue la demande.

Réception de la demande

Une fois la demande reçue, un accusé de réception est envoyé à l'individu pour confirmer que sa demande a été prise en compte.

La demande devra être traitée dans les trente (30) jours suivant sa réception.

Vérification de l’identité

Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable. Cela peut être fait en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.

Si l'identité ne peut pas être vérifiée de manière satisfaisante, Audrey-Anne Lamarre, T.S. peut refuser de divulguer les renseignements personnels demandés.

Réponse aux demandes incomplètes ou excessives

Si une demande d'accès aux renseignements personnels est incomplète ou excessive, la personne responsable de la protection des renseignements personnels communique avec l'individu pour demander des informations supplémentaires ou clarifications.

Audrey-Anne Lamarre, T.S. se réserve le droit de refuser une demande si elle est manifestement abusive, excessive ou non justifiée.

Traitement de la demande

Une fois l'identité vérifiée, la personne responsable de la protection des renseignements personnels pour traiter les demandes d'accès aux renseignements personnels procède à la collecte des renseignements demandés.

La personne responsable consulte les dossiers pertinents pour recueillir les renseignements personnels demandés, en veillant à respecter les restrictions légales éventuelles.

Examen des renseignements

Avant de communiquer les renseignements personnels à l'individu, la personne responsable examine attentivement les informations pour s'assurer qu'elles ne contiennent pas de renseignements tiers confidentiels ou susceptibles de porter atteinte à d'autres droits.

Si des renseignements de tiers sont présents, la personne responsable évalue s'ils peuvent être dissociés ou s'ils doivent être exclus de la divulgation.

Communication des renseignements

Une fois les vérifications terminées, les renseignements personnels sont communiqués à l'individu dans un délai raisonnable, conformément aux exigences légales en vigueur.

Les renseignements personnels peuvent être communiqués à l'individu par courrier postal sécurisé ou en personne, selon les préférences de l'individu et les mesures de sécurité appropriées.

Suivi et documentation

Toutes les étapes du processus de traitement de la demande d'accès aux renseignements personnels doivent être consignées de manière précise et complète.

Les détails de la demande, les actions entreprises, les décisions prises et les dates correspondantes doivent être enregistrés dans un registre de suivi des demandes d'accès.

- Date de réception de la demande ;
- Date de l’accusé de réception ;
- Date de la vérification de l’identité ;
- Méthode de vérification de l’identité ;
- Décision – demande d’accès acceptée ou refusée ;
- Date de la communication des renseignements (si applicable).

Protection de la confidentialité

Audrey-Anne Lamarre, T.S., seule personne impliquée dans le traitement des demandes d'accès aux renseignements personnels doit respecter la confidentialité et la protection des données.

Gestion des plaintes et des recours

Si un individu est insatisfait de la réponse à sa demande d'accès aux renseignements personnels, il doit être informé des procédures de réclamation et des recours disponibles devant la Commission d'accès à l'information.

Les plaintes doivent être traitées conformément aux politiques et procédures internes en matière de gestion des plaintes (section suivante).

Procédure de traitement des plaintes

Réception des plaintes

Les plaintes peuvent être déposées par écrit, par téléphone, par courrier électronique ou via tout autre canal de communication officiel. Elles doivent être enregistrées dans un registre centralisé, accessible uniquement à Audrey-Anne Lamarre, T.S..

Le référencement du client par Audrey-Anne Lamarre, T.S. à l'Ordre des Travailleurs sociaux et des Thérapeutes conjugaux et familiaux du Québec doit obligatoirement être fait en cas de plainte.

L'Ordre des Travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec a pour mandat de recevoir, d'analyser d'enquêter et de disposer des sanctions jugées en cas de plainte.

Procédure de demande de désindexation et de suppression des renseignements personnels

Réception des demandes

Les demandes de désindexation et de suppression des renseignements personnels doivent être transmises à Audrey-Anne Lamarre, T.S.

Les clients peuvent soumettre leurs demandes par courriel à contact@aalamarre.com ou par téléphone au 819 216-8048.

Vérification de l'identité

Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable.

Cela peut être fait en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.

Si l'identité ne peut pas être vérifiée de manière satisfaisante, Audrey-Anne Lamarre, T.S. peut refuser de donner suite à la demande.

Évaluation des demandes

Audrey-Anne Lamarre, T.S. doit examiner attentivement les demandes et les renseignements personnels concernés pour déterminer leur admissibilité à la désindexation ou à la suppression.

Les demandes doivent être traitées de manière confidentielle et dans le respect des délais prévus.

Raisons d'un refus

Il existe aussi des raisons parfaitement valables pour lesquelles nous pourrions refuser de supprimer ou de désindexer des renseignements personnels :

• Pour continuer à fournir des biens et des services au client ;

• Pour des raisons d'exigence du droit du travail ;

• Pour des raisons juridiques en cas de litige.

Désindexation ou suppression des renseignements personnels

Audrey-Anne Lamarre, T.S. doit prendre les mesures nécessaires pour désindexer ou supprimer les renseignements personnels conformément aux demandes admissibles.

Communication du suivi

Audrey-Anne Lamarre, T.S. est chargée de communiquer avec les demandeurs tout au long du processus, en fournissant des confirmations d'accusé de réception et des mises à jour régulières sur l'état d'avancement de leur demande.

Tout retard ou problème rencontré lors du traitement des demandes doit être communiqué aux demandeurs avec des explications claires.

Suivi et documentation

Toutes les demandes de désindexation et de suppression des renseignements personnels, ainsi que les actions entreprises pour y répondre, doivent être consignées dans un système de suivi dédié.

Les enregistrements doivent inclure les détails des demandes, les mesures prises, les dates et les résultats des actions effectuées.

Procédure de gestion des incidents de sécurité et violations des renseignements personnels

Aperçu

Un plan d'intervention est essentiel pour gérer des cyberincidents de manière efficace. Dans ces moments de crise, on ne sait pas toujours comment agir et prioriser les actions. Un plan d'intervention vient réduire le stress d'oublier des aspects importants.

Objectif

Le but de cette procédure est de s'assurer que l'organisation est prête à intervenir en cas de cyberincident de manière à pouvoir reprendre rapidement ses activités.

Portée

La portée de cette procédure inclut tous les réseaux et systèmes, ainsi que les parties prenantes (clients, partenaires, employés, sous-traitants, fournisseurs) qui accèdent à ces systèmes.

Reconnaître un cyberincident

Un incident de cybersécurité peut ne pas être reconnu ou détecté immédiatement. Toutefois, certains indicateurs peuvent être les signes d'une atteinte à la sécurité, qu'un système a été compromis, d'une activité non autorisée, etc. Il faut toujours être à l'affût de tout signe indiquant qu'un incident de sécurité s'est produit ou est en cours. Certains de ces indicateurs sont décrits ci-dessous :

1. Activité excessive ou inhabituelle de la connexion et du système, notamment à partir de tout identifiant d'utilisateur (compte d'utilisateur) inactif.

2. Accès distant excessif ou inhabituel dans votre organisation. Cela peut concerner le personnel ou des fournisseurs tiers.

3. L'apparition de tout nouveau réseau sans fil (Wi-Fi) visible ou accessible.

4. Une activité inhabituelle liée à la présence de logiciels malveillants, de fichiers suspects ou de fichiers et programmes exécutables nouveaux ou non approuvés.

5. Ordinateurs ou appareils perdus, volés ou égarés qui contiennent des données de cartes de paiement, renseignements personnels ou d'autres données sensibles.

Coordonnées des personnes-ressources

Rôle : Travailleuse sociale, responsable de la protection des renseignements personnels
Nom : Audrey-Anne Lamarre
Téléphone : 819 216-8048
Adresse de courriel : contact@aalamarre.com

Assureur en cybersécurité : Beazley Canada Limited
Téléphone : (844) 778-5950
Courriel : claims.canada@beazley.com

Atteinte à la protection des renseignements personnels – Intervention spécifique

S'il a été confirmé qu'un incident de sécurité lié à une atteinte à la protection des renseignements personnels s'est produit, il faudra effectuer les étapes suivantes :

♦ Compléter le registre d'incidents de confidentialité pour documenter l'incident.

♦ Examiner l'atteinte à la protection des renseignements personnels pour déterminer si des renseignements personnels ont été perdus en raison d'un accès ou utilisation non autorisés, d'une divulgation non autorisée ou de toute atteinte la protection de ces renseignements personnels et qu'il existe un risque de préjudice sérieux pour les personnes concernées. Dans un tel cas, le signaler à la Commission de l'accès à l'information au Québec. Et, le signaler également aux personnes dont les renseignements personnels sont visés par l'incident.

Rançongiciel – Intervention spécifique

S'il a été confirmé qu'un incident de sécurité de rançongiciel s'est produit, il faudra effectuer les étapes suivantes :

♦ Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.

♦ Ne RIEN EFFACER sur de vos appareils (ordinateurs, serveurs, etc.).

♦ Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera à comprendre comment l'éliminer.

♦ Communiquer avec les autorités locales pour signaler l'incident et coopérer à l'enquête.

♦ Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d'un antivirus, d'un anti-maliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil.

♦ Si le rançongiciel ne peut pas être supprimé de l'appareil (souvent le cas avec les programmes malveillants furtifs), l'appareil doit être réinitialisé au moyen des supports ou des images d'installation d'origine. Avant de procéder à la réinitialisation à partir de supports/ images de sauvegarde, vérifier qu'ils ne sont pas infectés par des maliciels.

♦ Si les données sont critiques et doivent être restaurées, mais ne peuvent être récupérées à partir de sauvegardes non affectées, rechercher les outils de déchiffrement disponibles sur nomoreransom.org.

♦ La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Il est également fortement recommandé de faire appel aux services d'un chef de projet expert en cyberattaques (breach coach).

♦ Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.

Liste de bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Utilisez des mots de passe forts : Utilisez des mots de passe comportant entre 16 et 20 caractères, composé d'une combinaison de lettres, de chiffres et de caractères spéciaux dans vos mots de passe. Évitez d'utiliser des informations personnelles évidentes et utilisez des mots de passe différents pour chaque compte.

Gestionnaires de mots de passe : Utilisez un gestionnaire de mots de passe tel que Dashlane, Bitwarden, NordPass, Keepass ou 1Password pour générer, stocker et gérer vos mots de passe.

Activez l'authentification à deux facteurs : Utilisez des méthodes d'authentification à deux facteurs (2FA) lorsque cela est possible. Cela ajoute une couche de sécurité supplémentaire en demandant une deuxième preuve d'identité lors de la connexion.

Méfiez-vous des messages suspects : Soyez vigilant avec les courriels, les messages instantanés et les appels téléphoniques non sollicités demandant des informations personnelles. Ne cliquez pas sur les liens suspects et n'ouvrez pas les pièces jointes sources inconnues.

Mettez à jour régulièrement vos logiciels : Maintenez vos systèmes d'exploitation, vos applications et vos antivirus à jour en installant les dernières mises à jour et correctifs de sécurité. Les mises à jour contiennent souvent des correctifs pour les vulnérabilités connues. Une gestion proactive des mises à jour OS et matérielles limitent de beaucoup les risques de sécurité.

Limitez les informations personnelles partagées en ligne : Évitez de publier des informations personnelles sensibles, telles que votre adresse, votre numéro de téléphone ou vos détails financiers, sur les réseaux sociaux ou d'autres plateformes en ligne.

Utilisez des réseaux Wi-Fi sécurisés : Évitez de vous connecter à des réseaux Wi-Fi publics pour effectuer des transactions sensibles ou accéder à des informations confidentielles. Privilégiez les réseaux Wi-Fi protégés par mot de passe ou utilisez un VPN en (presque) tout temps.

Suppression des cookies : Utilisez les outils de nettoyage du système d'exploitation pour supprimer les cookies de suivi et les données de navigation stockées sur vos appareils.

VPN (Virtual Private Network) : Utilisez un VPN pour chiffrer votre connexion Internet et protéger votre vie privée en ligne. Des services populaires tels que NordLayer, ExpressVPN ou CyberGhost offrent des fonctionnalités de protection de la vie privée.

Extensions de navigateur de confidentialité : Installez des extensions de navigateur telles que Privacy Badger, uBlock Origin ou HTTPS Everywhere pour bloquer les traqueurs publicitaires, les publicités intrusives et forcer les connexions sécurisées.

Chiffrement des communications : Utilisez des services de messagerie et de communication chiffrés, tels que Signal, WhatsApp (avec le chiffrement de bout en bout activé) ou Telegram (avec le chat secret activé), pour protéger la confidentialité de vos conversations.

Soyez prudent avec les informations de paiement en ligne : Lorsque vous effectuez des achats en ligne, assurez-vous de le faire sur des sites sécurisés et fiables. Vérifiez la présence d'un cadenas dans la barre d'adresse et utilisez des méthodes de paiement sécurisées, telles que PayPal ou les cartes de crédit protégées.

Chiffrement des fichiers : Utilisez des outils de chiffrement pour protéger vos fichiers sensibles. Des logiciels tels que VeraCrypt, AxCrypt ou BitLocker vous permettent de créer des conteneurs chiffrés ou de crypter des fichiers individuels.

Navigation privée : Utilisez le mode de navigation privée ou incognito de votre navigateur pour limiter la collecte de données et de cookies pendant vos sessions de navigation. Cela empêche également l'enregistrement de votre historique de navigation.

Vérification des paramètres de confidentialité : Passez en revue et ajustez les paramètres de confidentialité de vos comptes en ligne, tels que les réseaux sociaux, les services de messagerie et les applications, pour limiter la quantité d'informations personnelles partagées et restreindre l'accès à vos données.

Suppression des données personnelles : Supprimez régulièrement les données personnelles inutiles ou sensibles stockées sur vos appareils, tels que les anciens courriels, les fichiers temporaires, les caches de navigateur et les historiques de recherche.

Formation à la sensibilisation à la cybersécurité : Familiarisez-vous avec les meilleures pratiques de cybersécurité en suivant des cours en ligne, en lisant des ressources fiables et en restant informé des dernières menaces et techniques d'attaque.