ACCÈS TRAVAIL PORTNEUF

POLITIQUE DE CONFIDENTIALITÉ ET DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Adoptée le 9 avril 2025

TABLE DES MATIÈRES

Mise en contexte

Dans la foulée de l'adoption de la Loi 25, adoptée par le Gouvernement du Québec en 2021, Accès Travail Portneuf s'est doté de la présente politique qui traite de la confidentialité et du traitement accordé aux renseignements personnels. Il s'agit notamment du traitement des informations concernant les employé.e.s, les membres du conseil d'administration et les membres (s'il y a lieu), la clientèle, les fournisseurs et toute autre information jugée sensible en lien avec nos activités.

Objectifs de la politique

- ✓ S'assurer de la conformité d'Accès Travail Portneuf quant aux exigences légales en matière d'accès à l'information, de confidentialité et de protection des renseignements personnels.

- ✓ Assurer le respect de la vie privée des personnes et la sécurité des informations personnelles.

- ✓ Informer le personnel et les membres du conseil d'administration concernant les mesures et procédures adoptées par Accès Travail Portneuf dans le cadre de la confidentialité et du respect des renseignements personnels.

- ✓ Se donner des balises concernant les échanges d'information de l'organisme tant à l'interne qu'à l'externe.

Collecte et utilisation de renseignements personnels

Seules les informations nécessaires pour offrir nos services et la meilleure expérience de navigation sont collectées. Nous n'échangeons pas, ne vendons pas, ne louons pas ni ne cédons les renseignements personnels.

Nous recueillons, utilisons et conservons les renseignements personnels dans le but de nous conformer aux exigences des entités gouvernementales (ministère de l'Immigration, de l'Intégration et de la Francisation, ministère de l'Emploi et de la Solidarité sociale et ministère de la Santé et des Services sociaux) qui subventionnent les services que nous offrons. Certaines informations personnelles telles que les noms, numéros de téléphone, adresses courriel et profils de réseaux sociaux sont aussi recueillies pour faciliter la transmission d'information concernant nos services et activités.

Afin d'offrir nos prestations de services, nous concluons des ententes avec des partenaires (hébergeurs de sites Web, gestionnaires de plateformes de données, etc.) qui ont accès à nos bases de données. Il se peut aussi que des données soient hébergées hors Québec. Ces tiers sont également soumis au cadre juridique en matière de renseignements personnels et de la vie privée.

Données relatives aux visites sur le site web

Nous utilisons des cookies pour améliorer l'expérience de navigation et pour mieux comprendre comment notre site web est utilisé. Les cookies sont de petits fichiers qui sont stockés sur l'ordinateur servant à visiter notre site web. Ils contiennent des informations telles que la langue d'affichage et certaines habitudes de navigation. Les informations recueillies par les cookies sont confidentielles en tout temps. Les cookies peuvent être désactivés ou bloqués en configurant les paramètres des navigateurs.

Conservation et destruction des renseignements personnels

Nous conserverons les informations personnelles aussi longtemps que nécessaire pour mener à bien notre prestation de services à l'égard de la clientèle et pour répondre aux exigences de nos redditions de comptes tout en respectant les lois en vigueur.

Un calendrier de conservation des documents pour se conformer aux lois sur la protection des renseignements personnels et prévenir les incidents de confidentialité a été mis en place. Le calendrier couvre l'ensemble du cycle de vie des renseignements personnels recueillis par Accès Travail Portneuf.

Définitions

Renseignements personnels : toute information permettant d'identifier, directement ou indirectement, une personne physique.

Conservation : stockage sécurisé des renseignements personnels pendant la durée requise.

Destruction : suppression, élimination ou effacement définitif des renseignements personnels.

Calendrier de conservation des renseignements personnels

Durée de conservation

Renseignements personnels concernant les employés : 7 ans après la fin de l'emploi
Membres du CA : 7 ans après la fin du mandat
Membres : à la fin du membership
Clients : 5 ans après la dernière intervention
Fournisseurs de services : suppression des fournisseurs inactifs aux 2 ans

Méthodes de stockage sécurisé

Employés : Plateforme sécurisée avec 2FA, dans Office les documents avec renseignements personnels sont chiffrés avec mot de passe, version papier dans classeurs barrés
Membres du CA : Liste chiffrée avec mot de passe dans Office, version papier dans classeurs barrés
Membres : Liste chiffrée avec mot de passe dans Office, version papier dans classeurs barrés
Clients : Plateforme sécurisée avec 2FA (LGEstat et SIP), dans Office les documents avec renseignements personnels sont chiffrés avec mot de passe, version papier dans classeurs barrés
Fournisseurs de services : Plateforme sécurisée avec 2FA, dans Office les documents avec renseignements personnels sont chiffrés avec mot de passe

Destruction

À la fin de leur durée de vie, les documents papier sont déchiquetés par une firme offrant un service sécurisé et les documents numériques sont supprimés des bases de données et des ordinateurs.

Incident de confidentialité

Tout incident de confidentialité doit être consigné par écrit sur le formulaire « Registre des incidents » auquel tous les employé.e.s ont accès et la responsable de la protection des renseignements personnels doit en être informée.

La responsable de la protection des renseignements personnels analyse ensuite la nature de l'incident et décide si la Commission d'accès à l'information ou toute autre autorité doit en être avisée.

Suivi d'un incident

Lorsqu'un préjudice important et sérieux est susceptible de se produire, Accès Travail Portneuf :

- ✓ avisera rapidement la Commission d'accès à l'information, même si l'ensemble des informations relatives à l'incident ne sont pas colligés, et remplira la déclaration par la suite;
- ✓ avisera toute personne dont un renseignement personnel est concerné par l'incident, à moins que cet avis ne soit susceptible d'entraver une enquête[1];

- ✓ avisera toute personne ou tout organisme susceptible de diminuer ce risque.

[1] Un délai peut s'appliquer entre le moment où l'organisation prend connaissance de l'incident et celui où il en avise les personnes concernées. Ce délai peut être nécessaire afin, par exemple, d'identifier les renseignements personnels impliqués, les personnes concernées, la faille de sécurité et pour colmater celle-ci ou pour éviter d'entraver une enquête en cours.

Interventions spécifiques

Rançongiciel

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

- ✓ Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.
- ✓ Ne rien effacer sur vos appareils (ordinateurs, serveurs, etc.).
- ✓ Communiquer avec *Topologic* (compagnie qui gère notre parc informatique et nos licences Microsoft) afin qu’ils nous donnent la marche à suivre pour régler la situation.
- ✓ 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.
- ✓ La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Au besoin, faire appel aux services d’un expert en cyberattaques.
- ✓ Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs pour empêcher toute nouvelle attaque.

Piratage de compte

S’il a été confirmé qu'un piratage de compte s'est produit, il faut effectuer les étapes suivantes :

- ✓ Aviser nos clients et fournisseurs qu’ils pourraient recevoir des courriels frauduleux de notre part et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels.
- ✓ Vérifier si on a encore accès au compte en ligne.
- ✓ Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l’accès.
- ✓ Changer le mot de passe utilisé pour se connecter à la plateforme.
- ✓ Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.
- ✓ Activer le double facteur d’authentification pour la plateforme.
- ✓ Supprimer les connexions et les appareils non légitimes de l’historique de connexion.

Demande d’accès aux renseignements personnels

Une personne peut demander à accéder aux renseignements personnels qu’Accès Travail Portneuf détient sur elle. Toutes les demandes d’accès sont traitées de manière confidentielle, rapide et précise, tout en respectant le droit des individus concernés.

Procédure de demande d’accès

La personne qui désire accéder à ses renseignements personnels doit déposer une demande écrite à la responsable de la protection des renseignements personnels de l’organisation. La demande peut être envoyée par courriel, par téléphone 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.

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 ouvrables suivant sa réception.

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, l'organisation peut refuser de divulguer les renseignements personnels demandés.

Si une demande d'accès aux renseignements personnels est incomplète ou excessive, le responsable de la protection des renseignements personnels communique avec l'individu pour demander des informations supplémentaires ou clarifications. L'organisation se réserve le droit de refuser une demande si elle est manifestement abusive, excessive ou non justifiée.

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

Avant de communiquer les renseignements personnels à l'individu, la 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 responsable évalue s'ils peuvent être dissociés ou s'ils doivent être exclus de la divulgation.

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 voie électronique 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.

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)

Tout le personnel impliqué dans le traitement des demandes d'accès aux renseignements personnels doit respecter la confidentialité et la protection des données.

Suppression des renseignements personnels à la suite d'une demande spécifique

Le but de cette procédure est de fournir un mécanisme structuré pour gérer les demandes de suppression des renseignements personnels sur nos plateformes si un client en fait une demande spécifique.

Les clients peuvent soumettre leurs demandes par courriel ou par courrier postal. 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, l'organisation peut refuser de donner suite à la demande.

La demande doit être traitée de manière confidentielle et dans le respect des délais prévus. Elle devra être traitée dans les trente (30) jours ouvrables suivant sa réception.

Raisons d'un refus

Il existe aussi des raisons parfaitement valables pour lesquelles Accès Travail Portneuf pourrait refuser de supprimer des renseignements personnels :

- Pour assurer la reddition de comptes;
- Pour des raisons d'exigence du droit du travail;
- Pour des raisons juridiques en cas de litige.

Suppression des renseignements personnels

Les mesures nécessaires pour supprimer les renseignements personnels conformément aux demandes admissibles doivent être prises en charge par la responsable de la protection des renseignements personnels.

Suivi et documentation

Toutes les demandes de suppression de renseignements personnels, ainsi que les actions entreprises pour y répondre, doivent être consignées.

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

Procédures à l'embauche et au départ d'un.e employé.e

Embauche

Avant de fournir un accès aux appareils et systèmes ainsi qu'aux différentes plateformes et aux comptes d'Accès Travail Portneuf, l'employé.e nouvellement embauché.e est rencontré.e par un membre de l'administration qui lui fait part verbalement des consignes de sécurité à adopter. La personne doit aussi prendre connaissance et signer la politique et les ententes de confidentialité liée à son mandat.

Départ

Lors du départ d'un.e employé.e (congé sans solde, maladie prolongée, mise à pied temporaire ou fin d'emploi), tous ses accès aux plateformes et aux comptes sont désactivés, son adresse courriel et son numéro de téléphone (s'il y lieu) sont transférés à un collègue ou à un membre de la direction. Tous les équipements appartenant à Accès Travail Portneuf (ordinateur, téléphone, etc.) sont remis au dernier jour travaillé. De plus, la personne signe une entente à l'effet qu'elle s'engage à n'entretenir aucun contact avec la clientèle d'Accès Travail Portneuf pour éviter les bris de confidentialité. Dans cette entente, elle s'engage aussi à avoir remis l'ensemble des biens et données appartenant à Accès Travail Portneuf (incluant les données sur ses appareils personnels s'il y a lieu) et n'avoir fait aucune copie de ces données.