CSMO Habitation

Comité sectoriel de main-d'œuvre de l'habitation

Politique de confidentialité et de gestion des renseignements personnels

Mise à jour : 5 mars 2024

Sommaire :

Politique de confidentialité et de gestion des renseignements des sites internet du Comité sectoriel de main-d'œuvre de l'habitation. Le CSMO est un organisme à but non lucratif qui est financé par Services Québec selon la Politique de l'intervention sectorielle définie par la Commission des partenaires du marché du travail.

Mise à jour : 5 mars 2024.

Le Comité sectoriel de main-d'œuvre de l'habitation est engagé à protéger la confidentialité de vos données et à nous conformer à la loi 25 du Québec sur la protection des renseignements personnels. Cette politique de confidentialité explique comment nous collectons, utilisons, divulguons et protégeons vos informations. En utilisant nos sites web (Clicemplois.net, SolutionsRH.net) ou nos services, vous consentez à cette politique de confidentialité.

1. Collecte de données personnelles

Nous collectons des données personnelles lorsque vous interagissez avec notre site web ou nos services. Les données collectées peuvent inclure des informations de contact (nom, adresse électronique, numéro de téléphone), des informations professionnelles et des informations de navigation.

2. Utilisation des données personnelles

Nous utilisons vos données personnelles dans le but de vous fournir nos services, de répondre à vos demandes, de personnaliser votre expérience, d'améliorer notre site web et nos services, et de vous informer des mises à jour ou offres pertinentes liées à nos services.

3. Divulgation des données personnelles

Nous ne divulguons pas vos données personnelles à des tiers sans votre consentement.

4. Protection des données personnelles

Nous mettons en place des mesures de sécurité pour protéger vos données personnelles contre tout accès non autorisé, divulgation, altération ou destruction. Vos informations sont stockées en toute sécurité sur des serveurs protégés.

5. Accès et contrôle de vos données personnelles

Vous avez le droit d'accéder à vos données personnelles, de les corriger ou de les supprimer. Vous pouvez également exercer votre droit de retrait de consentement en contactant Joëlle Mc Gurrin, conseillère en communication et en marketing, à jmcgurrin@csmohabitation.com. Nous nous engageons à répondre rapidement à vos demandes.

6. Durée de conservation des données

Nous conservons vos données personnelles aussi longtemps que nécessaire pour maintenir avec vous notre prestation de services ou pour réaliser nos mandats de connaissance du marché du travail.

7. Cookies et technologies similaires

Nous utilisons des cookies et des technologies similaires pour améliorer votre expérience sur notre site web. Vous pouvez gérer l'utilisation des cookies au moyen des paramètres de votre navigateur.

8. Modifications de la politique de confidentialité

De temps à autre, nous pouvons mettre à jour cette politique de confidentialité pour refléter les changements dans nos pratiques. La date de la dernière mise à jour sera indiquée au haut de la politique de confidentialité.

9. Contactez-nous

Si vous avez des questions ou des préoccupations concernant notre politique de confidentialité ou la protection de vos données personnelles, veuillez nous contacter à jmcgurrin@csmohabitation.com.

Le Comité sectoriel de main-d'œuvre de l'habitation est déterminé à maintenir la confidentialité et la sécurité de vos données personnelles en conformité avec la loi 25 du Québec. Nous vous remercions de votre confiance en nos services.

CSMO Habitation

Comité sectoriel de main-d'œuvre de l'habitation

Politique de confidentialité et de gestion des renseignements personnels

Politique de confidentialité et de gestion des renseignements personnels

TABLE DES MATIÈRES

Avant-propos

La présente politique traite de la gestion et de la protection des informations personnelles à l'intérieur et à l'extérieur du Comité sectoriel de main-d'œuvre de l'habitation. Elle traite notamment des renseignements concernant les informations liées aux activités de l'organisme et des informations concernant la clientèle et des membres du personnel.

Elle s'applique aux relations entre toute personne : membres du personnel, clientèle et partenaires.

Elle poursuit les objectifs suivants :
Assurer le respect de la vie privée des personnes et la sécurité des informations personnelles détenues par le Comité sectoriel de main-d'œuvre de l'habitation.

1. Mission et valeurs de l’organisme

Le Comité sectoriel de main-d’œuvre (CSMO) fait la promotion de l’emploi dans l’industrie. Il assure la veille des besoins du marché du travail touchant l’évolution des compétences des métiers actuels et futurs. Il participe à l’adaptation des programmes de formation dans le réseau scolaire, à l’adaptation du programme d’apprentissage en milieu de travail (PAMT), et contribue au perfectionnement de la main-d’œuvre en emploi, ce qui contribue à orienter les mesures gouvernementales.

Avec ses partenaires, le CSMO propose aux manufacturiers des outils, des ressources et des solutions pouvant répondre aux préoccupations d’attraction, de recrutement, de rétention, d’adaptation de la main-d’œuvre, de formation et de gestion RH.

2. Nos ressources

Le Comité sectoriel publie une panoplie d’activités de formation qui sont disponibles en ligne ou en présentiel, que ce soit pour accompagner le transfert des connaissances par une formation de compagnon, la gestion des ressources humaines par une formation de contremaître, l’intégration de nouvelles technologies par le développement des compétences numériques ou des compétences spécifiques. Notre secteur compte plus de 1400 entreprises et près de 45 000 travailleurs.

Nous proposons des outils pour l’intégration des personnes immigrantes, des programmes d’apprentissage en milieu de travail, l’intégration des jeunes avec des programmes d’études en alternance travail-études dont les salaires sont subventionnés.

3. Définitions

Les données personnelles se définissent comme toute information se rapportant à une personne physique identifiée ou identifiable. Une personne est considérée comme identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un identifiant comme un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Pour limiter toute ambiguïté, nous avons convenu avec cette politique de ne plus recueillir des informations personnelles qui touchent les adresses domiciliaires, les dates de naissance et les numéros de sécurité sociale. Toutefois, les autres informations recueillies, seules ou combinées avec d’autres, peuvent être utilisées pour identifier une personne. Cela inclut, mais n’est pas limité à, des éléments tels que les adresses courriel,

les numéros de téléphone au travail, les adresses du lieu de travail ou les informations de localisation rattachées au travail. Ces données sont souvent au cœur des réglementations en matière de protection de la vie privée et de sécurité des données.

4. Engagements du Comité sectoriel de main-d'œuvre de l'habitation

Le Comité sectoriel de main-d'œuvre de l'habitation s'engage à :

- Mettre en place des mécanismes afin de protéger les informations confidentielles, au moyen de mots de passe complexes et de doubles authentifications lors de connexion sur une application ou autres;
- Assurer le traitement confidentiel des plaintes en recueillant les informations sur un registre Excel sécurisé;
- Recueillir seulement les données nécessaires ou utiles au Comité;
- Appliquer la politique de confidentialité et de télétravail (voir en annexe) dans le respect des valeurs du Comité sectoriel de main-d'œuvre de l'habitation.
- De tenir un registre en cas d'incidents de confidentialité, afin de limiter les risques, évaluer les préjudices possibles et, dans certains cas, en aviser la Commission et les personnes concernées.

5. Normes au sein du Comité sectoriel de main-d'œuvre de l'habitation

Toute personne qui, au sein du Comité sectoriel de main-d'œuvre de l'habitation, a des échanges qui ne sont pas liés à l'exercice de ses fonctions doit agir avec discrétion. De ce fait, elle doit :

- Respecter la vie privée des personnes;
- Ne pas divulguer l'information confidentielle obtenue au sein de l'organisme;
- Savoir garder les informations sensibles des personnes qui se confient;
- Agir selon les missions de l'organisme.

6. Normes

6.1 Échanges d'informations à l'extérieur du Comité sectoriel de main-d'œuvre de l'habitation

Le conseil d'administration, la direction et les employés ne doivent pas discuter de dossiers, de personnes ou de décisions propres au Comité sectoriel de main-d'œuvre de l'habitation avec des personnes extérieures ou non concernées, sauf si cela est nécessaire pour réaliser une intervention. Dans une telle situation, ils doivent :

- S'assurer de l'identité de la personne, qu'elle respecte les normes du Comité;
- Limiter les échanges d'informations au strict minimum;

- S’assurer du consentement de la personne (au moyen de formulaires).

6.2 Échanges d’informations à l’intérieur du Comité sectoriel de main-d’œuvre de l’habitation

Se référer aux politiques de télétravail signées lors de l’embauche d’un salarié.

6.3 Mesures de sécurité pour limiter l’accès à l’information

Ordinateurs et autres :

- Verrouiller les écrans d’ordinateur à l’heure du dîner ou en cas d’absence;
- Mettre en place des mots de passe complexes sur les comptes du Comité;
- Mettre en place la double authentification sur les comptes des membres du Comité.

6.4 Procédures de conservation et de destruction des dossiers confidentiels

Conserver les dossiers fermés en un lieu sûr dans le respect des normes du Comité sectoriel de main-d’œuvre de l’habitation.

Selon la gestion des dossiers de subvention, nous devons conserver durant sept ans, aux fins de conformité de vérification administrative, les documents qui pourraient inclure des données personnelles.

Chaque année, le responsable de la cybersécurité doit vérifier s’il n’y a pas une nouvelle base de données mise en place. Le cas échéant, il doit l’inscrire dans le tableau Excel (actif informationnel).

Procédures d’accès :

1. Les employés doivent soumettre une demande d’accès aux données personnelles à leur supérieur hiérarchique ou au responsable désigné.
2. La demande doit spécifier la raison justifiant l’accès aux données personnelles et la finalité du traitement.
3. Le responsable désigné examine chaque demande d’accès et évalue sa justification en fonction des besoins professionnels de l’employé.

Critères d'accès :

1. Les rôles et les responsabilités des employés doivent être clairement définis, en précisant les catégories de données personnelles auxquelles ils peuvent accéder.
2. L'accès est basé sur le principe du « besoin de savoir », c'est-à-dire que les employés ne doivent avoir accès qu'aux données personnelles rattachées aux activités professionnelles nécessaires à l'exécution de leurs tâches.

Processus d'approbation et de révocation des accès :

1. Toute demande d'accès doit être approuvée par le responsable désigné ou par une autorité compétente en matière de protection des données.
2. L'approbation est basée sur la justification de la demande, la conformité aux politiques de protection des données et la pertinence de l'accès demandé.
3. Les accès sont réévalués de manière trimestrielle pour s'assurer de leur pertinence continue. Les autorisations d'accès peuvent être révoquées si elles ne sont plus nécessaires ou si les responsabilités de l'employé changent.

Sécurité et confidentialité :

1. Les employés ayant accès aux données personnelles doivent respecter les mesures de sécurité et de confidentialité établies par l'entreprise.
2. Les informations d'identification (identifiants, mots de passe, etc.) doivent être protégées et ne doivent pas être partagées avec des tiers.
3. Les employés doivent être formés sur les bonnes pratiques de sécurité et de confidentialité des données personnelles.

Un incident de confidentialité peut être défini comme tout événement ou incident qui compromet la confidentialité, l'intégrité ou la disponibilité des données personnelles. Voici quelques exemples d'incidents de confidentialité :

1. Accès non autorisé : Tout accès à des données personnelles par une personne ou une entité qui n'est pas autorisée à y accéder. Cela peut inclure les tentatives de piratage, l'utilisation frauduleuse des identifiants d'accès, l'accès physique non autorisé à des dispositifs ou des locaux où les données sont stockées, etc. (faire référence au tableau Excel).
2. Divulgation involontaire : La divulgation accidentelle ou non intentionnelle de données personnelles à des tiers non autorisés. Cela peut se produire par le biais d'erreurs humaines, de courriels ou de documents envoyés à la mauvaise personne, de pertes de supports de stockage contenant des données personnelles, etc.
3. Violation de la sécurité des données : Toute violation de la sécurité des données personnelles qui compromet leur confidentialité, leur intégrité ou leur disponibilité. Cela peut inclure les attaques informatiques, les logiciels malveillants, les violations physiques (vol, destruction), les défaillances techniques, etc.

4. Utilisation abusive des données personnelles : L'utilisation non autorisée ou abusive des données personnelles à des fins illégales, frauduleuses ou nuisibles. Cela peut inclure la vente ou la divulgation des données personnelles à des tiers non autorisés, l'utilisation des données pour l'usurpation d'identité, le harcèlement, la discrimination, etc.

S'assurer que les dossiers fermés sont déchiquetés par un membre de la direction à la fin de la période de conservation.

Détruire tous autres documents confidentiels de la même manière.

Conserver les renseignements personnels aussi longtemps que l'exigent la loi ou les fins pour lesquelles ils ont été recueillis. Lorsqu'il n'y aura plus de besoin, le Comité sectoriel de main-d'œuvre de l'habitation prendra des mesures raisonnables pour les supprimer.

- Papier : déchiqueteuse;

- Anonymiser les données sur les factures ou autres documents où des informations personnelles apparaissent.

6.5 Politique d'évaluation de facteur de vie privée (EVFP)

Mot de passe et authentification :

L'accès aux systèmes et aux données personnelles nécessitera une authentification appropriée, y compris l'utilisation de mots de passe robustes et de mécanismes d'authentification à deux facteurs lorsque cela est approprié.

Sensibilisation à la sécurité :

Le Comité fournira une formation à ses employés sur la sécurité des données personnelles et les meilleures pratiques.

https://www.cai.gouv.qc.ca/evaluation-facteurs-relatifs-vie-privee/

7. Modalités d'application

La direction du Comité sectoriel de main-d'œuvre de l'habitation est responsable de la mise en œuvre et de l'application de la politique de confidentialité.

La direction et les employés doivent remplir, dès l'entrée en vigueur de cette politique, un formulaire d'engagement à respecter celle-ci.

En cas de non-respect de la politique de confidentialité par la direction, c'est le conseil d'administration qui doit intervenir.

Si un ou une employée a divulgué une information confidentielle, l'autorité compétente lui impose une sanction conforme aux politiques, règlements du Comité sectoriel de main-d'œuvre de l'habitation. La sanction peut aller de la réprimande au congédiement.

8. Politiques de transfert, sécurisation et sensibilisation des données

Le CSMO, axé sur la protection de la vie privée et la sécurité des données, instaure des mesures en matière de gestion et de transfert de données. Nous exigeons que les politiques de transfert de données, tant à l'intérieur qu'à l'extérieur de l'organisation, soient révisées quand des changements apparaissent dans la loi 25, pour garantir leur conformité et leur efficacité. Ces révisions permettent de s'assurer que les pratiques de l'organisation restent à jour avec les normes.

En outre, la loi stipule que les employés doivent recevoir une formation en matière de cybersécurité ainsi que remplir un formulaire (voir en annexe) annuellement sur les employés et les risques. Cette formation vise à sensibiliser et à éduquer le personnel sur les risques de brèches de sécurité, en fournissant des connaissances pratiques pour les prévenir et les gérer efficacement. Cette approche proactive renforce la culture de la sécurité au sein de l'organisation.

Concernant la procédure en cas de brèche de sécurité, la loi 25 exige la mise en place d'un système de signalement interne. Cela inclut la création d'un registre de plaintes sous forme de fichier Excel, permettant de documenter et de suivre chaque incident. En cas de brèche avérée, l'organisation doit informer les autorités compétentes dans un délai de 45 jours. Le cycle de vie de chaque plainte est ainsi clairement défini, avec des étapes spécifiques pour la notification, l'enquête, la résolution et le rapport final.

L'accent est également mis sur la communication interne, assurant que tous les membres de l'organisation soient informés des politiques, des procédures et des mises à jour relatives à la sécurité des données. Cette transparence favorise une meilleure compréhension des enjeux de sécurité et renforce la responsabilité collective en matière de protection des données.

Communications régulières :

1. Maintenir une communication avec les employés en diffusant des rappels sur la confidentialité des données, les dernières menaces de sécurité, les bonnes pratiques en matière de protection des informations personnelles, etc. Le tout à la charge du représentant de cybersécurité.
2. Encourager les employés à poser des questions, à signaler les préoccupations et à partager les informations pertinentes pour renforcer la culture de la sécurité de l'information.

Procédure des plaintes :

Certaines conditions rendent une plainte non recevable telles que l'anonymat, la mauvaise foi, les propos haineux ou diffamatoires, et le manque d'informations nécessaires au traitement. Les plaintes qui ne concernent pas la protection des renseignements personnels, comme les décisions relatives à l'interprétation des dispositions légales, ne sont pas prises en compte. Nous notons et conservons les plaintes sur un fichier Excel sécurisé.

Envoyer tout courriel de plainte à Christian Galarneau, directeur général, à cgalarneau@csmohabitation.com, ou à Joëlle Mc Gurrin, conseillère en communication et en marketing, à jmcgurrin@csmohabitation.com. Ce sont les personnes désignées pour s'occuper des plaintes.

Notification des incidents de confidentialité :

1. Identification de l'incident : Définissez clairement les critères qui indiquent qu'un incident de confidentialité s'est produit, par exemple, tout accès non autorisé à des données personnelles, toute divulgation involontaire ou toute violation de la sécurité des données.
2. Rapport initial : Les employés qui identifient un incident potentiel de confidentialité doivent être tenus de le signaler immédiatement à leur supérieur hiérarchique, au responsable de la sécurité des informations ou à une personne désignée.
3. Évaluation préliminaire : Le responsable désigné ou l'équipe de cybersécurité doit effectuer une évaluation préliminaire de l'incident pour déterminer sa gravité, ses impacts potentiels et les mesures d'atténuation immédiates à prendre.
4. Notification interne : Une fois que l'incident est confirmé, une notification interne doit être envoyée aux parties concernées telles que le responsable de la sécurité des informations, le service juridique et la direction de l'entreprise. La notification doit inclure des informations clés sur l'incident, sa gravité, les données personnelles impliquées et les mesures déjà prises pour gérer la situation.

5. Investigation et réponse : L'équipe de cybersécurité ou une équipe d'incident dédiée doit mener une enquête approfondie pour déterminer les causes de l'incident, identifier les mesures correctives à prendre et mettre en place des mesures préventives pour éviter de futurs incidents similaires.
6. Suivi et communication : Faire le suivi avec les parties concernées selon le niveau de gravité de l'incident.

9. Réalisation d'un audit de sécurité par une firme externe de cybersécurité

Évaluation des risques et conception de stratégies de sécurité :

- Identifier les vulnérabilités potentielles dans les systèmes informatiques, réseaux et applications.
- Bâtir des stratégies pour minimiser les menaces et les attaques.

Mise en œuvre des mesures de sécurité :

- À la suite du rapport, la direction générale mettra en place des solutions de sécurité adaptées, comme les pares-feux, antivirus, systèmes de détection d'intrusion, chiffrement des données et authentification à deux facteurs.
- Assurer l'application rigoureuse des politiques et procédures de sécurité.

Surveillance et détection des incidents :

- Surveiller en permanence les systèmes pour détecter toute activité suspecte ou violation de sécurité.
- Analyser les journaux de sécurité, les alertes et les incidents.
- Prendre des mesures pour résoudre les problèmes et minimiser les dommages.

Gestion des incidents de sécurité :

- Coordonner la réponse appropriée en cas d'incident de sécurité avéré.
- Mener des enquêtes pour déterminer la cause et l'étendue de l'attaque.
- Mettre en place les mesures nécessaires pour remédier à la situation et prévenir de futures attaques.

10. Assurance de conformité et sécurité des données : Politique de consentement d'audit par des tiers

Nous recueillons les données personnelles uniquement avec un consentement clair et informé, au moyen de formulaires de contact et de formation. Les personnes sont pleinement conscientes de l'usage de leurs données et peuvent retirer leur consentement à tout moment.

Sécurité des données :

- Des mesures robustes sont mises en place pour protéger les données contre les accès non autorisés, les pertes, les altérations ou la divulgation. Ces mesures incluent des protocoles de chiffrement, des pare-feux et des systèmes de détection d'intrusion.

Accès et transfert des données :

- L'accès aux données est strictement réglementé et surveillé. Le transfert de données en dehors de l'organisation est effectué conformément aux normes de confidentialité et de sécurité établies.

Rétention et destruction des données :

- Nous adhérons à des politiques concernant la rétention et la destruction sécurisée des données, en veillant à ce que les données ne soient conservées que pour la durée nécessaire et soient détruites de manière appropriée une fois leur utilité épuisée.

Gestion des incidents de confidentialité :

- En cas de violation de données, des procédures sont en place pour une réponse rapide et efficace, minimisant l'impact et informant les parties concernées conformément aux exigences légales.

Documentation et conformité réglementaire :

- Toutes nos pratiques de gestion de données sont documentées et révisées pour assurer la conformité avec la réglementation en vigueur, y compris les audits réguliers par des tiers.

En outre, nos politiques d'évaluation des facteurs relatifs à la vie privée (EFVP) sont cruciales pour évaluer l'impact de nos opérations sur la vie privée des individus.

11. Organigramme du Comité sectoriel de main-d'œuvre de l'habitation

Conseil d'administration (CA) :

- Supervision de la direction stratégique du comité.

Directeur général :

- Informe le conseil d'administration.
- Recueillement et gestion des plaintes.
- Responsable de la cybersécurité.
- Travaille en étroite collaboration avec toute l'équipe pour garantir la sécurité des données.
- Responsable de la gestion quotidienne du Comité.
- Coordonne les activités entre les différentes ressources du CSMO.

Technicienne comptable :

- Rapporte au directeur général.
- Gestion des dossiers administratifs.

Coordinateurs de projets :

- Gèrent les projets spécifiques au sein du Comité.
- Rapportent au directeur général.
- Collaborent avec le chef de la cybersécurité pour s'assurer que les projets respectent les normes de sécurité des données.

Responsable des communications :

- Gère la communication interne et externe.
- Rapporte au directeur général et aux coordinateurs de projets.
- Travaille en étroite collaboration avec le chef de la cybersécurité pour communiquer au sujet des politiques et des mesures de sécurité des données.

Chaque rôle est clairement défini pour assurer une gouvernance efficace et une sécurité des données optimale. Le chef de la cybersécurité joue un rôle central, s'assurant que toutes les nouvelles sources de données sont rapportées et gérées conformément aux normes de sécurité établies.

12. Entrée en vigueur

La présente politique entre en vigueur le 12 avril 2024 suivant l’adoption par le conseil d’administration. Elle pourra être modifiée au moment opportun après analyse. La modification doit respecter les valeurs et les règlements du Comité sectoriel de main-d’œuvre de l’habitation.