Mise en application de la loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Cadre d'application de la Loi 25

09 octobre 2024

TABLE DES MATIÈRES

A. Identification de l’entreprise

1. Introduction à la Loi 25 — Guide d’application

Afin de se conformer à la **Loi 25** (anciennement projet de loi n°64, 2021, chapitre 25) du Gouvernement du Québec, qui modernise les dispositions législatives en matière de protection des renseignements personnels, **le Centre d’autonomie** s'engage à mettre en œuvre les mesures suivantes :

1.1. **Énumération des données collectées** : Identifier et documenter tous les types de renseignements personnels collectés auprès des clients, employés, fournisseurs et partenaires.

1.2. **Obtention d'un consentement éclairé** : S'assurer que le consentement pour la collecte, l'utilisation ou la communication de renseignements personnels est libre, éclairé, spécifique et obtenu de manière valide, basé sur une information adéquate fournie aux individus concernés.

1.3. **Respect des droits des individus** : Respecter les droits des personnes concernant l'accès, la rectification, l'effacement, la portabilité et le droit de s'opposer au traitement de leurs renseignements personnels.

1.4. **Mécanismes de consentement pour les mineurs** : Obtenir le consentement parental ou du tuteur légal pour la collecte de renseignements personnels auprès de mineurs de moins de 14 ans, conformément aux dispositions de la Loi 25.

1.5. **Protection de la confidentialité** : Élaborer et appliquer des politiques et pratiques régissant la gouvernance des renseignements personnels, y compris des politiques internes de gestion et de protection des données.

1.6. **Formation et sensibilisation du personnel** : Offrir des formations aux employés sur les politiques de protection des renseignements personnels et les sensibiliser aux meilleures pratiques en matière de sécurité des données.

1.7. **Transparence et accessibilité de l'information** : Communiquer de manière transparente avec les individus sur les pratiques de gestion des renseignements personnels, y compris en rendant accessibles les politiques de confidentialité.

1.8. **Utilisation des données** : Définir clairement les finalités pour lesquelles les renseignements personnels sont utilisés et veiller à ce qu'ils ne soient pas utilisés à des fins incompatibles sans consentement supplémentaire.

1.9. **Sécurisation des données** : Mettre en place des mesures de sécurité physiques, administratives et techniques appropriées pour protéger les renseignements personnels contre la perte, le vol, l'accès non autorisé, la divulgation, la copie, l'utilisation ou la modification.

1.10. **Gestion des incidents** : Être prêt à réagir rapidement en cas d'incident de confidentialité, y compris la mise en place d'un plan d'intervention, la notification aux personnes concernées et à la Commission d'accès à l'information du Québec lorsque l'incident présente un risque sérieux de préjudice.

1.11. **Évaluations des Facteurs relatifs à la Vie Privée (EFVP)** : Effectuer des évaluations préalables des facteurs relatifs à la vie privée pour tout projet impliquant la collecte, l'utilisation ou la communication de renseignements personnels, afin d'identifier et atténuer les risques potentiels pour la vie privée.

1.12. **Limitation de la conservation des données** : Déterminer et respecter des délais de conservation pour les renseignements personnels, en veillant à ce qu'ils ne soient pas conservés plus longtemps que nécessaires aux fins pour lesquelles ils ont été collectés.

1.13. **Transfert international des données** : S'assurer que tout transfert de renseignements personnels à l'extérieur du Québec respecte les exigences légales, notamment en garantissant un niveau de protection équivalent.

1.14. **Nomination d'un responsable de la protection des renseignements personnels** : Désigner une personne responsable de veiller au respect et à la mise en œuvre de la Loi 25 au sein de l'organisation.

2. Contacts et ressources supplémentaires

Pour toute question ou besoin d'assistance concernant l'application de la Loi 25 au sein du **Centre d’autonomie**, veuillez contacter notre responsable, **Mme Hélène Paradis** aux coordonnées fournies ci-dessus.

Des ressources supplémentaires et des conseils d'experts peuvent également être obtenus auprès des autorités réglementaires compétentes et des conseillers juridiques spécialisés en protection des données.

3. Identification de l’entreprise

Nom d'entreprise : Centre d’autonomie

Succursales :
• Dolbeau-Mistassini, 399 avenue de La Friche, Dolbeau-Mistassini (Qc) G8L 2T3, 418 276-8336
• Chicoutimi, 690 rue des Actionnaires, Chicoutimi (Qc) G7J 5A8, 418 542-1255
Téléphone sans frai : 1 800-263-8337
Courriel : info@centreautonomie.com

4. Responsable

Nom : Hélène Paradis
Titre : Technicienne-Comptable
Courriel : comptabilite@centreautonomie.com
Téléphone : 418-276-8336 poste 227

B. Type de données collectées

5. Données des employés

5.1. **Informations personnelles des employés** : Collecte et conservation des informations nécessaires à la gestion des ressources humaines, y compris les noms, dates de naissance, adresses, numéros de téléphone, courriel, numéros d'assurance sociale et informations bancaires pour le paiement des salaires.

6. Données des clients

6.1. **Collecte des informations personnelles** : Nous collectons les noms, adresses postales, numéros de téléphone, courriel et préférences d'achat de nos clients, si nécessaire.

6.2. **Historique des transactions** : Détails des achats effectués, y compris les types de produits ou services, les quantités, les dates d'achat et les montants dépensés.

6.3. **Interactions avec le service client** : Enregistrement des demandes, réclamations, retours et toute autre interaction avec notre service client pour améliorer la qualité de nos services.

6.4. **Informations de paiement** : Collecte des informations nécessaires pour le traitement des paiements, en veillant à respecter les normes de sécurité les plus strictes.

7. Données des fournisseurs

7.1. **Collecte des informations d'identification** : Nous collectons les noms, adresses postales, numéros de téléphone et courriel de nos fournisseurs afin de faciliter les communications et les transactions commerciales.

7.2. **Informations transactionnelles** : Enregistrement des détails relatifs aux transactions, y compris les quantités commandées, les prix, les modalités de paiement et les dates de livraison.

7.3. **Correspondance électronique** : Conservation de toute correspondance électronique pour référence future, suivi des échanges et amélioration de nos relations avec les fournisseurs.

7.4. **Informations en ligne** : Conservation des liens vers les sites web et plateformes en ligne de nos fournisseurs pour un accès rapide et une référence aisée.

8. Données de navigation web

8.1. **Cookies et technologies similaires** : Collecte d'informations via des cookies ou technologies similaires sur notre site web, telles que les adresses IP, les préférences de navigation, l'historique des pages visitées, le type de navigateur et le système d'exploitation.

C. Droits des utilisateurs

9. Droit à l'information

9.1. **Transparence** : Les utilisateurs ont le droit de savoir comment leurs données sont utilisées, stockées et protégées. Nous nous engageons à fournir cette information de manière claire, concise et accessible.

10. Droit d'accès et de rectification

10.1. **Accès aux données** : Les utilisateurs peuvent demander à consulter les données personnelles que nous détenons à leur sujet.

10.2. **Rectification des données** : Si des informations sont inexactes ou incomplètes, les utilisateurs ont le droit de les faire corriger ou compléter.

11. Droit à la portabilité des données

11.1. **Transfert des données** : Les utilisateurs ont le droit de recevoir leurs données personnelles dans un format structuré.

12. Droit d'opposition et de retrait

12.1. **Retrait du consentement** : Les utilisateurs peuvent retirer leur consentement à tout moment pour le traitement de leurs données personnelles, ce qui peut affecter l'accès à certaines fonctionnalités ou services.

12.2. **Opposition au traitement** : Les utilisateurs ont le droit de s'opposer au traitement de leurs données personnelles pour des motifs légitimes, y compris le marketing direct.

13. Consentement éclairé

13.1. **Choix des utilisateurs** : Les utilisateurs ont le choix de fournir ou non leurs données personnelles. Toutefois, certaines fonctionnalités ou services peuvent nécessiter certaines informations pour fonctionner correctement.

13.2. **Consentement des mineurs** : Pour les personnes de moins de 14 ans, le consentement du titulaire de l'autorité parentale ou du tuteur est requis pour la collecte de leurs renseignements personnels, sauf si la collecte est manifestement au bénéfice du mineur.

D. Engagement de confidentialité

14. Accord de confidentialité des employés

14.1. **Obligation contractuelle** : Tous les employés signent un accord de confidentialité les engageant à protéger les informations confidentielles et les données personnelles auxquelles ils ont accès dans le cadre de leurs fonctions.

14.2. **Durée de l'engagement** : Cette obligation de confidentialité s'applique pendant la durée de l'emploi et subsiste trois ans après la fin de la relation d'emploi.

14.3. **Portée de l'engagement** : L'accord couvre toutes les données confidentielles, y compris les informations sur les clients, les fournisseurs, les employés et les informations internes de l'entreprise.

15. Sensibilisation et formation

15.1. **Programme de formation** : Mise en place de programmes de formation pour sensibiliser les employés à l'importance de la confidentialité et aux méthodes de protection des informations sensibles.

15.2. **Mise à jour des connaissances** : Les employés sont informés des évolutions réglementaires et des nouvelles menaces en matière de sécurité des données.

16. Responsabilité et conformité

16.1. **Suivi et audits internes** : Réalisation de suivis réguliers et d'audits internes pour s'assurer du respect des engagements de confidentialité par tous les employés.

16.2. **Mesures disciplinaires** : En cas de violation de l'accord de confidentialité, des mesures appropriées sont prises, pouvant inclure des sanctions disciplinaires ou légales.

E. Utilisation des données

17. Données des clients

17.1. **Traitement des commandes** : Utilisation des informations clients pour traiter les commandes, gérer les livraisons et fournir un service client de qualité.

17.2. **Communications marketing** : Avec le consentement explicite des clients, envoi d'informations sur des promotions, des nouveautés, des événements et des offres personnalisées.

17.3. **Personnalisation de l'expérience client** : Analyse des données d'achat et de navigation pour proposer des produits et services adaptés aux préférences individuelles des clients.

17.4. **Amélioration continue** : Utilisation des retours d'expérience et des données d'achat pour améliorer nos offres et services.

17.5. **Traitement sécurisé des paiements** : Les informations de paiement sont traitées en conformité avec les normes de sécurité les plus strictes pour protéger les informations financières de nos clients et prévenir les fraudes.

17.6. **Conformité légale** : Respect des obligations légales liées à la facturation, la comptabilité et la protection des consommateurs.

18. Données des fournisseurs

18.1. **Gestion des relations fournisseurs** : Les informations collectées sont utilisées pour gérer les commandes, les livraisons, les paiements et maintenir une communication efficace avec nos fournisseurs.

18.2. **Amélioration des services** : Analyse des données transactionnelles et des communications pour évaluer et améliorer la qualité de nos services et produits.

18.3. **Conformité légale et réglementaire** : Utilisation des données pour répondre aux obligations légales et réglementaires, notamment en matière de comptabilité, fiscalité et audits.

19. Données web

19.1. **Analyse web** : Utilisation d'outils d'analyse pour comprendre comment les utilisateurs interagissent avec notre site web, afin d'améliorer l'expérience utilisateur.

F. Protection des données

20. Politique de conservation des données

20.1. **Durée de conservation limitée** : Les données personnelles collectées sont conservées pour la durée nécessaire, sauf si une période plus longue est requise ou permise par la loi.

20.2. **Révision et suppression** : Les données personnelles sont évaluées pour déterminer si leur conservation est toujours nécessaire. Si ce n'est pas le cas, elles sont supprimées.

20.3. **Transparence et sécurité** : Engagement à gérer les données personnelles de manière transparente, sécurisée et conforme aux exigences légales en vigueur.

20.4. **Droits des individus** : Les clients, fournisseurs et employés peuvent nous contacter pour toute question ou demande concernant la gestion de leurs données personnelles, y compris les demandes de suppression ou de limitation du traitement.

21. Protection des informations électroniques

21.1. **Chiffrement et sécurité** : Les documents électroniques contenant des renseignements personnels sont chiffrés et protégés par des mots de passe robustes.

21.2. **Gestion des mots de passe** : Les mots de passe sont modifiés sporadiquement, notamment lors du départ d'un employé ou du changement de rôle de personnes ayant accès aux dossiers sensibles.

21.3. **Sauvegardes sécurisées** : Réalisation de sauvegardes régulières des données, stockées de manière sécurisée pour prévenir la perte d'informations en cas d'incident.

22. Protection des informations physiques

22.1. **Stockage sécurisé** : Les documents contenant des renseignements personnels en format papier sont conservés dans des classeurs verrouillables situés dans des zones sécurisées.

22.2. **Contrôle des accès** : Seules les personnes autorisées ont accès aux clés des classeurs, qui sont elles-mêmes conservées en lieu sûr.

23. Droits des individus

23.1. **Accès et rectification** : Les individus ont le droit de demander l'accès à leurs données personnelles, de les corriger ou de les mettre à jour en contactant notre responsable de la protection des renseignements personnels.

23.2. **Effacement et limitation** : Sur demande, nous pouvons supprimer ou limiter le traitement des données personnelles, sous réserve des obligations légales et réglementaires.

23.3. **Portabilité des données** : Les individus peuvent demander à recevoir leurs données personnelles dans un format structuré, couramment utilisé et lisible par machine.

24. Engagement de non-vente et de non-partage des données

24.1. **Confidentialité des données** : Nous nous engageons à ne pas vendre, louer ou partager les données personnelles de nos clients, fournisseurs et employés avec des tiers, sauf si la loi l'exige ou avec le consentement explicite des personnes concernées.

24.2. **Partenaires et sous-traitants** : Lorsque nous faisons appel à des partenaires ou sous-traitants, nous nous assurons qu'ils respectent des normes équivalentes en matière de protection des données personnelles.

24.3. **Révisions et formations** : Mise à jour sporadique de nos politiques de sécurité et formation continue du personnel aux protocoles de confidentialité pour garantir une protection optimale des données.

G.Mesures de sécurité

25. Sécurité des équipements informatiques

25.1. **Protection des postes de travail** : Tous les ordinateurs utilisés au sein de l'entreprise sont protégés par des mots de passe uniques et robustes, ainsi que par des logiciels antivirus et anti-malware régulièrement mis à jour.

25.2. **Contrôles d'accès** : Mise en place de contrôles d'accès pour restreindre l'accès aux informations sensibles uniquement aux employés autorisés (comptables et associés), selon le principe du moindre privilège.

26. Messagerie professionnelle sécurisée

26.1. **Plateforme sécurisée** : Utilisation de Microsoft Exchange pour notre messagerie professionnelle, offrant une sécurité renforcée pour les communications internes et externes.

26.2. **Protection contre les menaces** : Mise en place de filtres anti-spam, anti-phishing et anti-malware pour protéger contre les menaces potentielles.

27. Serveurs et stockage en nuage

27.1. **Serveurs sécurisés** : Utilisation de serveurs internes garantissant un environnement sécurisé pour le stockage et la gestion des données avec Blackburn & Blackburn.

27.2. **Sauvegardes :** Réalisation de sauvegardes journalières pour assurer la continuité des activités en cas d'incident.

27.3. **Chiffrement des données** : Les données sensibles sont chiffrées lorsqu'elles sont stockées sur nos serveurs et lors de leur transmission.

28. Site web sécurisé

28.1. **Hébergement sécurisé au Canada** : Notre site web est hébergé sur des serveurs sécurisés situés au Canada, assurant la conformité avec les lois canadiennes sur la protection des données.

28.2. **Certificat SSL/TLS** : Utilisation de certificats SSL/TLS pour chiffrer les communications entre le site web et les utilisateurs, prévenant ainsi l'interception ou l'altération des données.

28.3. **Protection contre les menaces en ligne** : Mise en place de mesures de sécurité pour protéger le site web contre les attaques telles que les injections SQL, les scripts intersites (XSS) et les attaques par déni de service (DDoS).

29. Transfert international des données

29.1. **Limitation des transferts** : Toutes les données collectées sont stockées et gérées exclusivement sur des serveurs situés au Canada. Aucun transfert de données personnelles à l'extérieur du Canada n'est effectué.

29.2. **Conformité légale** : En cas de nécessité de transfert international, nous nous assurons que des mesures adéquates sont en place pour garantir un niveau de protection équivalent, conformément aux exigences de la Loi 25.

H. Liens externes sur le site web

30. Politique de non-responsabilité

30.1. **Indépendance des sites tiers** : Notre site web peut contenir des liens vers des sites web tiers qui sont indépendants de notre entreprise et qui ont leurs propres politiques de confidentialité.

30.2. **Absence de contrôle** : Nous n'exerçons aucun contrôle sur le contenu, les pratiques de confidentialité ou les actions de ces sites tiers et déclinons toute responsabilité à cet égard.

31. Recommandations aux utilisateurs

31.1. **Vigilance recommandée** : Nous encourageons les utilisateurs à faire preuve de prudence lorsqu'ils quittent notre site web et à consulter les politiques de confidentialité des sites web tiers qu'ils visitent.

31.2. **Protection des informations** : Les informations fournies à des tiers sont soumises à leurs propres politiques et pratiques, et nous ne pouvons garantir leur niveau de sécurité ou de protection.

I. Gestion des incidents

32. Procédures en cas d'incidents de sécurité

32.1. **Surveillance proactive** : Nous surveillions constamment nos systèmes pour détecter rapidement tout incident de sécurité, y compris les fuites de données ou les cyberattaques.

32.2. **Signalement immédiat** : Tout membre du personnel ou tiers qui constate un incident de confidentialité doit le signaler immédiatement au responsable de la protection des renseignements personnels.

32.3. **Documentation des incidents** : Un formulaire de signalement doit être rempli, incluant une description détaillée de l'incident, les données affectées, les circonstances, les dates pertinentes et le nombre de personnes concernées.

33. Conservation des informations sur les incidents

33.1. **Registre des incidents** : Tous les incidents de confidentialité sont consignés dans un registre dédié et conservés pendant une période minimale de cinq ans, conformément aux exigences légales.

34. Évaluation et notification

34.1. **Évaluation du risque** : Le responsable de la protection des renseignements personnels évalue si l'incident présente un risque sérieux de préjudice pour les personnes concernées.

34.2. **Notification aux autorités** : Si un risque sérieux est identifié, nous notifierons sans délai la Commission d'accès à l'information du Québec.

34.3. **Information des personnes concernées** : Les individus affectés seront informés de l'incident, des données potentiellement compromises et des mesures qu'ils peuvent prendre pour se protéger.

35. Mesures post-incident

35.1. **Analyse approfondie** : Après un incident, une analyse complète est effectuée pour identifier les causes profondes et les failles de sécurité exploitées.

35.2. **Actions correctives** : Mise en œuvre de mesures correctives pour renforcer nos systèmes et prévenir la récurrence de tels incidents.

35.3. **Formation du personnel** : Renforcement de la formation et de la sensibilisation des employés aux meilleures pratiques de sécurité et aux protocoles en cas d'incident.

J. Mise à jour de l’application

36. Dernière mise à jour

36.1. **Actualisation régulière** : Cette politique de confidentialité a été mise à jour le **9 octobre 2024**. Nous nous réservons le droit de la modifier pour refléter les changements dans nos pratiques ou les évolutions législatives.

36.2. **Notification des modifications** : Toute modification significative sera communiquée aux utilisateurs via notre site web ou par d'autres moyens appropriés.

37. Contact pour questions relatives à la politique de confidentialité

37.1. **Coordonnées du responsable** : Pour toute question, demande ou préoccupation concernant cette politique de confidentialité ou la gestion de vos données personnelles, veuillez contacter notre responsable de la protection des renseignements personnels :

Nom : Hélène Paradis
Titre : Technicienne-Comptable
Courriel : comptabilite@centreautonomie.com
Téléphone : 418-276-8336 poste 227

38. Acceptation des termes

38.1. **Consentement** : En utilisant nos services et en entretenant des relations professionnelles avec notre entreprise, vous acceptez les termes de cette politique de confidentialité.

38.2. **Engagement envers la protection des données** : Nous reconnaissons l'importance de protéger vos données personnelles et nous nous engageons à le faire avec le plus grand soin, en conformité avec la législation en vigueur et les meilleures pratiques du secteur.