POLITIQUES ET PRATIQUES ENCADRANT LA GOUVERNANCE DES RENSEIGNEMENTS PERSONNELS

PAVAGE CARMICHAEL INC.

437, rue des Montérégiennes

Québec (QC) G1C 7J7

T 418 849-8713

F 418 686-1744

AVRIL 2024

Table des matières

1 – INTRODUCTION

1.0 Mot de la direction

PAVAGE CARMICHAEL INC.
437 rue des Montérégiennes
Québec, Qc G1C 7J7
T 418 849-8713 F 418 686-1744

1.0 Mot de la direction

Québec, avril 2024

PAVAGE CARMICHAEL INC. a à cœur le respect de la vie privée et s'engagent à protéger les renseignements personnels de l'ensemble de leurs employés et partenaires. La présente politique de confidentialité a pour but d'expliquer et d'informer sur les méthodes de traitement des données et renseignements personnels au sein de l'entreprise.

Lorsque des renseignements personnels sont recueillis par notre société; l'utilisation, la disposition et la communication de ceux-ci se font conformément à la présente politique de confidentialité et mesures légales. Pour ce faire, notre société a mis en place deux actions clés directement liées à la protection des renseignements personnels :

1. La mise en place d'un plan de traitement des plaintes relative à la protection des renseignements personnels.

2. La mise en place d'un programme visant à sensibiliser et informer l'ensemble du personnel de l'entreprise sur l'importance de la protection des renseignements personnels. Ce programme vise à assurer que tous les employés ayant accès à des renseignements personnels reçoivent la formation nécessaire pour se conformer aux exigence de protection de ceux-ci. Il comprend la création d'une présentation claire expliquant les changements liés à la protection des renseignements personnels, la présentation des politiques et pratiques de l'entreprise aux employés, la mise à jour régulière de la formation et la formation spécifique des employés impliqués dans la mise en œuvre du programme de protection des renseignements personnels.

Afin d’assurer la continuité de nos programme de protection des renseignements personnels, il est prévu d’effectuer une mise à jour annuelle des différentes politiques et des pratiques encadrant la conservation, la destruction et l'anonymisation de ces derniers. Cela implique de définir les dispositions de la politique applicable, d'identifier les outils à mettre en place, d'établir les pratiques de conservation et de destruction des renseignements personnels, de mettre en œuvre ces pratiques et de vérifier l'atteinte du degré requis d'anonymisation.

En terminant, *PAVAGE CARMICHAEL INC.* s’engage à se tenir aux faits de tout changement des lois et/ou réglementations et ainsi adapter la présente politique afin d’œuvrer en toute conformité.

2 – QUESTIONS/RÉPONSES

2.1 Informations collectées, conservées, communiquées et détruites

Afin d'établir le meilleur processus de collecte d'informations, voici les étapes que nous avons considérer :

1. Identification des informations nécessaires : Nous avons pris soin de déterminer en amont les types d'informations requises, en tenant compte de leur pertinence et de leur utilisation prévue. Or, nous procédons uniquement à la collecte des informations nécessaires et pertinentes afin d'éviter d'encombrer les bases de données avec des données inutiles.

2. Obtention du consentement : Nous avons mis en place un processus de consentement clair et transparent, conformément aux réglementations en matière de protection des renseignements personnels. Nous prenons soins d'informer les individus sur la collecte, l'utilisation et la communication de leurs informations personnelles, et obtenons leur consentement avant de procéder à la collecte.

3. Sécurisation des données : Des mesures de sécurité appropriées ont été mises en place afin protéger les informations collectées. Cela inclus des mesures telles que le cryptage des données, l'accès restreint aux informations sensibles et la mise à jour régulière des systèmes de sécurité.

4. Stockage et gestion des informations : Nous avons établi des procédures claires pour stocker et gérer les informations collectées. Nous utilisons également des bases de données sécurisées, la classification des informations en fonction de leur sensibilité et la tenue d'un inventaire des informations collectées.

5. Durée de conservation des informations : Nous avons déterminé la durée pendant laquelle les informations doivent être conservées en fonction des exigences réglementaires et des besoins opérationnels. Des lignes directrices claires ont été établies sur la durée de conservation des informations et l'utilisation d'un processus de suppression sécurisé des informations une fois qu'elles ne sont plus nécessaires.

6. Transparence et communication : Nous communiquons de manière transparente les pratiques de collecte d'informations auprès des individus concernés. Nous leur fournissons également les informations sur les finalités de la collecte ainsi que sur la manière dont ils peuvent accéder à leurs informations ou les mettre à jour.

7. Évaluation continue : Une surveillance et évaluation régulière du processus de collecte d'informations a été mise en branle afin d'assurer sa conformité aux réglementations et aux meilleures pratiques.

Il est important de noter que les détails spécifiques du processus de collecte d'informations peuvent varier en fonction des besoins et des exigences propre au type de cueillette;

Exemple : Renseignements personnels d'un employé vs d'un fournisseur.

NOUVEL EMPLOYÉ :

Lors de l'embauche, nous procédons à la collecte des renseignements personnels de la personne **conformément au processus précédemment cité** et créons un dossier *employé*. Voici la liste des données collectées (si requises selon le type d'emploi) :

- NOM, PRÉNOM ET DATE DE NAISSANCE
- ADRESSE DE RÉSIDENCE
- N° DE TÉLÉPHONE ET ADRESSE COURRIEL
- N° D'ASSURANCE SOCIAL
- CARTES DE COMPÉTENCES, DE FORMATION, SANTÉ ET SÉCURITÉ ET SYNDICAT **Si applicable*
- INFORMATIONS BANCAIRES (SPÉCIMEN DE CHÈQUE)
- PHOTO DU PERMIS DE CONDUIRE
- CONTACT EN CAS D'URGENCE
- TOUT AUTRE RENSEIGNEMENT JUGÉ PERTINENT

RAPPEL : Tous ces renseignements sont fournis volontairement et stockés dans une base de données sécurisée.

FOURNISSEUR :

Avant de débuter de nouvelles ententes commerciales avec un fournisseur, nous procédons à la collecte de certains renseignements personnels **conformément au processus précédemment cité** et créons un dossier *fournisseur*. Voici la liste des données collectées (si requise selon le type de service/commerce) :

- NOM DE L'ENTREPRISES ET DU CONTACT
- ADRESSE *DE L'ENTREPRISE
- N° DE TÉLÉPHONE ET ADRESSE COURRIEL
- N° DE TPS/TVQ

- INFORMATIONS BANCAIRES (SPÉCIMEN DE CHÈQUE)
- TOUT AUTRE RENSEIGNEMENT JUGÉ PERTINENT

RAPPEL : Tous ces renseignements sont fournis volontairement et stockés dans une base de données sécurisée.

CLIENT :

Lors de nouvelles ententes/contrats avec des clients, nous procédons à la collecte de certains renseignements personnels **conformément au processus précédemment cité** et créons un dossier *client.* Voici la liste des données collectées (si requises selon le type de contrat) :

- NOM DU CLIENT (ENTREPRISES, VILLE, ENTREPRENEUR, ETC.) ET DU CONTACT
- ADRESSE
- N° DE TÉLÉPHONE ET ADRESSE COURRIEL
- N° DE LICENCES RBQ, CNESST, CCQ **Si applicable*
- TOUT AUTRE RENSEIGNEMENT JUGÉ PERTINENT

RAPPEL : Tous ces renseignements sont fournis volontairement et stockés dans une base de données sécurisée.

2.2 Processus de rétention des données

Afin de maximiser la sécurité et faciliter la gestion des données au sein de l'entreprise, nous avons établi un plan en 5 étapes ;

1. Mise en place d'une politique de rétention des données : Élaboration de barèmes précis de durée de conservation des données personnelles en tenant compte des exigences légales, des obligations contractuelles, des finalités de traitement des données et des pratiques de l'industrie.

DURÉE DE RÉTENTION : 7 ans

2. Respect des principes de minimisation des données : Assurer la limitation de la collecte et la conservation des données personnelles aux informations nécessaires à des fins spécifiques. Nous évitons ainsi la conservation des données excessives, inutiles ou obsolètes.

3. Mise en place des mesures de sécurité : Mettre en œuvre des mesures appropriées pour protéger les données personnelles stockées. Cela peut inclure le cryptage, l'accès restreint, la surveillance des données et la protection contre les cyberattaques.

4. Suivre les délais de conservation appropriés : Assurer le respect des délais de conservation spécifiés dans nos politiques, les exigences légales ou les obligations contractuelles en veillant à supprimer les données périmées ou qui ne sont plus nécessaires.

5. Supprimer de manière sécurisée les données obsolètes : Lorsque les données personnelles ne sont plus utiles ou requises, celles-ci seront supprimées de manière sécurisée *(voir article 2.4 – Processus de destruction des données)*.

2.3.1 Raisons, principaux facteurs et paramètres encadrant la prise de décisions fondées exclusivement sur un traitement automatisé de renseignements personnels.

La prise de décisions exclusivement basée sur un traitement automatisé de renseignements personnels peut soulever des préoccupations en termes de protection de la vie privée et de l'équité. Il est donc essentiel de mettre en place des mesures de sécurité et de transparence pour garantir que les décisions automatisées sont justes et respectent les droits des individus. Or, notre prise de décisions fondées exclusivement sur un traitement automatisé de renseignements personnels est principalement motivée par les raisons, facteurs et paramètres suivants :

Efficacité et rapidité : Les systèmes de traitement automatisé peuvent analyser rapidement de grandes quantités de données, ce qui permet de prendre des décisions plus rapidement et efficacement.

Accessibilité et précision : Accès direct au système de traitement automatisés limitant les interactions humaines et le risque d'erreur potentiel. Les systèmes automatisés peuvent être conçus pour garantir une plus grande précision dans la prise de décisions.

Réduction des coûts : L'automatisation des processus de prise de décision peut réduire les coûts liés à l'emploi de personnel pour effectuer ces tâches ou au temps de travail de celui-ci.

Analyse de données complexes : Les algorithmes de traitement automatisé peuvent être utilisés pour analyser des ensembles de données complexes et identifier des tendances ou des modèles qui pourraient échapper à l'observation humaine.

PAVAGE CARMICHAEL INC.
437 rue des Montérégiennes
Québec, Qc G1C 7J7
T 418 849-8713 F 418 686-1744

2.3.2 Liste des personnes ayant accès aux données

NOM	TITRE	TYPE D'ACCÈS
M. Ian Thibodeau	*PRÉSIDENT-SECRÉTAIRE*	✓ INTÉGRAL
M. Martin Beaudoin	*DIRECTEUR*	✓ DOSSIERS CLIENTS ✓ DOSSIERS FOURNISSEURS
MME. Julie Landry	*CPA-CONTRÔLEURE*	✓ INTÉGRAL
MME. Francine Baril	*TECHNICIENNE-COMPTABLE*	✓ INTÉGRAL
MME. Ginger Renaud	*ADJOINTE ADMINISTRATIVE*	✓ INTÉGRAL
MME. Marie-Josée Bédard	*RESPONSABLE RESSOURCES HUMAINES*	✓ DOSSIERS EMPLOYÉS

PAVAGE CARMICHAEL INC.
437 rue des Montérégiennes
Québec, Qc G1C 7J7
T 418 849-8713 F 418 686-1744

2.4 Processus de destruction des données

1. Destruction des Documents Papier :

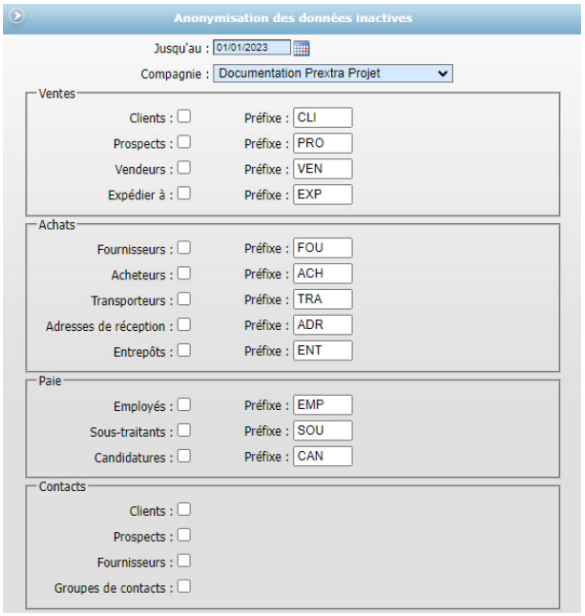
- Les documents papiers contenant des données sensibles seront détruits par déchiquetage après une période de conservation de 7 ans.

- À la fin de la période de conservation, les documents seront collectés et déchiquetés de manière sécurisée pour garantir la confidentialité des informations.

2. Anonymisation des données interactive :

- Sur demande, le système procédera à l'anonymisation des données en créant un préfixe au lieu des informations d'origine de la fiche. Cette procédure est définitive. Les données seront effacées de manière permanente et il est IMPOSSIBLE de renverser cette procédure.

1.



Exemple d'anonymisation des données par le système.

TYPE DE DONNÉES POUVANT ÊTRE ANONYMISÉES :

Ventes

Clients	Prospects	Vendeurs	Expédié à
➢Nom	➢Nom	➢Nom	➢Nom
➢Adresse	➢Adresse	➢Titre	➢Adresse
➢Ville	➢Ville	➢Adresse	➢Ville
➢Code postal	➢Code postal	➢Ville	➢Code postal
➢# Cellulaire	➢# Téléphone	➢Code postal	➢# Téléphone
➢# Téléphone	➢# Télécopieur	➢# Téléphone	➢# Télécopieur
➢# Télécopieur	➢Numéro sans frais		
➢Contact	➢Contact		
➢Courriel du contact	➢Courriel du contact		
➢Site web	➢Site web		
➢Courriel			

Achats

Fournisseurs	Acheteurs	Transporteurs	Adresses de réception	Entrepôt
➢Nom	➢Nom	➢Nom	➢Nom	➢Nom
➢Adresse	➢Adresse	➢Adresse	➢Adresse	➢Adresse
➢Ville	➢Ville	➢Ville	➢Ville	➢Ville
➢Code postal	➢Code postal	➢Code postal	➢Code postal	➢Code postal
➢# Téléphone	➢# Télécopieur	➢# Téléphone	➢Comté	➢# Téléphone
➢# Autre Tél.	➢Courriel	➢# Télécopieur	➢# Téléphone	➢# Télécopieur
➢# Télécopieur		➢Courriel	➢# Télécopieur	
➢Courriel		➢# NIR		
➢Site web				

Paie

Employés	Sous-traitants	Candidatures
➢Nom	➢Nom	➢Nom
➢Prénom	➢Prénom	➢Prénom
➢Adresse	➢Courriel	➢Adresse
➢Ville	➢Téléphone	➢Ville
➢Code postal	➢Cellulaire	➢Code postal
➢# Téléphone	➢Sexe	➢Téléphone
➢# Cellulaire		➢Cellulaire
➢Courriel		➢Courriel
➢# Assurance sociale		
➢Banque REER		
➢Compte REER		
➢Date de naissance		
➢Sexe		
➢# Permis de conduire		
➢# Assurance maladie		
➢# Pension alimentaire		
➢Contact d'urgence		
➢Téléphone d'urgence		
➢Courriel pour talon de paie		

Contacts

Clients	Prospects	Fournisseurs	Groupe de contact
➢Nom	➢Nom	➢Nom	➢Nom
➢Prénom	➢Prénom	➢Prénom	➢Adresse
➢Adresse	➢Adresse	➢Adresse	➢Ville
➢Ville	➢Ville	➢Ville	➢Code postal
➢Code postal	➢Code postal	➢Code postal	➢# Téléphone
➢Société	➢Société	➢Société	➢# Télécopieur
➢# Téléphone	➢# Téléphone	➢# Téléphone	
➢# Cellulaire	➢# Cellulaire	➢# Cellulaire	
➢# Télécopieur	➢# Télécopieur	➢# Télécopieur	
➢## Téléavertisseur	➢# Téléavertisseur	➢# Téléavertisseur	
➢Numéro sans frais	➢Numéro sans frais	➢Numéro sans frais	
➢Courriel	➢Courriel	➢Courriel	
➢Date de naissance	➢Date de naissance	➢Date de naissance	

3. Durée de Conservation :

- Toutes les données, qu'elles soient sous forme papier ou numérique, seront conservées pendant une période de 7 ans avant d'être détruites ou anonymisées selon les procédures établies.

Cette procédure de destruction des données vise à assurer la protection et la confidentialité des informations sensibles de l'entreprise. En suivant ces directives, nous garantissons une gestion sécurisée et conforme des données tout au long de leur cycle de vie. Si vous avez des questions supplémentaires ou besoin de clarifications, n'hésitez pas à contacter le service responsable de la gestion des données.

2.5.1 Incident de confidentialité

Un incident de confidentialité se produit lorsque des informations sensibles, confidentielles ou privées sont compromises, divulguées, accédées ou utilisées de manière non autorisée ou inappropriée. Ces incidents peuvent survenir dans divers contextes, notamment dans le domaine de la sécurité informatique, de la protection des données personnelles et de la gestion de l'information. Voici quelques exemples de ce qui pourrait constituer un incident de confidentialité dans le cadre de nos activités :

1. **Violation de données** : Lorsqu'une entreprise ou une organisation subit une violation de données, cela signifie généralement qu'un acteur malveillant a réussi à accéder à des informations confidentielles, telles que des données personnelles, des numéros de comptes bancaires, des mots de passe, etc.
2. **Fuite d'informations sensibles** : Il peut s'agir de la publication accidentelle ou non autorisée d'informations sensibles, comme des documents internes ou des données commerciales.
3. **Vol d'identité** : Lorsque les informations personnelles d'un individu sont utilisées de manière frauduleuse pour commettre des activités criminelles, telles que l'ouverture de comptes bancaires ou la souscription de prêts au nom de la victime.
4. **Perte de matériel ou de supports de stockage** : Si des ordinateurs portables, des disques durs, des clés USB ou d'autres supports de stockage contenant des données sensibles sont perdus ou volés, cela peut entraîner un incident de confidentialité.
5. **Attaques informatiques** : Les attaques telles que les ransomwares, les logiciels malveillants et les intrusions dans les systèmes informatiques peuvent entraîner la divulgation non autorisée de données confidentielles.
6. **Erreurs humaines** : Les erreurs commises par des employés, telles que l'envoi de courriels contenant des informations sensibles à la mauvaise personne ou la publication accidentelle de données sur Internet, peuvent également constituer des incidents de confidentialité.

7. **Hameçonnage** : Lorsque des individus sont trompés par des courriels ou des sites web frauduleux qui les incitent à divulguer des informations personnelles ou financières, cela peut conduire à une violation de la confidentialité.
8. **Accès non autorisé** : Lorsqu'une personne non autorisée obtient un accès illégitime à des systèmes, des réseaux ou des données, cela constitue un incident de confidentialité.
9. **Surveillance illégale** : La collecte illégale ou non autorisée d'informations personnelles ou privées par des gouvernements, des entreprises ou d'autres entités peut également être considérée comme un incident de confidentialité.

Dans tous ces cas, il est essentiel de prendre des mesures pour remédier à l'incident, minimiser les dommages potentiels, notifier les personnes concernées (si nécessaire) conformément à la réglementation en vigueur, et mettre en place des mesures préventives pour éviter de futurs incidents de confidentialité *(voir article 2.5.2 – Processus de traitement d'un incident de confidentialité).* La protection de la confidentialité des données est un enjeu majeur de nos sociétés modernes, c'est pourquoi notre entreprise s'est assurée de prendre des mesures actives afin de protéger les informations sensibles qu'elle détient.

2.5.2 Processus de traitement d'un incident de confidentialité

Le traitement d'un incident de confidentialité implique plusieurs étapes clés pour identifier, gérer et résoudre efficacement la violation de la confidentialité;

1. Détection de l'incident :

La première étape consiste à détecter l'incident. Cela peut se faire grâce à des alertes de sécurité, des rapports d'employés ou d'autres sources d'information.

2. Évaluation initiale :

La personne responsable de la protection des renseignements personnels de l'entreprise (*Mme. Julie Landry*) procède à l'évaluation du type d'incident et détermine si celui-ci requiert la

constitution d’une équipe responsable de la gestion de l’incident. Cette équipe peut inclure des experts en sécurité informatique, des responsables de la conformité, des responsables des systèmes d'information, des avocats et d'autres parties prenantes. Par la suite, l'équipe effectue une enquête pour comprendre la nature et l'étendue de l'incident, y compris quelles données ont été compromises, comment cela s'est produit et qui est potentiellement affecté.

3. *Containment* (confinement/rétention de l’information) :

Une fois que l'incident est bien cerné, l'équipe de réponse à l'incident prend des mesures pour contenir la situation. Cela peut inclure l'isolation des systèmes compromis, la désactivation des comptes d'accès non autorisé et la mise en place de pare-feu temporaires pour arrêter la propagation de l'incident.

4. Investigation numérique :

Une enquête forensique est menée pour déterminer la cause de l'incident, les méthodes utilisées par les attaquants, les vecteurs d'attaque et la portée de la compromission. Des preuves numériques sont collectées et préservées pour une éventuelle enquête légale.

5. Notification des parties prenantes :

Si des données personnelles ou sensibles ont été compromises et si la réglementation l'exige, les parties prenantes affectées, y compris les clients, les employés et les autorités de réglementation, seront informées de l'incident de confidentialité.

6. Réponse corrective :

L'équipe de réponse à l'incident travaille à résoudre les vulnérabilités ou les faiblesses qui ont permis l'incident. Cela peut inclure la mise à jour des systèmes, la correction des erreurs de configuration, le renforcement des politiques de sécurité, etc.

7. Rapport post-incident :

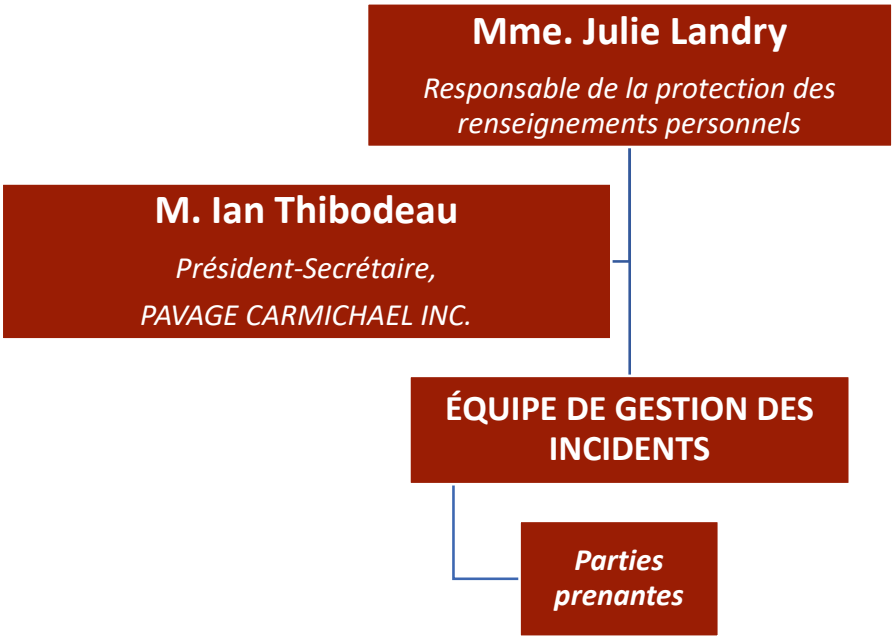
Après la résolution de l'incident, une analyse post-incident est effectuée pour évaluer les leçons apprises et les améliorations à apporter aux pratiques de sécurité. Un rapport complet sur

l'incident est généralement produit pour documenter les détails de l'incident, les mesures prises et les recommandations pour l'avenir.

8. **Bilan (mieux prévenir) :**

Enfin, des mesures de prévention sont mises en place pour éviter que des incidents similaires se reproduisent à l'avenir. Cela peut inclure des mises à jour de politiques, la formation des employés, la mise en œuvre de technologies de sécurité avancées, etc.

2.5.3 Liste des personnes avisées en cas d'incident et délais de notification



PAGAVE CARMICHAEL INC. croit que la rapidité et l'efficacité de la réponse peuvent avoir un impact significatif sur la gravité de l'incident et sur les répercussions de ceux-ci sur nos employés et partenaires. C'est pourquoi le processus ci-haut mentionné, est prêt à être activé dès l'apparition d'une fuite de confidentialité ou d'un simple doute d'incident.

3 - CONCLUSION

3.0 Conclusion

PAVAGE CARMICHAEL INC.
437 rue des Montérégiennes
Québec, Qc G1C 7J7
T 418 849-8713 F 418 686-1744

3.0 Conclusion

La loi 25 sur la protection des renseignements personnels représente une avancée majeure dans la préservation de la vie privée et de la sécurité des données personnelles au sein de notre société. En fournissant un cadre juridique solide et des normes de protection des données, cette loi a permis de renforcer la confiance des individus dans la manière dont leurs informations personnelles sont traitées et utilisées par les entreprises et les organisations.

L'application de la loi 25 a un impact significatif sur la manière dont ***PAVAGE CARMICHAEL INC.*** collecte, *stocke* et traite les données personnelles. Comme la mise en place des politiques de protection des données robustes, la nomination des responsables de la protection des données et la notification des violations de données aux autorités compétentes et aux individus concernés. Cela nous a conduit à une amélioration globale de la sécurité des données et à une meilleure transparence quant à la manière dont les données personnelles sont gérées.

De plus, la loi 25 a permis d'accroître la sensibilisation à la protection des données personnelles et à la vie privée, incitant nos collaborateurs à être plus prudents quant à la divulgation de leurs informations personnelles et à l'exigence d'un meilleur contrôle sur leurs données.

En conclusion, notre engagement quant à l'application de la loi 25 a apporté des avantages significatifs en matière de protection de la vie privée et de sécurité des données personnelles. C'est pourquoi, il est impératif de continuer à surveiller et renforcer la présente politique pour garantir que les droits et les informations personnelles des individus sont protégés de manière adéquate à l'ère numérique en constante évolution.