



LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Nomination d'un agent de conformité

De mettre en œuvre, de surveiller, de mettre à jour et d'exécuter le programme de conformité, y compris :

- Les politiques et les procédures
- La formation et la sensibilisation
- L'autorévision/autoévaluation du programme

De superviser le processus en cas d'atteinte à la vie privée, et de traiter les demandes de renseignements et les plaintes des clients

De faire état des nouveaux risques, des risques existants, des activités de surveillance et des changements d'ordre législatif ou réglementaire qui auront une incidence sur le programme de conformité aux décideurs principaux du cabinet, et ce, sur une base régulière

L'agent de conformité devrait avoir les pouvoirs et les ressources nécessaires pour s'acquitter efficacement de ses obligations. Il ou elle devrait occuper un poste de direction au sein du cabinet et ainsi être en mesure d'avoir un accès direct aux décideurs principaux. L'agent de conformité peut déléguer certaines fonctions à d'autres employés. Toutefois, la mise en œuvre du programme de conformité demeure la responsabilité de l'agent de conformité.

Nom : Geneviève Bauer

Titre : Directrice associée

Courriel : genevieve.bauer@planisource.com

La protection des renseignements personnels et nos affaires

Les clients fournissent des renseignements personnels qui sont essentiels aux affaires du cabinet. Il est crucial de protéger ces renseignements afin de maintenir leur confiance. La loi du Québec pertinente, la Loi sur la protection des renseignements personnels dans le secteur privé régit la collecte, l'utilisation et la communication des renseignements personnels. Par « renseignements personnels », on entend toute donnée se rapportant à une personne identifiable, y compris les données médicales ou financières, de même que les données d'affaires si elles n'ont pas été classées dans la catégorie des « coordonnées d'affaires ». Cette catégorie comprend le titre professionnel, le numéro de téléphone et



l'adresse courriel d'affaires de la personne, de même que les données qui sont utilisées dans le cadre de son emploi, de son entreprise ou de sa profession.

Planisource Inc. est responsable des renseignements personnels dont il a la gestion, et il lui incombe de prendre toutes les mesures nécessaires pour assurer la sécurité des renseignements personnels et confidentiels en sa possession. Dans certaines situations, cela signifie d'adopter de nouvelles pratiques commerciales afin de protéger la confidentialité des renseignements personnels.

Politique

Planisource Inc. met à la disposition du public l'information relative à ses politiques et à ses procédures, et il se conforme aux normes de confidentialité des compagnies qu'il représente (p. ex., la Canada Vie, Services d'investissement Quadrus, cabinet de services financiers Horizon groupe Financier, etc.). Puisque Planisource possède un site web, vous y retrouverez nos normes en matière de protection des renseignements personnels décrivant la façon dont les renseignements personnels sont recueillis, utilisés, divulgués et conservés, ou encore il renferme un lien vers de telles normes.

Préoccupation et demande de renseignements ou requêtes généraux.

Le titre et les coordonnées de la personne responsable de la protection des renseignements personnels sont affichés sur le site Web du cabinet : www.planisource.com

Toutes les préoccupations, demandes de nature générale ou requêtes liées à la confidentialité et au cabinet sont transmises à l'agent de conformité du cabinet. Ce dernier examinera les demandes et en accusera réception dans les 24 heures ; en son absence, les demandes seront transférées à une personne appropriée aux fins de traitement. Le client sera tenu au courant du progrès que réalise l'agent de conformité à l'égard de la situation, et la documentation complète de la préoccupation signalée et toutes les activités s'y rattachant seront conservées dans le dossier du client.

L'agent de conformité du cabinet fait suivre toutes les préoccupations, demandes de nature générale ou requêtes liées à la confidentialité et aux produits et services de la compagnie au chef de la conformité de cette compagnie.

Demandes de clients visant à accéder aux renseignements personnels

En vertu des lois relatives à la protection des renseignements personnels, les clients ont le droit d'accéder à leurs renseignements personnels consignés dans des dossiers tenus par le cabinet ou la compagnie et de contester leur exactitude, le cas échéant. Le cabinet a mis en place des procédures pour recueillir et fournir des renseignements personnels en réponse à une demande d'accès du client à ses renseignements personnels.

Procédure

Toute demande d'accès d'un client à ses renseignements personnels consignés dans les dossiers de client du cabinet est envoyée à l'agent de conformité du cabinet afin qu'il réponde à la demande du client dès que possible, et au plus tard 30 jours après la réception de la demande. 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. La demande peut





être envoyée par courriel ou par courrier postal. L'agent de la conformité aidera le client à préparer sa demande d'accès, au besoin.

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 être authentifiée de manière satisfaisante, Espace Finance peut refuser de divulguer les renseignements personnels demandés.

Corrigez ou modifiez tout renseignement personnel si son exactitude ou son intégralité sont remises en question et s'il s'avère que ce renseignement est effectivement erroné ou incomplet. Consignez au dossier tous les désaccords relatifs aux renseignements et, le cas échéant, informez-en les tierces parties.

Avant de communiquer les renseignements personnels de à l'individu que le demande, le responsable examine attentivement les informations au dossier pour s'assurer qu'elles ne contiennent pas de renseignements tiers confidentiels. Si tel est le cas, il faut vérifier s'ils doivent être exclus de la divulgation.

Si un client demande d'accéder à ses renseignements personnels détenus par la compagnie, suivez les processus qu'a établis cette dernière.

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 délais 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. Ce dernier contient les informations suivantes ;

- Date de réception de la demande
- Date de l'accusé de réception
- Date de la vérification de l'identité
- Méthode de vérification utilisée
- Décision : demande d'accès acceptée ou refusée
- Date de la communication des renseignements (si applicable)

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.

Voir la section traitement des plaintes dans le Programme de conformité visant l'assurance





Usage à mauvais escient des renseignements personnels

L'agent de conformité du cabinet doit signaler sans délai tout usage à mauvais escient de renseignements personnels ou toute atteinte possible aux mesures de sécurité quant aux produits et aux services de la compagnie au chef de la conformité de la compagnie.

Processus visant les incidents en matière de confidentialité et les atteintes à la vie privée

Une atteinte à la vie privée survient lors de la divulgation non autorisée de renseignements personnels, de l'accès non autorisé à de tels renseignements ou de la perte de renseignements personnels découlant d'une atteinte aux mesures de sécurité. Une atteinte à la vie privée se produit également lorsque des renseignements personnels sont conservés d'une façon non conforme à la législation relative à la protection des renseignements personnels, comme lorsque des renseignements personnels sont conservés même s'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés.

Toutes les atteintes doivent faire l'objet d'une évaluation afin de déterminer le risque pour le client.

Les évaluations peuvent être qualifiées de risques réels de préjudice grave (RRPG) ou de risque de préjudice sérieux (RPS, semblable au RRPG), et seront désignées par le terme « évaluation » dans l'ensemble du présent document. Lorsque l'évaluation détermine que le risque est grave ou sérieux, l'atteinte doit être signalée à la Commission d'accès à l'information (OPC) au Québec et/ou au Commissariat fédéral à la protection de la vie privée du Canada (CPVP) et aux commissaires provinciaux à la protection de la vie privée en dehors du Québec, selon le cas, tous étant désignés par le terme « le commissaire ».

Le cabinet prend au sérieux les atteintes présumées ou réelles, les plaintes ou toutes les préoccupations reliées à un problème de confidentialité, peu importe qu'elles touchent une personne ou un fournisseur, sont immédiatement déclarées à l'agent de conformité du cabinet et à la compagnie.

L'agent de conformité du cabinet empêchera la divulgation des renseignements, évaluera la situation, corrigera la situation et contribuera à l'amélioration des mesures de contrôle afin d'éviter toute atteinte semblable à l'avenir.

Processus de confinement des atteintes

En cas d'atteinte à la vie privée touchant les renseignements des clients (p. ex., cyberattaque, accès non autorisé aux données), communiquez avec :

- L'agent de conformité de l'entreprise, Geenvieve Bauer
- Les partenaires du cabinet tel que La Conformité des conseillers pour les affaires de la Canada Vie, Groupe Financier Horizon et Quadrus Investissement Ltée
- Les autres compagnies visées ainsi que les organismes de réglementation concernés.

Processus de documentation

Commencer le processus de documentation de toute atteinte à la vie privée dès que cette atteinte est contenue. Tous les dossiers d'atteinte à la vie privée doivent être conservés de façon sûre.





Au Québec, le cabinet doit tenir à jour un registre de toutes les atteintes à la vie privée pendant cinq ans à partir du moment où il a pris connaissance de l'atteinte et être prêt à fournir ce registre à la Commission d'accès à l'information (CAI) sur demande.

À l'extérieur du Québec, conservez les dossiers sur toutes les atteintes à la vie privée pendant 24 mois. La pratique devrait être en mesure de fournir les dossiers au commissaire ou à d'autres organisations sur demande.

Le ou les dossiers doivent être gardés dans un endroit sûr et comprendre ce qui suit :

- Date de l'atteinte
- Description des circonstances de l'atteinte
- Nombre de personnes visées
- Types de renseignements personnels en cause
- Sensibilité de l'information visée par l'atteinte
- Probabilité de l'utilisation à mauvais escient
- Préjudice potentiel qui pourrait découler de l'atteinte
- Un indicateur pour confirmer :
 - o Si l'atteinte a entraîné un risque grave ou sérieux pour la personne, et une explication quant à cette conclusion
 - o Que la ou les personnes visées ont été avisées
 - o La date de confirmation et d'avis visant le commissaire pour ceux qui vivent à l'extérieur du Québec et qui sont touchés par l'atteinte
- Mesures prises pour éviter que des atteintes semblables se reproduisent

Les cabinets du Québec doivent aussi consigner les renseignements suivants :

- Date à laquelle le cabinet a été mis au courant de l'incident
- Si la description des renseignements personnels n'est pas fournie, indiquez pourquoi
- Si on détermine qu'il y a un risque grave ou sérieux – la date et la confirmation de l'avis à la CAI et aux personnes touchées et si des avis publics ont été émis et les raisons de l'avoir fait.

Un registre de suivi comprenant une liste de toutes les atteintes à la vie privée par région consignée à un seul endroit peut aussi être conservé. Les cabinets du Québec peuvent s'en servir comme registre pour les besoins de la CAI.

Déclaration obligatoire des atteintes à la vie privée en vertu des lois provinciales en matière de protection des renseignements personnels ou de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).

- Si le cabinet détermine que l'incident présente un risque grave ou sérieux, les personnes visées doivent être avisées, si cela n'interfère pas avec une enquête officielle, et selon l'emplacement des personnes concernées, il faut faire une déclaration au CAI (au Québec) et au commissaire, et ce, dès que possible et même s'il n'y a qu'une seule personne visée.
- Le cabinet doit également informer de l'incident toute autre organisation ou entreprise qui pourrait atténuer le préjudice aux personnes concernées (p. ex., ajouter un indicateur aux comptes des clients). Pour les clients de la Canada Vie, communiquez avec l'équipe [Conformité des conseillers, Québec](#) ou avec l'équipe [Conformité des conseillers](#). Dans le cas de tout autre produit vendu à travers Groupe Financier Horizon ou Quadrus Investissement Ltée, communiquer avec leur équipe respective de conformité.





Avis aux personnes concernées

Le cas échéant, un avis sur l'atteinte aux mesures de protection des renseignements personnels sera fourni par le cabinet aux personnes concernées et il doit renfermer les éléments suivants :

- une description des circonstances de l'atteinte;
- la date à laquelle l'atteinte s'est produite ou la période sur laquelle elle s'est échelonnée, ou, si les dates précises sont inconnues, une approximation des dates;
- une description des renseignements personnels touchés, dans la mesure où il est possible de le déterminer; d. une description des mesures que la pratique a mises en place pour réduire les risques de préjudice découlant de l'atteinte;
- une description des mesures que pourraient prendre les personnes concernées pour réduire les risques de préjudice découlant de l'atteinte ou atténuer ces préjudices; et f. les coordonnées permettant aux personnes concernées de se renseigner davantage au sujet de l'atteinte.

Avis aux organismes de réglementation dans le cas des atteintes considérées comme des RRP/RS

- Envoyez un avis à la Commission d'accès à l'information (CAI) en téléchargeant le Formulaire de déclaration d'un incident de sécurité portant atteinte à des renseignements personnels du site Web de la CAI. Vous référer au site web suivant : [Pour les citoyens - Commission d'accès à l'information du Québec \(gouv.qc.ca\)](http://www.cai.gc.ca/fr/les_citoyens)
- Envoyez un avis au Commissariat à la protection de la vie privée du Canada (fédéral) au moyen du formulaire [Formulaire : Rapport d'atteinte à la LPRPDE \(priv.gc.ca\)](http://www.priv.gc.ca/fr/rapport_d_atteinte).

Amélioration des mesures de contrôle

Passez en revue tous les processus, toutes les mises à jour du système, toutes les formations des employés, puis apportez des améliorations au besoin afin d'éviter que les incidents ne se reproduisent. Comme cela est décrit à la section 2.4 « Processus de documentation », évaluez les mesures de contrôle qui peuvent être améliorées pour réduire au minimum les risques futurs et instaurez les nouvelles mesures de contrôle nécessaires pour faire face aux risques.

Obtenir l'autorisation valide et éclairée du client

L'autorisation est considérée comme valide uniquement s'il est raisonnable de s'attendre à ce que les personnes comprennent la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication de leurs renseignements personnels auxquelles elles consentent

Politique

Au début de la relation avec un client, Planisource Inc. obtiendra son autorisation écrite pour la collecte, l'utilisation et la communication de ses renseignements personnels et l'aviser de la possibilité de stocker ces renseignements à l'extérieur du Canada.





Lors d'interactions ultérieures au cours desquelles des renseignements personnels supplémentaires sont recueillis, nous vérifions verbalement que le consentement est toujours valable et nous le notons dans le dossier du client.

En ce qui concerne les personnes âgées de moins de 14 ans, le consentement doit être donné par le titulaire de l'autorité parentale ou par le tuteur, sauf si la collecte des renseignements est manifestement dans l'intérêt de la personne mineure.

Les clients sont informés que leurs renseignements personnels peuvent éventuellement être divulgués à l'extérieur du Canada ou de leur province de résidence dans le cadre des activités quotidiennes, y compris à des fins de stockage. Avant que les renseignements personnels ne soient transférés à l'extérieur du Québec, une Évaluation des répercussions sur la protection des renseignements personnels sera effectuée.

Lors de la collecte de renseignements auprès de clients existants et potentiels, expliquez le but de la collecte de ces renseignements et fournissez des renseignements sur les politiques en matière de protection des renseignements personnels du cabinet.

Communiquez uniquement des renseignements personnels sur les clients à une autre personne ou société si une autorisation verbale ou écrite du client a été obtenue ou lorsque la loi vous y autorise ou vous y oblige. S'il s'agit de renseignements de nature délicate, vous devez obtenir une autorisation écrite.

Le cabinet recommandera les services d'autres professionnels ou conseillers aux clients s'ils en font la demande ou si les clients peuvent tirer avantage de tels services. Le cabinet ne fournit jamais le nom des clients ni d'autres renseignements les concernant à des tiers susceptibles d'utiliser ces renseignements en vue d'offrir leurs services, à moins que les clients en aient été informés et y aient consenti.

Nouveaux droits d'accès et nouvelles utilisations des renseignements du client

Politique

Planisource Inc obtiendra l'autorisation écrite du client advenant tout changement de l'objectif ayant motivé la collecte, l'utilisation et la communication des renseignements personnels du client, ainsi que l'accès à ceux-ci.

Procédure

Nous passons en revue le nouvel objectif et les nouveaux droits d'accès, d'utilisation et de communication avec le client et conservons une copie de la nouvelle autorisation dans le dossier de client.

Si le client s'oppose à un transfert ou aux nouveaux droits d'accès, il peut :

- Demander que ses renseignements ne soient pas communiqués
- Demander de faire affaire avec un nouveau conseiller
- Demander le nom d'autres conseillers qu'il peut joindre ou le nom et le numéro de téléphone du directeur général régional auquel il peut s'adresser pour demander un autre conseiller





Évaluations des répercussions sur la protection des renseignements personnels (ERPRP)

Le cabinet réalisera une ERPRP avant de modifier ou de remanier un système qui implique le traitement de renseignements personnels – la collecte, l'utilisation, la communication, le stockage ou la destruction de tels renseignements. L'objectif de l'ERPRP est de définir les risques liés à la protection des renseignements personnels et de mettre en place des mesures de protection des renseignements personnels avant de procéder à un changement. Il peut s'agir d'un transfert de renseignements à l'extérieur du Québec, de la préparation de renseignements sur les clients en vue de leur transfert de dossiers papier à des dossiers électroniques, de l'ajout de nouveaux fournisseurs de services ou de logiciels.

L'évaluation et les mesures de protection seront proportionnelles à la sensibilité des renseignements personnels visés.

Procédure suivie

Nous effectuons une évaluation des répercussions sur la protection des renseignements personnels (ERPRP)

Le cabinet doit d'abord consulter son agent de conformité, qui devra superviser et approuver la mesure prévue. Commencez l'évaluation, qui doit comprendre une description de la mesure à prendre et tenir compte d'éléments tels que :

- Quel type de renseignements personnels sont concernés (nom, adresse, NAS); se limitent-ils à ce qui est nécessaire?
- De nouveaux renseignements sont-ils collectés et comment?
- Quel est le degré de sensibilité des renseignements personnels?
- Des renseignements seront-ils collectés pour permettre de repérer, identifier ou définir des actions ou des comportements, notamment par l'utilisation de témoins ou de pixels?
- Comment ces renseignements seront-ils utilisés et y aura-t-il un nouvel objectif? • Un nouveau consentement est-il nécessaire?
- Quelle est la quantité de renseignements concernés?
- Quelles mesures sont en place pour protéger les renseignements.
- Sur quel support les renseignements sont-ils stockés?
- Qui aura accès aux renseignements?
- Ces renseignements sont-ils transmis à un tiers?
- Des procédures ont-elles été mises en place pour faire respecter les droits en matière de protection des renseignements personnels, c'est-à-dire la rectification, l'accès, etc.
- Les exigences en matière de conservation et de destruction peuvent-elles être respectées? • Si des renseignements sont transférés à l'extérieur du Québec, où vont-ils et quelles sont les lois applicables?
- Y aura-t-il une technologie de prise de décision automatisée et un être humain peut-il outrepasser la décision?
- Le système décisionnel automatisé fournira-t-il une piste d'audit?





Si un fournisseur est concerné, reportez-vous à la section 3.1.2 Contrats avec les fournisseurs. Attribuez un niveau de risque inhérent (faible, moyen, élevé), définissez la manière dont ces risques seront atténués et déterminez le niveau de risque résiduel. Vous devez vous abstenir de prendre des mesures si les renseignements personnels sont exposés à des risques nouveaux ou supplémentaires.

Contrats avec les fournisseurs

Politique

Le cabinet exige l'autorisation du client avant de transférer les renseignements d'un client à un fournisseur et conserve le contrôle sur les renseignements lors du transfert de renseignements personnels à un fournisseur aux fins de traitement.

Les transferts de renseignements aux fournisseurs aux fins de traitement, y compris les services infonuagiques, sont effectués pour différentes raisons, notamment le stockage de données et le traitement ou la manipulation des renseignements personnels du client.

Procédure

Avant de conclure, de modifier substantiellement ou de renouveler une entente contractuelle avec un fournisseur, le cabinet évalue les mesures de protection afin de s'assurer que le fournisseur est en mesure de protéger les renseignements du client de façon appropriée.

Le cabinet effectuera une vérification auprès d'un conseiller juridique avant d'accepter les modalités du fournisseur et conservera une copie imprimée de l'entente pour ses dossiers.

Exception visant les autorisations de transactions commerciales

Les transactions commerciales comprennent, par exemple, la vente d'un cabinet, une fusion de deux organisations ou plus ou toute autre entente prescrite entre deux organisations ou plus visant à mener une activité commerciale.

Politique

Lorsque nécessaire, le cabinet transfère des renseignements personnels afin de déterminer si une transaction doit être effectuée ou afin d'effectuer une transaction. Les renseignements doivent uniquement être utilisés ou communiqués aux fins relatives à la transaction, protégés de façon adéquate, retournés ou détruits lorsqu'ils ne sont plus nécessaires à cette fin, et les clients concernés doivent être avisés que leurs renseignements personnels ont été transférés à une autre organisation.

Procédure

Lors de la réception de renseignements personnels, le cabinet conclut une entente visant à utiliser ou à communiquer les renseignements uniquement dans le cadre de la transaction et à les protéger et à les retourner ou à les détruire si la transaction n'est pas effectuée. Si la transaction est effectuée, le cabinet avisera les clients concernés que leurs renseignements personnels ont été transférés à une autre organisation.





Collecte de renseignements personnels

Politique

Lors de la collecte de renseignements personnels :

- Planisource Inc. limite la quantité et le type des renseignements recueillis au strict nécessaire pour la réalisation des fins visées.
- Nous faisons tous les efforts raisonnables pour veiller à ce que les renseignements sur les clients existants et éventuels faisant partie des dossiers clients soient exacts et mis à jour ou corrigés au besoin.
- Nous prenons les mesures nécessaires afin de nous assurer que les renseignements recueillis sont utilisés aux fins déterminées et non à d'autres fins, et qu'ils ne sont pas communiqués à une tierce partie sans le consentement du client existant ou éventuel, sauf indication contraire dans la loi.
- Si des renseignements personnels sont recueillis dans un site Web ou une autre technologie accessible au public qui permet d'identifier, de localiser ou de profiler la personne, le paramètre par défaut doit être que la fonction à cet effet soit désactivée et une formulation facile à comprendre doit être fournie pour permettre à la personne de choisir les options qu'elle préfère en matière de protection des renseignements personnels.
 - Les paramètres de confidentialité doivent être définis par défaut au plus haut niveau.

Les paramètres par défaut des fonctionnalités reliées à l'établissement de profils ou de géolocalisation doivent être désactivés. (gestionnaire de témoins désactivé par défaut sur le site web). Seuls les témoins essentiels sont acceptés.

Contrats avec les fournisseurs

Politique

Le cabinet exige l'autorisation du client avant de transférer les renseignements d'un client à un fournisseur et conserve le contrôle sur les renseignements lors du transfert de renseignements personnels à un fournisseur aux fins de traitement.

Les transferts de renseignements aux fournisseurs aux fins de traitement, y compris les services infonuagiques, sont effectués pour différentes raisons, notamment le stockage de données et le traitement ou la manipulation des renseignements personnels du client.

Procédure

Avant de conclure, de modifier substantiellement ou de renouveler une entente contractuelle avec un fournisseur, le cabinet évalue les mesures de protection afin de s'assurer que le fournisseur est en mesure de protéger les renseignements du client de façon appropriée.

Le cabinet effectuera une vérification auprès d'un conseiller juridique avant d'accepter les modalités du fournisseur et conservera une copie imprimée de l'entente pour ses dossiers.





Exception visant les autorisations de transactions commerciales.

Les transactions commerciales comprennent, par exemple, la vente d'un cabinet, une fusion de deux organisations ou plus ou toute autre entente prescrite entre deux organisations ou plus visant à mener une activité commerciale.

Lors de l'évaluation, le cabinet prend en considération les éléments suivants ; expérience d'affaires, réputation et leur politique en matière de protections des renseignements. Nous revoyons leur politique en ce qui a trait aux ; Déclaration des incidents, Planification des urgences, Stockage des renseignements à l'extérieur de la province (Québec), et le Stockage des renseignements à l'extérieur du pays.

Les transactions commerciales comprennent, par exemple, la vente d'un cabinet, une fusion de deux organisations ou plus ou toute autre entente prescrite entre deux organisations ou plus visant à mener une activité commerciale.

Politique

Lorsque nécessaire, le cabinet transfère des renseignements personnels afin de déterminer si une transaction doit être effectuée ou afin d'effectuer une transaction. Les renseignements doivent uniquement être utilisés ou communiqués aux fins relatives à la transaction, protégés de façon adéquate, retournés ou détruits lorsqu'ils ne sont plus nécessaires à cette fin, et les clients concernés doivent être avisés que leurs renseignements personnels ont été transférés à une autre organisation.

Procédure

Lors de la réception de renseignements personnels, le cabinet conclut une entente visant à utiliser ou à communiquer les renseignements uniquement dans le cadre de la transaction et à les protéger et à les retourner ou à les détruire si la transaction n'est pas effectuée. Si la transaction est effectuée, le cabinet avisera les clients concernés que leurs renseignements personnels ont été transférés à une autre organisation.

Collecte de renseignements personnels

Politique

Lors de la collecte de renseignements personnels :

- Planisource Inc. limite la quantité et le type des renseignements recueillis au strict nécessaire pour la réalisation des fins visées.
- Nous faisons tous les efforts raisonnables pour veiller à ce que les renseignements sur les clients existants et éventuels faisant partie des dossiers clients soient exacts et mis à jour ou corrigés au besoin.
- Nous prenons les mesures nécessaires afin de nous assurer que les renseignements recueillis sont utilisés aux fins déterminées et non à d'autres fins, et qu'ils ne sont pas communiqués à une tierce partie sans le consentement du client existant ou éventuel, sauf indication contraire dans la loi.
- Si des renseignements personnels sont recueillis dans un site Web ou une autre technologie accessible au public qui permet d'identifier, de localiser ou de profiler la personne, le paramètre par défaut doit être que la fonction à cet effet soit désactivée et une formulation





facile à comprendre doit être fournie pour permettre à la personne de choisir les options qu'elle préfère en matière de protection des renseignements personnels.

- Les paramètres de confidentialité doivent être définis par défaut au plus haut niveau.

Les paramètres par défaut des fonctionnalités reliées à l'établissement de profils ou de géolocalisation doivent être désactivés. (Gestionnaire de témoins désactivé par défaut sur le site web). Seuls les témoins essentiels sont acceptés.

Site web Planisource Inc.

Notre site web est hébergé sur la plateforme Bluehost. Celui-ci utilise un programme de sécurité de l'information basé sur les meilleures pratiques internationales et une sécurité multicouche. Leur programme est en constante évolution pour faire face aux menaces émergentes. Ils mettent également en œuvre un cryptage des données en utilisant HTTPS, TLS 1.2 et plus, et SSL. Les données sont cryptées lorsqu'en transit tandis que les données au repos utilisent AES-256, la norme de cryptage la plus puissante sur le marché.

Pour les visiteurs de notre site web, le gestionnaire des témoins (aussi appelé « cookies ») est désactivé par défaut afin de limiter au strict minimum les données récoltées par le site (témoins essentiels). Si un visiteur décide de l'activer en acceptant les cookies, nous pouvons alors recueillir des renseignements sur votre visite afin de mesurer l'efficacité de notre site web ou de rehausser son expérience client.

Lorsqu'un visiteur fait une demande de renseignements via notre formulaire de prise de contact, il accepte que Planisource Inc. recueille son nom, son numéro de téléphone, son adresse électronique et tout autre renseignement qu'il décide de nous fournir via le formulaire. Espace Finance utilise ces renseignements strictement pour communiquer avec ses visiteurs et répondre à leurs questions ou demandes.

Par précaution, nous recommandons toutefois aux visiteurs de ne jamais nous faire parvenir d'information personnelle ou sensible via cette plateforme.

Enregistrement des entretiens téléphoniques avec les clients

Politique

Tout enregistrement des appels avec les clients implique la collecte de renseignements personnels. Par conséquent, l'appelant doit consentir à l'enregistrement. Le client est informé que la conversation est enregistrée dès le début de l'appel. Un effort raisonnable est fait pour s'assurer que le client est au courant des fins auxquelles servira l'enregistrement.

Utilisation, communication et conservation

Politique

Les renseignements personnels ne doivent pas, sans consentement, être utilisés ou communiqués à un tiers à des fins autres que celles auxquelles ils ont été recueillis, sauf si cette utilisation ou communication est requise ou permise par la loi.





Le cabinet ne conserve les renseignements personnels que pendant la période où ils sont nécessaires aux fins déterminées ou comme requis ou permis par la loi, et est entièrement responsable de la garde en lieu sûr de ces documents et de la protection de la confidentialité de ceux-ci. En outre, s'il existe des raisons sérieuses et légitimes de conserver les renseignements personnels, ceux-ci peuvent être conservés, mais ils doivent être rendus anonymes au moyen de pratiques exemplaires généralement acceptées. Les renseignements personnels qui ne sont plus nécessaires aux fins précisées au moment de la collecte sont détruits ou effacés de façon sécuritaire.

Le cabinet maintient un dossier sur toutes les ERPRP tout au long du processus et, une fois, les ERPRP terminées, pendant cinq ans.

Destruction sécuritaire

Politique

- Les documents papier renfermant tout renseignement personnel concernant un client existant ou éventuel doivent être détruits par déchiquetage, et non recyclés.
- Les renseignements sont supprimés de tous les supports électroniques avant la destruction de ces derniers. Les dispositifs de stockage doivent être détruits afin de s'assurer que les données qu'ils contiennent ne peuvent pas être récupérées.
- Lors de l'élimination ou de la destruction des renseignements personnels, prenez les mesures appropriées pour empêcher les parties non autorisées d'accéder aux renseignements.
- Au moment de se défaire d'équipements ou d'appareils utilisés pour conserver des renseignements personnels (par exemple, des classeurs, des ordinateurs, des disquettes et des bandes sonores), prenez les mesures appropriées pour supprimer tous les renseignements consignés ou empêcher autrement des parties non autorisées d'y accéder.

Conservation des documents

Politique

Les dossiers, évaluations et documents relatifs aux clients du cabinet doivent être conservés pendant au moins la durée minimale stipulée par la loi.

Procédure

Le cabinet conserve les dossiers pendant la période la plus longue des exigences suivantes en matière de conservation :

- Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes – les dossiers des clients doivent être conservés pendant cinq ans à compter de la date de la dernière transaction.
- Exigences de l'Organisme canadien de réglementation des investissements (OCRo) – Les dossiers/documents des clients relatifs aux fonds communs de placement doivent être conservés pendant sept ans à compter de la date de création du dossier.
- Réglementation québécoise à l'égard des cabinets – Les dossiers clients doivent être conservés pendant cinq ans après la fermeture définitive du dossier client, la dernière date de prestation d'un service au client (par le cabinet) ou l'échéance sans renouvellement ou remplacement du dernier produit vendu au client, selon la dernière éventualité.

Les dossiers peuvent être conservés au-delà de la période de conservation requise à des fins de litiges. Les dossiers conservés à ces fins doivent être stockés séparément, en toute sécurité, et n'être accessibles qu'en cas de litige.





Les bonnes pratiques généralement acceptées seront utilisées pour rendre anonymes les renseignements personnels conservés à des fins sérieuses et légitimes.

Mesures de protection

Politique

Les mesures de protection appropriées doivent être prises pour ce qui est du stockage et de l'élimination des renseignements sur les clients. Toutes les personnes liées au cabinet ou à son emploi sont tenues de respecter les procédures décrites dans cette section.

Procédure

Le cabinet utilise une combinaison de mesures de protection technologiques, physiques et organisationnelles pour protéger les renseignements personnels des clients contre le vol et la mauvaise utilisation, ainsi que contre l'accès, la communication, la reproduction, l'utilisation ou les modifications non autorisées.

Mesures de protection technologiques

Les outils technologiques nécessitant des mesures de protection comprennent entre autres :

- Les ordinateurs : ordinateurs de bureau, portables, serveurs et assistants personnels (tablettes et téléphones intelligents)
- Le matériel informatique et les logiciels
- Les appareils mobiles • Les médias portables – clés USB, CD, DVD
- Les imprimantes, numériseurs, télécopieurs et photocopieurs avec options d'impression sécurisées
- Le courrier électronique et les services Internet (p. ex. l'infonuagique) Chiffrement, antivirus et coupe-feu Politique
- Les logiciels de chiffrement, les antivirus et les coupe-feu sont installés et tenus à jour sur tous les outils technologiques utilisés en contexte professionnel afin d'assurer la sécurité des données des clients. Cela comprend le chiffrement des données de nature délicate lorsqu'elles sont stockées ou transmises, y compris lors de leur transmission vers les serveurs de sauvegarde.
- Les mesures de protection de ces outils technologiques sont revues régulièrement et mises à niveau lorsque nécessaire.
- Lorsque ces outils technologiques sont sans surveillance ou en cours de transport, tous les appareils doivent être fermés (éteints). Si vous ne faites que fermer votre session, verrouiller l'appareil ou le laisser en mode veille, les mesures de sécurité supplémentaires peuvent être inefficaces.

Courriel sécurisé

Protection à l'aide d'un mot de passe. Lorsque nous traitons des renseignements de nature délicate, les courriels comprenant ces renseignements sont sécurisés sont chiffrés.

Mesures de protection physiques

Nous tenons compte des mesures de sécurité suivantes :

Aménagement du bureau





- Les bureaux ou les espaces de travail sont aménagés de manière à ce qu'ils soient en retrait des aires de circulation du bureau.
- Les télécopieurs, les photocopieurs et les imprimantes sont placés dans les aires dont l'accès est plutôt restreint.
- Les associés ou les membres du personnel qui traitent les renseignements de nature délicate sont situés dans une aire de travail où les conversations ne peuvent pas être facilement entendues.
- Les dossiers de renseignements personnels des clients sont conservés à l'écart des aires de circulation sous verrou
- Les dossiers comprenant des renseignements personnels sont conservés dans des classeurs verrouillés.

Ordinateurs et appareils électroniques grand public

Peu importe où nous nous trouvons, que ce soit au bureau, à la maison, dans une chambre d'hôtel ou dans une salle de réunion, nous prenons les dispositions nécessaires pour protéger notre ordinateur portable et nos appareils mobiles contre le vol en utilisant un dispositif antivol (p. ex. un câble de verrouillage).

- Nous gardons nos appareils sous clé en lieu sûr lorsque vous ne les utilisons pas.
- Pour prévenir le vol, nous ne laissons pas notre ordinateur portable dans notre véhicule.
- Nous fermons notre ordinateur portable et le mettons hors tension – de cette façon, toutes les applications seront adéquatement fermées.
- Nous fermons toute session ouverte dans un site Web ou un programme quand nous n'avons plus à nous en servir. De plus, nous n'enregistrons pas nos renseignements de manière que la session s'ouvre automatiquement la fois suivante : ainsi si notre appareil mobile est perdu ou volé, une autre personne ne pourrait pas accéder à vos comptes ou dossiers.
- Nous rangeons les ordinateurs et appareils électroniques grand public (et, le cas échéant, les ordinateurs des associés ou membres du personnel) en lieu sûr pendant toute période d'absence (soirées, fins de semaine, congé de maladie ou vacances) de sorte à éviter tout accès non autorisé aux données

Bureaux et dossiers

Les renseignements personnels de nature délicate ou d'autres documents confidentiels ne doivent jamais être laissés sans surveillance. Lorsque des renseignements personnels doivent être imprimés pour être traités activement, tous les dossiers et leur contenu devraient être disposés de manière à ne pas être à la vue de personnes qui n'ont pas l'autorisation de les lire.

Tous les renseignements personnels de nature délicate doivent être conservés dans des pièces, des classeurs ou des tiroirs verrouillés et à accès restreint lorsqu'ils ne sont pas utilisés.

Conservation des documents à l'extérieur des lieux de travail

Il faut assurer la protection des renseignements des clients, qu'ils se trouvent dans un bureau personnel, dans une voiture ou dans tout autre lieu. Les dossiers papier qui renferment des renseignements personnels doivent être retirés du lieu de travail uniquement lorsque cela s'avère absolument nécessaire ou pour assurer un service approprié aux clients.





Aux fins de suivi et pour faciliter les démarches en cas de perte ou de vol, il faut prendre note de tous les dossiers ou documents avant qu'ils ne soient retirés du lieu de travail. Tous les associés et les membres du personnel doivent prendre connaissance de ces exigences et s'y conformer.

Boîte vocale

Les messages laissés aux clients ne doivent comporter aucun renseignement personnel à moins que le client en ait déjà été avisé. Le client doit aussi confirmer qu'il désire que ces renseignements lui soient laissés dans sa boîte vocale.

Identification de l'appelant

Si une demande est effectuée par téléphone, il est nécessaire d'identifier la personne avant de fournir quelque renseignement personnel que ce soit.

Pour identifier l'appelant, la personne doit répondre à trois des questions qui figurent dans la procédure interne d'identification de l'appelant.

Si les réponses ne sont pas exactes, indiquez à l'appelant que le cabinet est responsable de la protection de la vie privée et de la confidentialité des renseignements personnels du client et qu'il ne peut, par conséquent, divulguer des renseignements sans d'abord confirmer que l'appelant a bien droit de les obtenir. Demandez-lui de présenter sa demande par écrit.

Courrier

Tout document envoyé au client qui contient de l'information sensible, telle que, entre autres, des polices d'assurance, des renseignements médicaux, financiers, etc., doit être posté sous forme de poste recommandée, avec un numéro de suivi et une exigence de signature du destinataire (preuve de réception du client).

Courrier électronique

Les messages envoyés aux clients ne doivent comporter aucun renseignement personnel, à moins que le client en ait été avisé et qu'il ait consenti à ce que ces renseignements lui soient transmis par courriel.

La mise en garde suivante doit être ajoutée à tout courriel renfermant des renseignements personnels sur le client :

« Le contenu de la présente communication, y compris tout fichier joint, est confidentiel et peut être privilégié. Si vous n'êtes pas le destinataire visé (ou si vous ne recevez pas la présente communication au nom du destinataire visé), veuillez en aviser immédiatement l'expéditeur et supprimer ou détruire le présent message sans le lire, en tirer des copies, le retransmettre ou en enregistrer le contenu. Merci. À noter : Nous avons pris des mesures de protection contre les virus, mais nous n'assumons aucune responsabilité pour ce qui est de la perte ou des dommages causés par la présence d'un virus. »

Authentification de courriels

Les renseignements de nature délicate ne devraient pas être communiqués par courriel, sauf si le client en a fait la demande. Si une demande est effectuée par courriel, il est nécessaire d'identifier la personne avant de fournir des renseignements personnels par courriel selon la procédure détaillée interne d'authentification de courriels.





Télécopies

Les télécopies ne doivent pas comporter de renseignements personnels, à moins que le client en ait déjà été avisé et qu'il ait consenti à recevoir ces renseignements par télécopieur.

La mise en garde suivante doit être ajoutée au bordereau de toutes les télécopies comportant des renseignements personnels :

« Le contenu de la présente télécopie, y compris toute pièce jointe, est confidentiel et peut être privilégié. Si vous n'êtes pas le destinataire visé (ou si vous ne recevez pas la présente télécopie au nom du destinataire visé), veuillez en aviser immédiatement l'expéditeur et supprimer ou détruire la présente télécopie sans la lire, en tirer des copies, la retransmettre ou en enregistrer le contenu. Merci. »

Mesures de protection organisationnelles

Autorisation et limite d'accès uniquement en cas de nécessité

- L'accès aux renseignements personnels est accordé uniquement en cas de nécessité (c.-à-d. aux renseignements nécessaires pour accomplir certaines tâches). L'accès aux dossiers (papier, système ou électroniques) est revu lors de l'embauche d'associés ou de membres du personnel ou de leur transfert à un poste différent.
- Lorsqu'il est prévu qu'un associé ou membre du personnel quitte son emploi, il faut révoquer son accès aux renseignements sur les clients, y compris les données électroniques accessibles au moyen des ordinateurs et les renseignements consignés dans les documents se trouvant dans les aires de travail.
- Une liste complète des actions à prendre lors de la terminaison d'un employé a été mise en place.

Ententes de confidentialité

Les employés sont avisés de l'importance de protéger la sécurité et la confidentialité des renseignements personnels. Lorsque des renseignements personnels sont de nature délicate ou que les conséquences possibles d'une communication non appropriée sont importantes, le cabinet :

- Utilise les ententes de confidentialité avec les employés
- Prend des mesures appropriées pour protéger les renseignements de client contre des tiers qui peuvent avoir accès aux bureaux, notamment les agents de sécurité, les préposés à l'entretien ménager et les fournisseurs
- Obtient, le cas échéant, une entente de non-divulgence de la personne ou de l'entreprise chargée de la réparation de l'appareil si les renseignements confidentiels ne peuvent pas être retirés d'un appareil avant sa réparation
- Une liste est en place pour s'assurer de gérer adéquatement la suppression des accès des employés lorsqu'ils quittent l'employeur.

Adoption des politiques et des procédures



Politiques et procédures adoptées le 15 septembre 2023 par Réginald Barbe et tous les employés du cabinet.

Planisource Inc. s'engage à tenir à jour cette politique et à se former régulièrement afin de toujours répondre aux normes législatives en matière de protection des renseignements personnels.

