

# POLITIQUE DE CONFIDENTIALITÉ

## Table des matières

<b>POLITIQUE DE CONFIDENTIALITÉ</b> .....	<b>2</b>
<b>1. CONTEXTE ET POLITIQUE</b> .....	<b>2</b>
1.1. SOMMAIRE DES DIX PRINCIPES DE LA LPRPDE .....	2
<b>2. DÉFINITIONS</b> .....	<b>3</b>
<b>3. OBJECTIFS DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS</b> .....	<b>3</b>
<b>4. CONSENTEMENT</b> .....	<b>4</b>
<b>5. LIMITES DE LA COLLECTE</b> .....	<b>4</b>
<b>6. LIMITES D'UTILISATION, DE COMMUNICATION ET DE CONSERVATION</b> .....	<b>4</b>
6.1. UTILISATION DES RENSEIGNEMENTS PERSONNELS .....	4
6.2. COMMUNICATION ET TRANSFERT DES RENSEIGNEMENTS PERSONNELS.....	4
6.3. CONSERVATION DES RENSEIGNEMENTS PERSONNELS .....	5
<b>7. EXACTITUDE</b> .....	<b>5</b>
<b>8. MESURES DE SÉCURITÉ</b> .....	<b>5</b>
8.1. UTILISATION DES MESURES DE SÉCURITÉ .....	5
8.2. ATTEINTES AUX MESURES DE SÉCURITÉ .....	6
8.3. SUIVI DES ATTEINTES.....	6
<b>9. TRANSPARENCE</b> .....	<b>7</b>
<b>10. ACCÈS INDIVIDUEL</b> .....	<b>7</b>
<b>11. PLAINTES/RECOURS</b> .....	<b>7</b>
<b>ANNEXE 1 : FORMULAIRE : RAPPORT D'ATTEINTE À LA LPRPDE</b> .....	<b>9</b>
<b>ANNEXE 2 : ÉVALUER LE RISQUE RÉEL DE PRÉJUDICE GRAVE</b> .....	<b>10</b>
<b>ANNEXE 3 : ÉNONCÉ DE CONFIDENTIALITÉ</b> .....	<b>12</b>

# POLITIQUE DE CONFIDENTIALITÉ

## 1. CONTEXTE ET POLITIQUE

---

Cette politique a été mise au point pour se conformer à la *Loi sur la protection des renseignements personnels et les documents électroniques* (« LPRPDE » ou la « Loi »). La LPRPDE établit les règles de la collecte, de l'utilisation et de la communication de renseignements personnels dans le cadre des activités commerciales, conformément à leurs définitions dans la Loi.

### 1.1. Sommaire des dix principes de la LPRPDE

---

Les dix principes de la LPRPDE qui étayent la présente Politique de confidentialité sont les suivants :

1. **Responsabilité** : une organisation est responsable des renseignements personnels qu'elle collecte, utilise, conserve et communique dans le cadre de ses activités commerciales, y compris sans toutefois s'y limiter, la nomination d'un chef ou d'une cheffe de la protection des renseignements personnels;
2. **Détermination des fins de la collecte des renseignements** : les fins auxquelles les renseignements personnels sont recueillis doivent être déterminées par l'organisation au moment de la collecte; les renseignements ne peuvent être utilisés qu'à ces fins expresses;
3. **Consentement** : toute personne doit être informée par l'organisation de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir de façon expresse ou tacite;
4. **Limitation de la collecte** : l'organisation peut recueillir seulement le type et la quantité de renseignements personnels nécessaires et raisonnables aux fins déterminées;
5. **Limitation de l'utilisation, de la communication et de la conservation** : à moins que la personne concernée n'y consente, les renseignements personnels ne doivent être utilisés qu'aux fins auxquelles ils ont été recueillis et ne doivent pas être communiqués à de tierces parties;
6. **Exactitude** : l'organisation doit veiller à ce que les renseignements personnels soient aussi exacts, complets et à jour que possible;
7. **Mesures de sécurité** : l'organisation doit avoir recours à des mesures de sécurité matérielles, organisationnelles et technologiques pour protéger les renseignements personnels contre tout accès ou toute communication non autorisés.
8. **Transparence** : l'organisation doit informer ses clients de ses politiques et procédures de confidentialité et former son personnel à leur sujet;
9. **Accès aux renseignements personnels** : les personnes ont le droit d'accéder aux renseignements personnels sous la gestion de l'organisation qui les concernent et de remettre en question leur exactitude au besoin; et
10. **Offrir un droit de recours** : l'organisation doit informer ses clients et employés de la façon de demander l'accès aux renseignements personnels ou de porter plainte auprès du chef ou de la cheffe de la protection des renseignements personnels. Elle doit également répondre promptement à toute demande ou toute plainte déposée par une personne.

Cette politique de confidentialité est en vigueur pour le conseil des directeurs, les employés et les employés contractuels de Pender. De plus, Pender aura recours aux services de fournisseurs tiers pour signer les ententes de confidentialité avant tout transfert de renseignements personnels dans le cadre de son offre de services ou d'information.

## 2. DÉFINITIONS

---

« Coordonnées d'affaires » renvoient aux renseignements qui permettraient de communiquer avec une personne dans son lieu de travail et comprennent le nom, le titre ou le nom du poste, le numéro de téléphone au travail, l'adresse de l'entreprise, le courriel de l'entreprise ou le numéro de télécopieur de l'entreprise. Les coordonnées d'affaires ne sont pas visées par cette politique ni par la LPRPDE.

« Chef ou cheffe de la protection des renseignements personnels » renvoie à la personne qui a la responsabilité de veiller à ce que Pender respecte sa politique et la LPRPDE. Cette personne est Gina Jones, notre cheffe de la conformité.

« Base de données » renvoie à la liste des noms, adresses et numéros de téléphone des clients ou personnes, détenue par Pender sous forme de fichiers électroniques, documents papier et fichiers sauvegardés sur des disques durs informatiques, entre autres méthodes.

« Consentement exprès » signifie que la personne a signé un contrat, ou un autre formulaire renfermant des renseignements personnels, qui autorise Pender à recueillir, utiliser et communiquer les renseignements personnels de la personne aux fins déclarées dans le contrat.

« Consentement implicite » signifie que l'organisation a présumé que la personne a consenti à ce que ses renseignements personnels soient utilisés, conservés ou communiqués aux fins originalement déterminées, à moins d'avis contraire par la personne.

« Renseignements personnels » renvoient aux renseignements d'une personne pouvant être identifiée, notamment son nom, son âge, son adresse postale et son numéro de téléphone, son numéro d'assurance sociale, son statut matrimonial, sa religion, son revenu, ses antécédents de crédit, ses renseignements médicaux, son éducation et l'information sur son emploi. Les renseignements personnels n'incluent pas les coordonnées (décrites ci-dessous).

« Préjudice grave » vise notamment la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles.

« Tierce partie » renvoie à une personne ou entreprise qui fournit des services de soutien à Pender pour ses programmes, avantages sociaux et autres services offerts par Pender.

## 3. OBJECTIFS DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS

---

À moins que les objectifs de la collecte des renseignements personnels ne soient évidents et que le client fournisse volontairement ses renseignements personnels à ces fins, nous communiquerons les objectifs pour lesquels les renseignements personnels sont recueillis, oralement ou par écrit, avant ou au moment de la collecte.

Nous ne recueillons que les renseignements sur le client, le consommateur ou le membre qui sont nécessaires pour répondre aux besoins suivants :

- Vérifier l'identité;
- Vérifier la solvabilité;
- Connaître les préférences des clients;
- Comprendre les besoins financiers des clients;
- Ouvrir et gérer des comptes;
- Offrir les produits et services demandés;

- Offrir un service de grande qualité à nos clients; et
- Répondre aux exigences réglementaires.

#### **4. CONSENTEMENT**

---

Nous obtiendrons le consentement du client pour recueillir, utiliser ou divulguer des renseignements personnels (sauf si, comme indiqué ci-dessous, nous sommes autorisés à le faire sans consentement).

Le consentement peut être fourni [oralement, par écrit, par voie électronique ou par l'intermédiaire d'un représentant autorisé] ou il peut être implicite lorsque le but de la collecte, de l'utilisation ou de la communication des renseignements personnels sera considéré comme étant évident et que le client fournit volontairement des renseignements personnels à cette fin.

Sous réserve de certaines exceptions (par exemple, lorsque les renseignements personnels sont nécessaires pour fournir le service ou le produit ou lorsque le retrait du consentement nuirait à l'exécution d'une obligation légale), les clients peuvent retirer leur consentement ou refuser de consentir à ce que Pender utilise leurs renseignements personnels d'une certaine façon. La décision des clients de refuser de consentir ou de retirer le consentement à certaines utilisations des renseignements personnels pourrait restreindre notre habileté à offrir nos services. Dans une telle situation, nous expliquerons la situation afin de permettre aux clients de prendre des décisions éclairées.

#### **5. LIMITES DE LA COLLECTE**

---

Les renseignements personnels recueillis se limiteront aux fins énoncées dans la présente politique de confidentialité, les contrats Pender et/ou autres documents.

#### **6. LIMITES D'UTILISATION, DE COMMUNICATION ET DE CONSERVATION**

---

##### **6.1. Utilisation des renseignements personnels**

---

Les renseignements personnels ne seront utilisés qu'aux fins établies et auxquelles la personne a consenti, sous réserve des exceptions suivantes, permises en vertu de la LPRPDE :

- l'organisation a de bonnes raisons de croire que l'information serait utile dans le processus d'enquête d'une atteinte à une loi fédérale, provinciale ou de compétence étrangère et l'information est utilisée à cette fin;
- une situation urgente est présente qui met en danger la vie, la sécurité ou la santé d'une personne;
- l'information servira à des études statistiques et à la recherche;
- l'information appartient au domaine public;
- l'utilisation s'effectue dans l'intérêt évident de la personne et l'obtention du consentement n'est pas possible en temps opportun;
- le consentement et le fait de porter à la connaissance de la personne compromettraient la disponibilité ou l'exactitude de l'information; et
- la collecte est requise pour faire enquête sur une atteinte à une entente.

##### **6.2. Communication et transfert des renseignements personnels**

---

Nous n'utiliserons ou ne divulguerons les renseignements personnels des clients que si cela est nécessaire pour atteindre les objectifs identifiés au moment de la collecte [ou à une fin raisonnablement associée à ces fins, comme :

- Communiquer directement avec nos clients au sujet de produits et services qui pourraient les intéresser.

Nous n'utiliserons ni ne divulguons les renseignements personnels des clients, consommateurs ou membres du personnel pour tout autre objectif à moins d'obtenir le consentement pour ce faire.

Nous ne vendrons pas de listes de clients, consommateurs ou membres du personnel à d'autres parties [à moins d'avoir obtenu un consentement pour ce faire].

La LPRPDE permet à Pender de divulguer des renseignements personnels à des tierces, à l'insu et sans le consentement d'une personne :

- à un avocat représentant Pender;
- pour recouvrer une dette due par la personne ou le client à Pender;
- pour respecter une assignation, un mandat ou une ordonnance d'un tribunal ou d'un organisme de compétence;
- à une agence chargée de l'application de la loi dans le cadre d'une enquête civile ou criminelle;
- à une agence gouvernementale ou à un ministère demandant l'information; ou
- pour respecter la loi.

La LPRPDE permet à Pender de transférer des renseignements personnels à une tierce partie, à l'insu d'une personne ou sans son consentement, si le transfert s'effectue à des fins de traitement seulement et que la tierce partie utilise les renseignements aux seules fins qui ont motivé le transfert. Pender prendra les mesures nécessaires pour veiller, par contrat ou par d'autres moyens, à ce que la tierce partie protège les renseignements et les utilise conformément aux raisons qui ont motivé le transfert.

### **6.3. Conservation des renseignements personnels**

---

Si nous utilisons les renseignements personnels du client, consommateur ou membre du personnel pour prendre une décision qui a des répercussions sur le client, consommateur ou membre du personnel, nous conserverons ces renseignements personnels pendant au moins un an afin que le client, consommateur ou membre du personnel puisse avoir une chance raisonnable de demander l'accès à ces renseignements.

Nous conservons les renseignements personnels des clients, des consommateurs et des membres du personnel seulement pour la période nécessaire à l'atteinte des objectifs identifiés, ou d'objectifs juridiques ou commerciaux.

## **7. EXACTITUDE**

---

Nous prendrons des mesures raisonnables pour garantir l'exactitude et l'exhaustivité des renseignements personnels lorsque ceux-ci peuvent être utilisés pour prendre une décision concernant le client ou être divulgués à une autre organisation.

Les clients peuvent demander que des corrections soient apportées à leurs renseignements personnels pour veiller à leur exactitude et exhaustivité. Pour corriger les renseignements personnels, une demande doit être déposée par écrit et fournir suffisamment d'information pour cibler les renseignements personnels et les corrections souhaitées.

S'il est démontré que les renseignements personnels sont inexacts ou incomplets, nous les corrigerons au besoin et enverrons les renseignements modifiés à toute organisation à laquelle ces renseignements personnels ont été divulgués au cours de l'année précédente. Si la correction n'est pas effectuée, nous annoterons le dossier pour qu'il fasse état de la demande du client.

## 8. MESURES DE SÉCURITÉ

---

### 8.1. Utilisation des mesures de sécurité

---

Nous nous sommes engagés à assurer la sécurité des renseignements personnels de nos clients afin de les protéger contre un accès, une collecte, une utilisation, une divulgation, une copie, une modification ou une suppression non autorisés, ou des risques comparables.

Les mesures de sécurité suivantes seront mises en œuvre afin que les renseignements personnels des clients soient correctement protégés :

- utilisation de classeurs verrouillés;
- sécurité physique des bureaux où sont conservés les renseignements personnels;
- utilisation d'identifiants d'utilisateur, de mots de passe, de cryptage, de protections informatiques;
- restriction de l'accès des employés aux renseignements personnels, le cas échéant (c'est-à-dire que seuls ceux qui ont besoin de savoir y auront accès);
- exiger contractuellement des fournisseurs qu'ils mettent en place des mesures de sécurité comparables; et
- les employés et le conseil d'administration sont tenus de signer une entente de confidentialité les engageant à maintenir la confidentialité des renseignements personnels auxquels ils ont accès.

Nous aurons recours à des mesures de sécurité appropriées pour détruire les renseignements personnels des clients, comme le déchiquetage de documents et la suppression de l'information stockée électroniquement.

Nous examinerons et mettrons à jour en permanence nos politiques et mesures de sécurité suivant l'évolution de la technologie en ce qui a trait à la sécurité des renseignements personnels.

### 8.2. Atteintes aux mesures de sécurité

---

En vertu de la LPRPDE, Pender est tenue de signaler au Commissariat à la protection de la vie privée (« CPVP ») et à la personne victime d'une atteinte de toute violation des mesures de sécurité impliquant les renseignements personnels dont elle a la gestion s'il est raisonnable de croire, dans les circonstances, que l'atteinte crée un risque réel de préjudice grave pour une personne. Le rapport est inclus aux présentes à l'Annexe 1.

L'avis transmis à la personne doit être apparent et contenir suffisamment d'information pour permettre à cette personne de comprendre l'importance de la violation et les mesures qu'elle peut prendre pour atténuer/réduire les dommages, entre autres renseignements à fournir. Cet avis doit être transmis directement à la personne dans les plus brefs délais.

Dans son évaluation de risque réel de préjudice, Pender doit considérer :

- le degré de sensibilité des renseignements personnels en cause;
- la probabilité que les renseignements personnels aient été mal utilisés ou soient en train ou sur le point de l'être; et
- tout autre facteur devant être considéré.

Consulter l'Annexe 2 pour de plus amples renseignements.

En cas d'atteinte, Pender informera également toute autre organisation ou institution gouvernementale de l'atteinte si Pender estime que l'autre partie peut être en mesure de réduire le risque de préjudice qui pourrait en résulter.

### **8.3. Suivi des atteintes**

---

Pender conservera un registre des atteintes et effectuera un suivi de celles-ci lorsque ces atteintes visent les renseignements personnels dont elle a la gestion, et ce, même s'il n'y a aucune obligation de signaler la violation ou d'aviser une personne (c'est-à-dire que l'atteinte n'entraîne pas de « risque réel de préjudice grave » pour une personne).

Le registre contiendra toute l'information requise pour permettre au commissaire de vérifier la conformité par l'entreprise de ses obligations de signalement et d'avis en cette matière. L'entreprise doit conserver le registre pendant 24 mois après le jour où la violation s'est produite (et peut le conserver plus longtemps pour se conformer à d'autres exigences légales) et fournira le registre au commissaire sur demande.

Le registre doit contenir toute information permettant au CPVP de vérifier la conformité aux exigences de signalement et de notification des atteintes aux mesures de sécurité prévues aux [articles 10.1\(1\) et \(3\) de la LPRPDE](#), y compris les exigences d'évaluation du risque réel de préjudice grave.

Le registre doit contenir au minimum :

- la date ou la date estimée de l'atteinte;
- la description générale des circonstances ayant mené à l'atteinte;
- la nature des renseignements personnels en cause;
- une note indiquant si l'atteinte a été signalée au CPVP et si la personne concernée a été avisée;
- assez de détails pour que le CPVP puisse évaluer si l'entreprise a correctement utilisé les normes visant les risques réels de préjudice grave et a respecté ses obligations quant au signalement et à la notification de toute atteinte posant un réel risque de préjudice grave.

## **9. TRANSPARENCE**

---

Pender veillera à communiquer ses politiques et procédures de confidentialité aux personnes au moyen de sa politique de confidentialité ainsi que la Déclaration de confidentialité de l'entreprise contenue aux présentes dans l'Annexe 3.

## **10. ACCÈS INDIVIDUEL**

---

Les clients ont un droit d'accès à leurs renseignements personnels, sous réserve de certaines exceptions. Parmi les exceptions qui pourraient s'appliquer, on retrouve :

- le coût pour fournir les renseignements est prohibitif;
- l'information comporte des références à d'autres personnes;
- les renseignements ne peuvent pas être communiqués pour des raisons légales, commerciales ou de sécurité; et
- l'information est assujettie au privilège entre client et avocat ou un privilège relatif au litige.

Pour accéder aux renseignements personnels, une demande doit être déposée par écrit et doit fournir suffisamment d'information pour cibler les renseignements personnels souhaités. Une demande d'accès aux renseignements personnels doit être transmise au chef ou cheffe de la protection des renseignements personnels.

Sur demande, nous informerons également les clients sur la façon dont leurs renseignements personnels sont utilisés et les personnes à qui ils ont été communiqués, le cas échéant.

Nous rendrons les renseignements demandés disponibles dans les 30 jours ouvrables ou fournirons un avis écrit si un délai supplémentaire est nécessaire pour répondre à la demande.

Des frais minimaux peuvent être exigés pour fournir l'accès aux renseignements personnels. Lorsque des frais s'appliquent, nous informerons le client du coût et lui demanderons s'il souhaite donner suite à la demande.

Si une demande est refusée en tout ou en partie, nous aviserons le client par écrit, en lui indiquant les raisons du refus et les recours dont il dispose.

## 11. PLAINTES/RECOURS

---

Si une personne a des inquiétudes quant aux pratiques de Pender liées au traitement des renseignements personnels, une plainte peut être adressée par écrit au responsable de la confidentialité.

Après vérification de l'identité de la personne, le chef de la protection des renseignements personnels agira rapidement pour enquêter sur la plainte et fournira un rapport écrit sur les conclusions de l'enquête à la personne.

Lorsque le chef de la protection des renseignements personnels détermine que la plainte de la personne est fondée, celui-ci ou celle-ci prendra les mesures nécessaires pour corriger le processus de traitement en cause et/ou modifiera les politiques et procédures de confidentialité de Pender.

Lorsque le chef de la protection des renseignements personnels détermine que la plainte de la personne n'est pas fondée, celle-ci en sera avisée par écrit.

Si la personne n'est pas satisfaite de la conclusion et des mesures correspondantes prises par le chef de la protection des renseignements personnels de Pender, elle peut déposer une plainte auprès du Commissariat à la protection de la vie privée.



## **ANNEXE 1 : FORMULAIRE : RAPPORT D'ATTEINTE À LA LPRPDE**

---

<https://www.priv.gc.ca/fr/signaler-un-probleme/signaler-une-atteinte-a-la-vie-privee-dans-votre-organisation/signaler-une-atteinte-a-la-vie-privee-au-sein-de-votre-entreprise/>

## ANNEXE 2 : ÉVALUER LE RISQUE RÉEL DE PRÉJUDICE GRAVE<sup>1</sup>

---

En tant qu'organisation responsable, il convient d'élaborer un cadre permettant d'évaluer le risque réel de préjudice grave. De cette façon, toutes les atteintes seront évaluées de façon uniforme.

Les éléments servant à établir si une atteinte aux mesures de sécurité présente un risque réel de préjudice grave à l'endroit de l'intéressé incluent :

- le degré de sensibilité des renseignements personnels en cause; et
- la probabilité que les renseignements personnels aient été mal utilisés ou soient en train ou sur le point de l'être.

Dans le cadre de votre évaluation, vous tiendrez compte de ce qui suit :

i. **Sensibilité :**

- La LPRPDE ne définit pas le terme « sensibilité ». Toutefois, le concept de la sensibilité des renseignements personnels est abordé au principe 4.3.4 de la LPRPDE, lequel stipule ce qui suit :

Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.

- À la suite d'une atteinte, pour déterminer le caractère sensible, il est donc important d'examiner à la fois les renseignements personnels qui font l'objet de l'atteinte et les circonstances de l'incident.
- Certains renseignements peuvent être clairement sensibles, alors que d'autres ne le sont pas.
- Les circonstances de l'atteinte peuvent rendre les renseignements plus ou moins sensibles. Le préjudice potentiel que pourrait subir une personne est aussi un facteur important.

ii. **Probabilité d'un mauvais usage :**

Voici quelques questions à garder en tête :

- Qu'est-il arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'atteinte?
- Qui a, en fait, eu accès aux renseignements personnels ou aurait pu y avoir accès?
- Depuis combien de temps les renseignements personnels ont-ils été exposés?
- L'intention malveillante a-t-elle été démontrée (p. ex., vol, piratage)?
- Un certain nombre de renseignements personnels font-ils l'objet de l'atteinte, élevant ainsi le risque d'un mauvais usage?
- Les renseignements faisant l'objet de l'atteinte sont-ils en soi entre les mains d'une personne ou d'une entité qui représente un risque pour la réputation de la personne intéressée (p. ex., un ex-conjoint ou un patron, en fonction de circonstances précises)?
- Les renseignements ont-ils été exposés à des entités restreintes/connues qui se sont engagées à détruire et à ne pas divulguer les données?
- Les renseignements ont-ils été exposés à des personnes ou à des entités peu susceptibles de partager les renseignements d'une façon qui causerait un préjudice (p. ex., dans le cas d'une divulgation accidentelle à des personnes auxquelles ils ne sont pas destinés)?
- Les renseignements ont-ils été exposés à des personnes ou à des entités inconnues, ou à un grand nombre de personnes, alors que certaines personnes pourraient utiliser ou partager les renseignements d'une façon qui pourrait causer un préjudice?
- Est-il connu que les renseignements ont été exposés à des personnes ou à des entités

qui sont susceptibles de tenter de les utiliser pour causer un préjudice (p. ex., voleurs de renseignements)?

- Un préjudice s'est-il matérialisé (démonstration du mauvais usage)?
- Les renseignements ont-ils été perdus, consultés de manière inappropriée ou volés?
- Les renseignements personnels ont-ils été récupérés?
- Les renseignements personnels sont-ils cryptés adéquatement, anonymisés ou autrement difficiles d'accès?

---

[https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd\\_pb\\_201810/-dans-votre-entreprise/gd\\_pb\\_201810/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/-dans-votre-entreprise/gd_pb_201810/)

## **ANNEXE 3 : ÉNONCÉ DE CONFIDENTIALITÉ**

---

La protection des renseignements personnels et la confidentialité de nos clients sont une priorité pour nous. Pender se conforme à cette politique pour faire en sorte que les renseignements que vous nous transmettez soient traités avec la plus grande confidentialité et conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada.

### **Responsabilité**

Pender a la responsabilité de tous les renseignements personnels qui lui sont soumis et a nommé sa cheffe de la conformité en tant que cheffe de la protection des renseignements personnels, à laquelle il incombe de veiller à ce que ces principes soient respectés.

### **Détermination des fins**

Pender déterminera et documentera les objectifs de la collecte, de l'utilisation et de la communication des renseignements personnels avant ou au moment où les renseignements sont recueillis. Seuls les renseignements qui sont nécessaires aux affaires de Pender seront recueillis.

### **Consentement**

Les clients doivent avoir connaissance de la collecte, de l'utilisation ou de la communication des renseignements personnels et y consentir.

### **Collection**

Seuls les renseignements qui sont nécessaires pour offrir des services aux clients de Pender seront recueillis. Lorsque des renseignements personnels sont requis, ceux-ci seront obtenus directement auprès des clients. Au besoin, seules des sources réputées et dignes de confiance pourront être utilisées pour compléter l'information.

### **Limites d'utilisation, de communication et de conservation**

Les renseignements personnels ne seront pas utilisés ou communiqués à des fins autres que celles déterminées pour la collecte, sauf si la personne y consent ou que la loi nous y oblige. Les renseignements personnels sont conservés pendant la période nécessaire pour répondre aux objectifs.

### **Exactitude**

Les renseignements personnels seront exacts, exhaustifs et à jour selon les besoins et les objectifs de leur utilisation.

### **Mesures de sécurité**

Pender protégera les renseignements personnels à l'aide de mesures de sécurité adéquates en fonction de la sensibilité des renseignements personnels du client.

### **Transparence**

Pender communiquera à ses clients l'information propre aux politiques et procédures en ce qui a trait à la gestion de leurs renseignements personnels.

## **Accès individuel**

Sur demande, les clients de Pender seront tenus informés de l'existence, de l'utilisation et de la communication de leurs renseignements personnels et auront accès à cette information. Ils seront en mesure de vérifier l'exactitude et l'exhaustivité de ces renseignements et pourront demander que des corrections soient apportées, advenant des inexactitudes.

## **Traitement des plaintes, demandes et suggestions**

Toute personne est invitée à adresser ses questions, inquiétudes ou plaintes à l'égard de ces principes à notre cheffe de la protection des renseignements personnels au 604-688-1511 ou par la poste à l'adresse suivante : Gestion de capital PenderFund Ltée, suite 1640 – 1066 West Hastings Street, Vancouver (Colombie-Britannique) V6E 3X1.

## **Protection des données**

Pender respecte votre vie privée et accorde une grande importance aux relations qu'elle entretient avec ses clients.

Vos renseignements personnels seront protégés, ne seront jamais vendus et seront seulement utilisés par Pender et les sociétés affiliées, les partenaires d'affaires et les entités émettrices des deux entreprises afin de :

- (a) procurer du matériel marketing d'ordre général, des produits, des services et de l'information et des offres à nos partenaires commerciaux;
- (b) effectuer des analyses de marché et des ventes;
- (c) conserver l'exactitude de ses dossiers pour communiquer et répondre aux demandes, ainsi que gérer ses relations avec les clients; et
- (d) satisfaire d'autres intérêts d'affaires raisonnables et légitimes.

Pender n'entend pas partager les renseignements des clients. Pender ne recueillera, n'utilisera, ni ne communiquera les renseignements personnels des clients pour toutes autres fins que celles indiquées ci-dessus.

Pender s'est engagée à protéger les renseignements personnels de ses clients en se conformant pleinement à sa politique de confidentialité et aux lois applicables. Pender reconnaît les craintes à l'endroit de la sécurité en ligne et de la sécurité de vos renseignements, aussi nous prenons toutes les mesures raisonnables pour prévenir les pertes, mauvaises utilisations ou altération des renseignements soumis à Pender.

## **Renonciation**

Si les clients ne souhaitent pas être contactés ou aimeraient qu'on les retire de toute initiative de marketing, de sondages, de télémarketing ou de listes d'envoi par la poste ou par courriel, ou aimeraient limiter l'utilisation ou la communication de leurs renseignements personnels par Pender, ils pourront contacter Pender afin de se désabonner.

Sauf lorsque permis ou exigé par la loi en vigueur, Pender respectera les souhaits de ses clients en ce qui a trait à l'utilisation des renseignements personnels et veillera à ce que leurs dossiers fassent état des limites qui ont été demandées.

### **Correction des erreurs**

Les clients peuvent corriger les erreurs dans les renseignements permettant de les identifier en communiquant avec Pender à [info@penderfund.com](mailto:info@penderfund.com). Remarque : on pourra demander aux clients leurs nom, adresse et autres coordonnées.

### **Liens à des sites externes**

Le site Web de Pender contient des liens qui mènent à des sites externes sur lesquels Pender n'exerce aucun contrôle. Pender n'est pas responsable de ces sites, ni des omissions, des politiques ou du contenu de leurs sites Web. Pender vous recommande de lire les politiques de confidentialité de ces sites avant de prendre une décision visant à fournir des renseignements personnels à l'opérateur de ces sites.

Bien que Pender prenne des mesures raisonnables pour veiller à ce que les renseignements qu'elle possède sur ses clients sont exacts, exhaustifs et à jour, l'entreprise compte en partie sur ses clients pour l'informer de toute modification à leurs coordonnées ou toute autre information pertinente.