

Sarnia Lambton Workforce Development Board	
<b>DEPARTMENT: tous les départements</b>	<b>Politique</b>
<b>Politique: Customer Privacy Policy</b>	
<b>DATE D'adoption: March 3, 2020</b>	<b>DATE de Révision: 3 mars, 2020</b>

### **Objectif**

S'assurer que tous les programmes et services de la Commission du développement de la main-d'œuvre de Sarnia Lambton (SLWDB) sont conformes à la législation sur la protection des renseignements personnels énoncée dans la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) ainsi que par le biais du Commissaire à l'information et à la protection de la vie privée de l'Ontario (IPCO).

SLWDB s'engage à respecter la vie privée des particuliers et des entreprises, que ce soit ils répondent à l'une de nos enquêtes, fournissent des informations personnelles, participent à un événement ou utilisent notre site Web.

Cette politique s'applique à tous les biens et services fournis par le Sarnia Lambton Workforce Development Board, par tout moyen, y compris en personne, par téléphone, par voie électronique, par courrier, visuellement, oralement ou par écrit.

La politique s'applique à tous les employés, bénévoles, membres du conseil d'administration et tiers qui traitent avec le public au nom du conseil de développement de la main-d'œuvre de Sarnia Lambton.

### **Responsabilités**

Le Chief Privacy Officer (CPO) est le directeur exécutif. Le rôle du BCP est de veiller à ce que les politiques et les pratiques de la SLWDB soient conformes à la législation actuelle du gouvernement du Canada en matière de protection de la vie privée, y compris la LPRPDE, ainsi qu'à la législation de l'Ontario en matière de protection de la vie privée, tel que décrit par l'IPCO.

Le CPO répondra à toutes les questions de confidentialité internes et externes au nom de l'organisation et répondra à toutes les demandes, corrections et plaintes, y compris en expliquant les raisons de la collecte, de l'utilisation et de la divulgation des informations personnelles et du dépôt des plaintes.

Le CPO doit suivre les incidents et les atteintes à la vie privée et veiller à ce que des incidents similaires ne se reproduisent pas à l'avenir. Ils informeront tous les employés et bénévoles des nouveaux problèmes de confidentialité soulevés par les changements technologiques, les examens internes, les plaintes du public et les décisions de justice.

### **Définition**

Les informations personnelles comprennent, mais sans s'y limiter:

1. Toute information au-delà du nom, du titre, de l'adresse professionnelle, de l'e-mail professionnel et du ou des numéros de téléphone professionnel d'une personne.
2. Des données personnelles sensibles telles que des informations financières ou médicales, ou des identifiants personnels tels que le numéro d'assurance sociale;
3. Toute information pouvant entraîner un vol d'identité ou une autre fraude connexe; ou
4. Toute information qui pourrait autrement causer un préjudice ou une gêne préjudiciable à la carrière, à la réputation, à la situation financière, à la sécurité, à la santé ou au bien-être d'une personne.

### **Collecte et conservation des informations personnelles**

1. Les employés et les bénévoles doivent obtenir leur consentement avant de collecter des informations personnelles. La demande de retrait d'informations personnelles peut survenir à tout moment.
2. Le but de la collecte de renseignements personnels sera identifié au début de tout projet ou ouverture de participation.
  - a. Les adresses électroniques qui ont été collectées afin de partager des envois électroniques seront conservées jusqu'à ce qu'une personne choisisse de se désinscrire.
  - b. Les sondages indiqueront clairement le but de la collecte de renseignements personnels sur demande.
  - c. Si des informations personnelles sont collectées et combinées à partir de plusieurs sources, elles ne seront PAS utilisées à d'autres fins que celles pour lesquelles le consentement a été reçu.
- ré. Les informations personnelles seront détruites après l'achèvement d'un projet.
3. Lorsqu'elles ne seront plus nécessaires aux fins identifiées, les informations personnelles seront détruites.
4. Les informations personnelles seront conservées dans des armoires verrouillées et / ou dans des fichiers électroniques protégés par des clés physiques et / ou des mots de passe électroniques.
5. Aucune information personnelle ne sera divulguée, sauf si cela est demandé dans le cadre d'une procédure judiciaire. La SLWDB se conformera à toutes les demandes des agences gouvernementales compétentes et du système judiciaire.

### **Demandes de renseignements personnels**

1. Les informations personnelles peuvent être demandées à tout moment en contactant le CPO. Les demandes seront traitées dans les trente (30) jours.
2. Les renseignements personnels seront fournis à une personne sans frais.

### **Réclamations**

1. Les plaintes doivent être adressées au CPO par écrit ou par l'intermédiaire d'un équivalent accessible approprié.
2. Les plaintes seront traitées dans les quinze (15) jours suivant leur réception.

3. Toutes les plaintes feront l'objet d'une enquête par le CPO. Lorsque les plaintes sont jugées justifiées, des mesures correctives seront prises, les politiques modifiées et les employés recyclés.
4. Les plaintes qui ne sont pas résolues avec succès peuvent faire l'objet d'un suivi auprès de l'IPCO ainsi que du Commissariat à la protection de la vie privée du Canada.

### **Protocole de violation**

Une atteinte à la vie privée est la perte, l'accès non autorisé ou la divulgation de renseignements personnels. Cela peut se produire à la suite du vol ou de la perte d'informations ou d'équipements de stockage de données, ou de la collecte, l'utilisation, la divulgation, l'accès, le stockage ou l'élimination inappropriés ou non autorisés d'informations, y compris la correspondance mal acheminée.

Lorsque SLWDB découvre ou est informé d'une violation, nous prendrons immédiatement les mesures suivantes:

#### 1. Évaluation et confinement

- a) Décrire les circonstances à l'origine de l'atteinte à la vie privée;
- b) Faire l'inventaire des informations personnelles qui ont été ou pourraient avoir été compromises;
- c) Identifier les parties dont les informations personnelles ont été indûment divulguées ou consultées, volées ou perdues, ou si cela n'est pas possible, identifier les groupes d'individus susceptibles d'avoir été affectés;
- d) Identifier toute autre information pertinente (par exemple, des incidents similaires ou connexes);
- e) Supprimer, déplacer ou séparer les informations ou fichiers exposés pour empêcher tout accès illicite;
- f) Arrêter temporairement le site Web, l'application ou l'appareil pour permettre une évaluation complète de la violation et résoudre les vulnérabilités;
- g) Tenter de récupérer des documents ou des copies de documents qui ont été divulgués ou pris à tort par une personne non autorisée.

#### 2. Notification aux personnes concernées

- a) La SLWDB avisera toutes les personnes concernées dès que possible après la violation afin de permettre aux personnes de prendre des mesures pour se protéger contre le vol d'identité ou tout autre préjudice possible ou pour atténuer les dommages causés par celui-ci.
- b) Des précautions seront prises dans le processus de notification pour ne pas alarmer indûment les personnes, en particulier lorsque la SLWDB ne peut pas confirmer que certaines personnes ont été affectées par la violation.
- c) La préférence sera donnée à la notification des personnes concernées par téléphone ou en personne.
- d) Dans le cas où les individus ne peuvent pas être localisés ou le nombre d'individus est si important que la tâche deviendrait trop onéreuse, SLWDB affichera un avis bien visible sur notre site Web et partagera ces informations via notre newsletter mensuelle.
- e) Une description générale de l'incident, y compris la date et l'heure;
- f) La source de la violation (une institution, une partie contractante ou une partie à un accord de partage);
- g) Une liste des informations personnelles qui ont été ou pourraient avoir été compromises;

- h) La notification comprendra:
- i. Une description générale de l'incident, y compris la date et l'heure;
  - ii. La source de la violation;
  - iii. Une liste des informations personnelles qui ont été ou pourraient avoir été compromises;
  - iv. Une description des mesures prises ou à prendre pour récupérer les informations personnelles, contenir la violation et prévenir la répétition;
  - v. Conseils à la personne pour atténuer les risques de vol d'identité ou pour traiter des informations personnelles compromises;
  - vi. Le nom et les coordonnées du CPO avec qui les individus peuvent discuter de la question plus avant ou obtenir de l'aide;
  - vii. Une référence à l'effet que l'IPCO a été informé de la nature de l'infraction et que la personne a le droit de porter plainte auprès de ce bureau, le cas échéant;
  - viii. Une référence à l'effet que le ministère du Travail, de la Formation et du Développement des compétences a été informé de la nature de l'infraction; et
  - ix. Que la SLWDB continuera à informer les personnes concernées de l'évolution de la situation au fur et à mesure que l'enquête se poursuit et que les problèmes en suspens sont résolus.

3. Notification à l'IPCO

4. Notification au ministère du Travail, de la Formation et du Développement des compétences

5. Notification au comité exécutif de la SLWDB

6. Atténuation et prévention

- a) La SLWDB s'assurera qu'un plan est élaboré pour atténuer les risques identifiés au cours de l'enquête et que le plan est mis en œuvre; et
- b) Informer l'IPCO, le ministère du Travail, de la Formation et du Développement des compétences et les parties concernées de tout plan d'atténuation des risques à mettre en œuvre.

7. Partage des enseignements tirés

- a) Le personnel et les bénévoles seront formés sur tout nouveau protocole développé.

**Coordonnées supplémentaires**

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Rue Bloor Est,

Suite 1400

Toronto, Ont.

M4W 1A8

1-800-387-0073

<https://www.ipc.on.ca/>