



Commissariat
à la protection de
la vie privée du Canada

Office of the
Privacy Commissioner
of Canada

Guide sur la protection de la vie privée à l'intention des entreprises

Ce que les entreprises canadiennes doivent savoir pour se conformer à la loi fédérale sur la protection des renseignements personnels



Pour plus de renseignements, communiquez avec :

Commissariat à la protection de la vie privée du Canada
30, rue Victoria, 8^e étage
Gatineau (Québec)
K1A 1H3

Téléphone : 819-994-5444
Sans frais : 1-800-282-1376
ATS : 819-994-6591

Pour plus de renseignements, consultez : priv.gc.ca/entreprise
Suivez-nous sur Twitter : [@priveeprivacy](https://twitter.com/priveeprivacy)

Bien qu'il ait été élaboré avec soin pour assurer un contenu exact et exhaustif, le présent guide n'a aucune valeur juridique. Pour obtenir de plus amples renseignements concernant la Loi, veuillez consulter notre site Web à l'adresse priv.gc.ca/entreprise ou téléphonez au Commissariat à la protection de la vie privée du Canada.

Numéro de catalogue : IP54-94/2019F
Numéro ISBN : 978-0-660-32106-6

Mise à jour : septembre 2020

Le présent guide ne porte que sur la partie 1 de la Loi. Toutes les références à la Loi mentionnées dans ce document se rapportent donc expressément à cette partie. Les parties 2 à 5 de la Loi portent sur l'utilisation des documents électroniques et les signatures comme substituts légaux aux documents originaux et aux signatures. Pour plus de renseignements à ce sujet, veuillez communiquer avec le ministère de la Justice.

Table des matières

Aperçu	2
Rôle du Commissariat à la protection de la vie privée du Canada	3
Survol de la LPRPDE	3
Modalités d'application de la Loi	4
Qu'entend-on par « renseignements personnels »?	5
Qu'est-ce qui n'est pas visé par la LPRPDE?	5
Vos responsabilités en vertu de la LPRPDE	6
Principes relatifs à l'équité dans le traitement de l'information	7
1 Soyez responsable	8
2 Déterminez les fins de la collecte de renseignements	12
3 Obtenez un consentement valable et éclairé	14
4 Limitez la collecte	17
5 Limitez l'utilisation, la communication et la conservation	18
6 Soyez précis	20
7 Utilisez des mesures de protection appropriées	21
8 Faites preuve de transparence	23
9 Accordez l'accès aux personnes concernées	25
10 Recevez les plaintes à l'égard du non-respect des principes	27
Gérer un cas d'atteinte	29
Risque réel de préjudice grave	30
Ce qui doit figurer dans votre rapport d'atteinte au Commissariat	30
Ce que doit contenir votre avis aux personnes touchées	31
Ce que doivent contenir les dossiers dans votre propre registre des atteintes	31
Plaintes adressées au commissaire à la protection de la vie privée du Canada	32
Processus de plainte	33
Vérifications	37
Demander une audience à la Cour fédérale	38
La Loi canadienne anti-pourriel et la LPRPDE	40
Services-conseils aux entreprises	42

Aperçu



Les Canadiens sont de plus en plus préoccupés par la protection de leur vie privée. De plus en plus, ils choisissent de faire affaire avec des organisations qui sont sensibles à leurs préoccupations et qui peuvent démontrer qu'elles traiteront leurs renseignements personnels avec diligence.

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) est la loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada. Elle établit les règles de base régissant le traitement des renseignements personnels par les entreprises dans le cadre de leurs activités commerciales.

Le Commissariat à la protection de la vie privée du Canada (le Commissariat) a préparé ce guide pour aider les organisations à comprendre et à respecter leurs obligations en vertu de la LPRPDE.

Rôle du Commissariat à la protection de la vie privée du Canada

Le Commissariat a pour mission de protéger et de promouvoir le droit à la vie privée. À titre d'agent du Parlement, le commissaire à la protection de la vie privée relève directement de la Chambre des communes et du Sénat du Canada. Cette indépendance contribue à assurer l'impartialité du commissaire dans son rôle d'ombudsman en matière de protection de la vie privée.

Le Commissariat supervise la conformité à la LPRPDE en menant des enquêtes indépendantes et impartiales et/ou des vérifications des pratiques des entreprises à l'égard du traitement des renseignements personnels.

Le Commissariat veille également à ce que les organisations respectent leurs obligations en matière de protection de la vie privée en leur fournissant des renseignements et une orientation. Il procède aussi à des activités de mobilisation, qui comprennent des services de sensibilisation et des services-conseils.

Survol de la LPRPDE

Il faut respecter un certain nombre d'exigences afin d'être conforme à la Loi. Les organisations visées par la LPRPDE doivent habituellement obtenir le consentement des personnes lorsqu'elles recueillent, utilisent ou communiquent des renseignements personnels les concernant. Les personnes ont le droit de consulter les renseignements personnels que détient une organisation à leur sujet. Elles ont aussi le droit d'en contester l'exactitude.

Les renseignements personnels ne peuvent être utilisés qu'aux fins auxquelles ils ont été recueillis. L'organisation qui entend les utiliser à d'autres fins doit, de nouveau, obtenir le consentement de le faire. Les renseignements personnels doivent être protégés par des mesures appropriées.



Modalités d'application de la Loi

La LPRPDE s'applique aux organisations du secteur privé du Canada qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales.

Selon la Loi, une « [activité commerciale](#) » s'entend de toute activité régulière ainsi que de tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds.

Lois provinciales sur la protection des renseignements personnels

[L'Alberta](#), [la Colombie-Britannique](#) et [le Québec](#) ont leurs propres [lois en matière de protection des renseignements personnels dans le secteur privé](#) jugées être essentiellement similaires à la LPRPDE. Les organisations assujetties à des lois provinciales essentiellement similaires en matière de protection des renseignements personnels sont habituellement exonérées de la LPRPDE en ce qui a trait à la collecte, à l'utilisation ou à la communication de renseignements personnels dans la province en question.

L'Ontario, le Nouveau-Brunswick, la Nouvelle-Écosse et Terre-Neuve-et-Labrador ont également adopté des lois essentiellement similaires à l'égard de la collecte, de l'utilisation et de la communication de renseignements personnels sur la santé.

Des renseignements qui traversent les frontières

Toutes les entreprises qui exercent des activités au Canada et qui traitent des renseignements personnels qui vont au-delà des frontières provinciales ou nationales dans le cadre de leurs activités commerciales sont assujetties à la LPRPDE, quel que soit le territoire ou la province où elles se situent (y compris dans des provinces dotées de lois essentiellement similaires).

Organisations sous réglementation fédérale

Les organisations sous réglementation fédérale qui exercent leurs activités au Canada sont toujours assujetties à la LPRPDE. La Loi s'applique également aux renseignements personnels de leurs employés.

Ces organisations comprennent :

- les aéroports, les aéronefs et les lignes aériennes;
- les banques et les banques étrangères autorisées;
- les entreprises de transport interprovinciales ou internationales;
- les entreprises de télécommunication;
- les entreprises exerçant des activités de forage en mer;
- les radiodiffuseurs et les télédiffuseurs.

Remarque : Les organisations situées dans les Territoires du Nord-Ouest, au Yukon et au Nunavut sont réputées être sous réglementation fédérale et sont donc également visées par la LPRPDE.

Qu'entend-on par « renseignements personnels »?

Aux termes de la LPRPDE, on entend par renseignement personnel tout renseignement factuel ou subjectif, consigné ou non, concernant une personne identifiable. Il peut s'agir de tout type de renseignement, par exemple :

- l'âge, le nom, un numéro d'identification, le revenu, l'origine ethnique ou le groupe sanguin;
- une opinion, une évaluation, un commentaire, le statut social ou une mesure disciplinaire;
- le dossier d'un employé, un dossier de crédit ou de prêt, un dossier médical, l'existence d'un différend entre un consommateur et un commerçant ou le projet d'une personne (par exemple, l'intention d'acquérir des biens ou des services ou de changer d'emploi).

Qu'est-ce qui n'est pas visé par la LPRPDE?

Il y a des cas où la LPRPDE ne s'applique pas, par exemple :

- les renseignements personnels traités par les organisations fédérales mentionnées dans la [*Loi sur la protection des renseignements personnels*](#);
- les renseignements personnels gérés par les gouvernements provinciaux et territoriaux et leurs mandataires;

- les coordonnées d'affaires, comme le nom, le titre, l'adresse professionnelle, le numéro de téléphone ou l'adresse courriel d'un employé, recueillies, utilisées ou communiquées uniquement dans le but de contacter la personne pour les besoins de son emploi ou de sa profession;
- les renseignements personnels recueillis, utilisés ou communiqués par une personne à des fins strictement personnelles (p. ex. la constitution d'une liste de personnes à qui adresser des cartes de vœux);
- les renseignements personnels recueillis, utilisés ou communiqués par une organisation à des fins strictement journalistiques, artistiques ou littéraires.

À moins qu'elles ne réalisent des [activités commerciales](#) qui ne sont pas essentielles à l'exécution de leur mandat et qui nécessitent l'utilisation de renseignements personnels, les entités suivantes ne sont pas visées par la LPRPDE :

- [les organisations caritatives et à but non lucratif](#);
- [les associations et partis politiques](#).

Les [municipalités, universités, écoles et hôpitaux](#) sont normalement régis par les lois provinciales. La LPRPDE peut s'appliquer dans certaines situations.

Vos responsabilités en vertu de la LPRPDE

Afin de protéger les renseignements personnels, les entreprises doivent respecter les [dix principes relatifs à l'équité dans le traitement de l'information](#) énumérés à l'Annexe 1 de la LPRPDE.

En suivant ces principes, vous contribuerez à établir la confiance envers votre entreprise et l'économie numérique.

Ces principes sont les suivants :

1. Responsabilité
2. Détermination des fins de la collecte des renseignements
3. Consentement
4. Limitation de la collecte
5. Limitation de l'utilisation, de la communication et de la conservation
6. Exactitude
7. Mesures de sécurité
8. Transparence
9. Accès aux renseignements personnels
10. Possibilité de porter plainte à l'égard du non-respect des principes

Principes relatifs à l'équité dans le traitement de l'information



Les dix principes relatifs à l'équité dans le traitement de l'information de la LPRPDE jettent les bases non seulement de la collecte, de l'utilisation et de la communication des renseignements personnels, mais également de l'accès aux renseignements personnels. Ils permettent aux personnes d'exercer un certain contrôle sur la manière dont leurs renseignements personnels sont traités dans le secteur privé.

En plus de ces principes, la LPRPDE énonce qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable jugerait acceptables dans les circonstances.

Le Commissariat a déterminé que les fins suivantes seraient généralement jugées non acceptables par une personne raisonnable (c.-à-d. des zones interdites) :

- recueillir, utiliser ou communiquer des renseignements personnels d'une manière qui serait autrement illégale;
- procéder au profilage ou au classement de personnes de manière pouvant se traduire par un traitement inéquitable, non éthique ou discriminatoire contraire aux lois relatives aux droits de la personne;
- recueillir, utiliser ou communiquer des renseignements personnels à des fins qui causent ou sont susceptibles de causer un préjudice grave à une personne;
- publier des renseignements personnels avec l'intention de facturer leur retrait;
- demander des mots de passe à des comptes de médias sociaux à des fins de présélection d'employés;

- exercer des activités de surveillance à l'égard d'une personne au moyen des fonctions audio ou vidéo de son propre appareil.

La présente section énonce les responsabilités des organisations en ce qui concerne chacun des dix principes. Elle explique comment s'acquitter de ces responsabilités et donne des conseils à cet égard.

1 **Soyez responsable**

Vos responsabilités

- Vous conformer aux dix principes relatifs à l'équité dans le traitement de l'information.
- Nommer une personne chargée de la conformité de votre organisation à la LPRPDE.
- Protéger tous les renseignements personnels détenus par votre organisation, y compris tout renseignement personnel que vous transférez à une tierce partie pour traitement.



- Élaborer et mettre en œuvre des politiques et des pratiques concernant les renseignements personnels.

Comment vous acquitter de vos responsabilités

Élaborez un programme de gestion de la protection de la vie privée

- Ce programme devrait être conçu, au minimum, pour être conforme à la Loi, y compris aux dix principes relatifs à l'équité dans le traitement de l'information.
- Il doit indiquer qui est le représentant désigné par votre organisation en matière de protection de la vie privée, et fournir son nom ou son titre à l'interne et à l'externe (p. ex. sur votre site Web ou dans une publication).
- Votre représentant désigné en matière de protection de la vie privée doit avoir le soutien de la haute direction ainsi que le pouvoir d'intervenir pour toute question relative à la protection de la vie privée.
- Procédez à une évaluation des facteurs relatifs à la vie privée et à une analyse des menaces découlant des pratiques de votre organisation relatives au traitement des renseignements personnels, qui

tient compte des activités courantes, des nouvelles initiatives et des nouvelles technologies.

- En premier lieu, utilisez la liste de contrôle qui suit :
 - » Quels renseignements personnels recueillons-nous? S'agit-il de renseignements sensibles? (Les renseignements sensibles pourraient exiger des mesures de sécurité supplémentaires.)
 - » Pourquoi recueillons-nous ces renseignements?
 - » Comment les recueillons-nous?
 - » À quoi servent-ils?
 - » Où les conservons-nous?
 - » Comment sont-ils sécurisés?
 - » Qui y a accès ou qui les utilise?
 - » Avec qui les partageons-nous?
 - » Quand sont-ils éliminés?
- Élaborez, documentez et mettez en œuvre des politiques et des procédures pour assurer la protection des renseignements personnels :
 - » Déterminez les fins de la collecte.
 - » Obtenez un consentement valable.
 - » Limitez la collecte, l'utilisation et la communication des renseignements personnels.
 - » Assurez-vous que les renseignements sont exacts, complets et à jour.
 - » Assurez-vous que les mesures de sécurité sont appropriées pour la protection des renseignements.
 - » Élaborez ou mettez à jour un échéancier pour la conservation et la destruction des documents.
 - » Élaborez et mettez en œuvre des politiques et des procédures de réponse aux plaintes, aux questions et aux demandes d'accès à des renseignements personnels.

- » Élaborez, documentez et mettez en œuvre des protocoles de gestion des incidents et des atteintes en matière de sécurité des renseignements personnels.
- » Documentez et mettez en œuvre des évaluations des risques.
- » Élaborez, documentez et mettez en œuvre des pratiques appropriées à l'intention des tiers qui fournissent des services.
- » Élaborez, documentez et offrez une formation appropriée sur la protection de la vie privée à l'intention de vos employés.
- Passez régulièrement en revue votre programme de gestion de la protection de la vie privée et corrigez toute lacune relevée.
- Soyez prêt à faire la preuve que vous avez des politiques et des procédures en place aux fins de la protection des renseignements personnels; que vous avez fourni à vos employés une formation appropriée en matière de protection de la vie privée; et que vous avez nommé une personne chargée de la gouvernance en matière de vie privée.
- Faites en sorte que vos clients et employés puissent accéder facilement à vos politiques et procédures en matière de protection de la vie privée (p. ex. dans des brochures et sur les sites Web).

Formez tous les membres du personnel afin qu'ils puissent répondre aux questions suivantes :

- Comment donner suite aux demandes de renseignements du public au sujet des politiques de l'organisation en matière de protection de la vie privée?
- Qu'est-ce qu'un consentement valable? Quand et comment l'obtenons-nous?
- Comment reconnaître et traiter les demandes d'accès aux renseignements personnels?
- À qui devrais-je faire part de plaintes relatives à la protection de la vie privée?
- Quelles sont les initiatives actuelles ou nouvelles de mon organisation en matière de protection des renseignements personnels?

Au moment de transférer des renseignements personnels à des tierces parties aux fins de traitement à l'extérieur du Canada :

- évaluez les risques susceptibles d'avoir une incidence défavorable sur la protection des renseignements personnels lorsqu'ils sont transférés à des tiers fournisseurs de services exerçant des activités à l'extérieur du Canada;
- veillez, par des moyens contractuels ou autres, à ce que la tierce partie fournisse un degré de protection des renseignements personnels qui est comparable à celui exigé dans la LPRPDE;
- limitez l'utilisation des renseignements personnels par la tierce partie aux fins nécessaires à l'exécution du contrat;
- faites preuve de transparence dans vos pratiques, notamment en informant les clients que leurs renseignements personnels pourraient être envoyés dans un autre territoire de compétence aux fins de traitement, et que les tribunaux, organismes d'application de la loi et autorités nationales de sécurité de ce territoire pourraient y accéder pendant que les renseignements s'y trouvent.

Liens connexes

- [Premier principe relatif à l'équité dans le traitement de l'information de la LPRPDE - Responsabilité](#)
- [Un programme de gestion de la protection de la vie privée : la clé de la responsabilité](#)
- [Bulletin d'interprétation : Responsabilité](#)



2 Déterminez les fins de la collecte de renseignements

Vos responsabilités

- Déterminer et documenter les fins auxquelles vous recueillez des renseignements personnels. Cela vous aidera à établir quels renseignements personnels précis vous devez recueillir à ces fins.
- Préciser à vos clients la raison pour laquelle votre organisation a besoin de leurs renseignements personnels avant ou au moment de la collecte. Selon la façon dont se fait la collecte, cette précision peut être communiquée de vive voix ou par écrit.
- Obtenir à nouveau leur consentement si vous déterminez une nouvelle fin.

Comment vous acquitter de vos responsabilités

- Examinez les renseignements personnels que vous avez en votre possession pour vous assurer qu'ils sont tous destinés à une fin précise.
- Lorsque vous demandez des renseignements personnels à un client, expliquez-lui verbalement ou par écrit les fins auxquelles les renseignements sont recueillis.
- Consignez par écrit toutes les fins définies et les consentements que vous avez obtenus.
- Assurez-vous que les fins auxquelles les renseignements sont destinés se limitent à ce qu'une personne raisonnable estimerait acceptable dans les circonstances.

Conseils

Définissez le plus clairement et le plus précisément possible à quelles fins les renseignements personnels sont recueillis, de façon à ce que les personnes concernées comprennent comment ils seront utilisés ou communiqués. Voici quelques exemples précis de fins de collecte :

- ouvrir un compte;
- vérifier la solvabilité d'une personne;
- verser des prestations à un employé;
- traiter une demande d'abonnement à un magazine;
- transmettre de l'information au sujet de l'adhésion à une association;
- garantir une réservation de voyage;
- établir les préférences d'un client;
- déterminer l'admissibilité d'un client à un rabais ou à une offre spéciale.

Évitez de définir des fins de collecte trop vastes.

Lien connexe

- [Deuxième principe relatif à l'équité dans le traitement de l'information de la LPRPDE - Détermination des fins de la collecte de renseignements](#)



3 Obtenez un consentement valable et éclairé

Vos responsabilités

- Le consentement valable est un élément essentiel de la LPRPDE. Les organisations doivent généralement obtenir un consentement valable pour la collecte, l'utilisation et la communication de renseignements personnels.
 - Afin de donner un consentement valable, les personnes doivent comprendre ce à quoi on leur demande de consentir. Le consentement ne sera jugé valable que s'il est raisonnable de s'attendre à ce que vos clients comprennent la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication de leurs renseignements personnels.
 - Un consentement ne peut être requis que pour la collecte, l'utilisation ou la communication nécessaires à une fin explicite et légitime. Pour les collectes, les utilisations et les communications non intégrales, un choix doit être donné aux personnes.
 - La forme du consentement doit tenir compte du caractère sensible du renseignement personnel.
- Assurez-vous que l'information sur la protection de la vie privée est facilement accessible dans sa forme intégrale, en mettant l'accent ou en attirant l'attention sur quatre questions clés :
 - » Quels sont les renseignements personnels recueillis? (Fournir suffisamment de détails pour que les personnes comprennent bien ce à quoi elles consentent.)
 - » À quelles parties les renseignements personnels seront-ils communiqués?
 - » À quelles fins les renseignements personnels sont-ils recueillis, utilisés ou communiqués? (Fournir suffisamment de détails pour que les personnes comprennent bien ce à quoi elles consentent.)
 - » Quels sont les risques de préjudice et autres conséquences?
 - Fournissez l'information de manière à ce qu'elle soit facile d'accès et facile à utiliser.
 - Offrez aux personnes un choix clair et facilement accessible pour toute collecte, utilisation ou communication non nécessaire à la fourniture du produit ou à la prestation du service.

La manière dont vous demanderez un consentement dépendra des circonstances et du type de renseignement que vous recueillez.

- Une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable, et vous devez informer la personne des conséquences du retrait.

Comment vous acquitter de vos responsabilités

- Tenez compte des perspectives de vos clients afin que les processus de consentement soient conviviaux et généralement compréhensibles.
- Obtenez un consentement lorsque vous apportez des changements importants à vos pratiques en matière de protection de la vie privée, notamment en ce qui concerne l'utilisation de données à de nouvelles fins ou des communications à de nouvelles tierces parties.
- Ne recueillez, n'utilisez ou ne communiquez des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.
- Permettez aux personnes de retirer leur consentement (sous réserve de restrictions légales ou contractuelles).
- Déterminez la forme appropriée du consentement : obtenez un consentement explicite pour les collectes, les utilisations ou les communications qui, en général :
 - i) touchent des renseignements de nature délicate;
 - ii) dépassent ce à quoi s'attendrait raisonnablement une personne; et/ou iii) créent un risque résiduel important de préjudice grave.
- Consentement et enfants : obtenez le consentement d'un parent ou d'un tuteur pour toute personne qui n'est pas en mesure de fournir elle-même un consentement valable (le Commissariat a adopté la position que, dans toutes les circonstances sauf dans des situations exceptionnelles, cela comprend toutes les personnes âgées de moins de 13 ans), et assurez-vous que le processus de consentement des jeunes personnes en mesure de fournir elles-mêmes un consentement tient raisonnablement compte de leur niveau de maturité.
- Qu'il soit implicite ou explicite, le consentement n'élimine pas les autres obligations d'une organisation en vertu de la LPRPDE, telles que la responsabilisation démontrable, les mesures de sécurité et l'existence de motifs raisonnables pour le traitement des renseignements personnels.

Forme de consentement

Il est important que les organisations examinent la forme de consentement (explicite ou implicite) qui convient pour la collecte, l'utilisation ou la communication de renseignements personnels nécessitant l'obtention d'un consentement. Le consentement devrait généralement être explicite, mais un consentement implicite peut être suffisant dans des circonstances strictement définies. Les organisations doivent prendre en compte la nature sensible des renseignements et les attentes raisonnables de la personne, qui sont toutes deux fonctions du contexte.

En règle générale, les organisations doivent obtenir un consentement **explicite** dans les cas suivants :

- les renseignements recueillis, utilisés ou communiqués sont sensibles;
- la collecte, l'utilisation ou la communication de l'information ne répond pas aux attentes raisonnables de la personne;
- la collecte, l'utilisation ou la communication crée un risque résiduel important de préjudice grave.

Les conseils qui suivent peuvent contribuer à rendre votre processus de consentement plus valable :

- Permettez aux personnes de déterminer l'étendue des détails qu'elles souhaitent recevoir, et à quel moment.
- Concevez ou adoptez des façons créatives d'obtenir un consentement, en temps opportun, qui sont propres au contexte et conviennent au type d'interface.
- Rappelez périodiquement aux personnes les choix de consentement qu'elles ont faits et ceux qui leur sont offerts.
- Effectuez périodiquement une vérification des communications touchant la vie privée afin de veiller à ce qu'elles reflètent exactement les pratiques en cours en matière de gestion des renseignements personnels.
- Soyez prêt à faire la preuve de la conformité – en particulier, du fait que le processus de consentement est compréhensible du point de vue de l'utilisateur.
- Dans la conception du processus de consentement, envisagez de :
 - » consulter des utilisateurs et d'obtenir leurs points de vue;
 - » faire des essais pilotes ou d'utiliser des groupes de discussion afin d'évaluer le caractère compréhensible des documents;
 - » faire appel à des spécialistes de la conception axée sur l'interaction et de l'expérience utilisateur (IU/EU);
 - » consulter des experts ou des organismes de réglementation en matière de protection de la vie privée;
 - » suivre les pratiques exemplaires ou les normes établies.

Liens connexes

- [Troisième principe relatif à l'équité dans le traitement de l'information de la LPRPDE – Consentement \(comprend les exceptions au principe du consentement\)](#)
- [Lignes directrices pour l'obtention d'un consentement valable](#)
- [Dix conseils pour améliorer votre politique de confidentialité en ligne et la transparence de vos pratiques en matière de protection de la vie privée](#)

4 Limitez la collecte

Vos responsabilités

- Recueillir uniquement les renseignements personnels dont votre organisation a besoin à une fin légitime établie.
- Faire preuve d'honnêteté au sujet des raisons pour lesquelles vous recueillez des renseignements personnels.
- Recueillir des renseignements personnels en utilisant des moyens équitables et légaux. Cette exigence vise à empêcher que des organisations recueillent des renseignements d'une façon trompeuse ou qui induit les gens en erreur quant aux fins visées.

Comment vous acquitter de vos responsabilités

- Définissez le type de renseignements personnels recueillis dans vos politiques et pratiques en matière de traitement des renseignements.
- Limitez la quantité et le type de renseignements recueillis à ceux qui sont nécessaires aux fins établies.
- Assurez-vous que les membres de votre personnel sont en mesure d'expliquer les fins pour lesquelles votre organisation a besoin de ces renseignements.



Conseils

- En réduisant la quantité de renseignements recueillis, vous pouvez réduire les coûts liés à la collecte, au stockage, à la conservation et, finalement, à l'archivage ou à l'élimination des données.
- Le fait de recueillir moins de renseignements entraîne également une réduction des risques ou des incidences en cas de perte ou d'accès, d'utilisation ou de communication inappropriés.

Liens connexes

- [Quatrième principe relatif à l'équité dans le traitement de l'information de la LPRPDE - Limitation de la collecte](#)
- [Collecte du numéro du permis de conduire en vertu des lois sur la protection des renseignements personnels applicables au secteur privé - Guide à l'intention des détaillants](#)
- [Lignes directrices sur la surveillance vidéo au moyen d'appareils non dissimulés dans le secteur privé](#)
- [Document d'orientation sur la surveillance vidéo secrète dans le secteur privé](#)
- [Lignes directrices en matière d'identification et d'authentification](#)



5 Limitez l'utilisation, la communication et la conservation

Vos responsabilités

- À moins qu'une personne ne donne son consentement en conséquence – ou à moins qu'il ne soit par ailleurs nécessaire de le faire en vertu de la loi –, votre organisation doit s'assurer d'utiliser ou de communiquer des renseignements personnels uniquement aux fins pour lesquelles ils ont été recueillis. Ne conservez les renseignements personnels que pendant la durée nécessaire pour la réalisation de ces fins.
 - Être au fait des renseignements personnels dont vous disposez, de l'endroit où ils se trouvent et de ce que vous en faites.
 - Obtenir un nouveau consentement si vous avez l'intention d'utiliser ou de communiquer des renseignements personnels à une nouvelle fin.
 - Recueillir, utiliser ou communiquer des renseignements personnels uniquement à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.
- Établir des lignes directrices et des procédures relatives à la conservation et à la destruction des renseignements personnels.
 - Conserver pendant un temps raisonnable les renseignements personnels utilisés pour prendre une décision au sujet d'une personne. Cela pourrait être utile dans l'éventualité où une personne cherche à avoir accès aux renseignements à des fins de réparation.
 - Détruire, supprimer ou dépersonnaliser tout renseignement personnel dont votre organisation n'a plus besoin.

Comment vous acquitter de vos responsabilités

- Documentez toute nouvelle fin pour l'utilisation de renseignements personnels.
- Limitez et surveillez l'accès des employés aux renseignements personnels, et prenez des mesures appropriées en cas d'accès non autorisé aux renseignements.
- Établissez des périodes de conservation maximale et minimale en tenant compte des exigences ou des restrictions législatives, ainsi que des mécanismes d'appel.
- Détruisez les renseignements personnels qui ne répondent pas à une fin précise ou qui ne sont plus nécessaires pour réaliser une fin établie. Éliminez les renseignements de manière à empêcher les atteintes à la vie privée, comme en déchiquetant de manière sécuritaire les dossiers papier ou en supprimant efficacement les dossiers électroniques. Si les renseignements doivent être conservés uniquement à des fins statistiques, utilisez des techniques efficaces afin de les dépersonnaliser.

- Assurez-vous que tous les renseignements personnels sont entièrement supprimés avant de vous départir d'appareils électroniques comme des ordinateurs, des photocopieurs et des téléphones cellulaires.
- Assurez-vous que vos employés suivent une formation appropriée sur leur rôle et leurs responsabilités en matière de protection des renseignements personnels.

Conseils

- Utilisez des processus efficaces pour détruire, effacer ou dépersonnaliser des renseignements personnels.
- Élaborez des directives et mettez des procédures en place relativement à la conservation des renseignements personnels.
- Procédez à des examens périodiques pour évaluer la nécessité de conserver les renseignements.
- Établissez un calendrier de conservation pour faciliter le processus.

Liens connexes

- [Cinquième principe relatif à l'équité dans le traitement de l'information de la LRPDE - Limitation de l'utilisation, de la communication et de la conservation](#)
- [La LRPDE et la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes \(LRPCFAT\)](#)
- [Conservation et retrait des renseignements personnels : Principes et pratiques exemplaires](#)



6 Soyez précis

Votre responsabilité

- Réduire au minimum les possibilités d'utilisation de renseignements inexacts au moment de prendre une décision concernant une personne ou de communiquer les renseignements à de tierces parties.

Comment vous acquitter de cette responsabilité

- Veillez à ce que les renseignements personnels soient aussi exacts, exhaustifs et à jour que nécessaire, compte tenu de leur utilisation et des intérêts des personnes concernées.
- Établissez des politiques qui régissent les types de renseignements devant être mis à jour.

Conseils

L'une des façons de déterminer si des renseignements doivent être mis à jour consiste à vous demander si l'utilisation ou la communication de renseignements non exhaustifs ou désuets pourrait porter préjudice à la personne concernée.

Utilisez la liste de vérification suivante pour vous assurer de l'exactitude des renseignements :

- Dressez une liste précise des renseignements personnels dont vous avez besoin pour la prestation d'un service.
- Dressez la liste des endroits où tous les renseignements personnels sont conservés.
- Consignez la date à laquelle les renseignements personnels ont été obtenus ou mis à jour.
- Consignez les mesures prises pour vérifier si les renseignements personnels sont exacts, complets et opportuns. Pour ce faire, vous devrez peut-être examiner vos dossiers ou communiquer avec votre client.

Lien connexe

- [Sixième principe relatif à l'équité dans le traitement de l'information de la LPRPDE - Exactitude](#)

7 Utilisez des mesures de protection appropriées

Vos responsabilités

- Protéger les renseignements personnels d'une manière qui correspond à leur degré de sensibilité.
- Protéger tous les renseignements personnels (quelle que soit la manière dont ils sont stockés) contre la perte, le vol ou tout accès, communication, copie, utilisation ou modification non autorisé.

Remarque : La LPRPDE ne précise aucune mesure de sécurité particulière à mettre en place. Votre organisation doit constamment s'assurer qu'elle protège de manière appropriée tous les renseignements personnels en sa possession alors que les technologies évoluent et qu'émergent de nouveaux risques.

Comment vous acquitter de vos responsabilités

- Élaborez et mettez en œuvre une politique de sécurité visant à protéger les renseignements personnels.
- Utilisez des mécanismes de sécurité pertinents pour garantir la protection nécessaire. Voici quelques exemples :
 - » des moyens matériels (p. ex., le verrouillage des classeurs, la restriction de l'accès aux bureaux et des systèmes d'alarme);
 - » des outils technologiques à jour (p. ex. des mots de passe, le chiffrement, les pare-feu et les correctifs de sécurité);

- » des contrôles organisationnels (p. ex. des habilitations de sécurité, des limites d'accès, la formation du personnel et des ententes).

- Tenez compte des facteurs suivants pour choisir la bonne mesure de sécurité :
 - » la nature délicate des renseignements et le risque de préjudice pour la personne (p. ex., des renseignements financiers et des renseignements sur la santé seraient considérés comme très délicats);
 - » la quantité de renseignements;
 - » l'étendue de leur communication;
 - » le format des renseignements (p. ex. électronique ou papier);
 - » le type de stockage;
 - » les types et les niveaux de risques potentiels auxquels votre organisation est confrontée.
- Vérifiez régulièrement les mesures de sécurité pour vous assurer qu'elles sont à jour et que vous avez corrigé les vulnérabilités connues à la suite de vérifications ou de tests réguliers de sécurité.
- Assurez-vous que vos employés sont conscients de l'importance de préserver la sécurité et la confidentialité des renseignements personnels, et organisez régulièrement des formations du personnel sur les mesures de sécurité.



Conseils

- Assurez-vous de supprimer ou de masquer les renseignements personnels qui n'ont pas de rapport avec la transaction lorsque vous distribuez des copies de renseignements.
- Conservez les dossiers qui contiennent des renseignements de nature délicate dans un endroit sécurisé ou dans un système informatique sécurisé, et limitez-en l'accès aux employés selon le principe du « besoin de connaître ».

Liens connexes

- [Septième principe relatif à l'équité dans le traitement de l'information de la LPRPDE – Mesures de sécurité](#)
- [Sécurité des renseignements personnels](#)
- [Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations](#)
- [Bulletin d'interprétation : Mesures de sécurité](#)
- [Dix trucs pour empêcher les employés de fureter](#)
- [Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité](#)
- [Prévenir une atteinte à la vie privée et réagir en cas d'atteinte](#)

Remarque : Pour des renseignements sur les atteintes à la vie privée, consultez la section portant sur ce sujet.



8 Faites preuve de transparence

Les pratiques détaillées de gestion des renseignements personnels de votre organisation doivent être claires et faciles à comprendre. Elles doivent être facilement accessibles.

Les consommateurs trouvent que les politiques en matière de protection de la vie privée sont difficiles à comprendre, mais se sentent tout de même obligés de donner leur consentement afin d'obtenir les biens et les services qu'ils veulent.

On ne devrait pas s'attendre à ce que les gens décodent un langage juridique complexe afin de prendre des décisions éclairées quant à la pertinence ou non de donner leur consentement. (Pour en savoir plus, consultez le Principe 3 portant sur le consentement.)

Vos responsabilités

- Informer vos clients et vos employés du fait que vous avez mis en place des politiques et des pratiques de gestion des renseignements personnels.
- Faire en sorte que ces politiques et pratiques soient compréhensibles et faciles d'accès.

Comment vous acquitter de vos responsabilités

- Conformez-vous aux directives sur l'obtention d'un consentement valable.
- Assurez-vous que vos employés de première ligne connaissent bien les procédures de réponse aux demandes de particuliers concernant leurs renseignements personnels.



- Fournissez, en des termes faciles à comprendre :
 - » le nom ou la fonction de même que les coordonnées de la personne responsable de la politique et des pratiques de confidentialité de votre organisation;
 - » le nom ou la fonction de même que les coordonnées de la personne à qui les demandes d'accès devraient être acheminées;
 - » la marche à suivre pour avoir accès à ses renseignements personnels;
 - » la marche à suivre pour déposer une plainte auprès de votre organisation;
 - » tout document expliquant les politiques, normes ou codes de votre organisation;
 - » une description de tous les renseignements personnels communiqués à d'autres organisations, y compris les filiales de votre organisation et toute tierce partie, et les raisons pour lesquelles ces renseignements sont communiqués.

Conseils

- L'information concernant vos politiques et pratiques devrait être accessible de diverses manières, par exemple, en personne, par écrit, par téléphone, dans des publications ou sur le site Web de votre organisation.
- L'information présentée devrait être cohérente, et ce, peu importe le format.

Liens connexes

- [Huitième principe relatif à l'équité dans le traitement de l'information de la LPRPDE - Transparence](#)
- [Dix conseils pour améliorer votre politique de confidentialité en ligne et la transparence de vos pratiques en matière de protection de la vie privée](#)
- [Lignes directrices pour l'obtention d'un consentement valable](#)



9 Accordez l'accès aux personnes concernées

En général, toute personne a le droit de consulter les renseignements personnels que détient une organisation à son sujet. Elle a également le droit de contester l'exactitude ou l'exhaustivité des renseignements personnels et de demander des corrections, le cas échéant.

Vos responsabilités

- Indiquer à toute personne qui en fait la demande quels sont les renseignements personnels la concernant au sein de votre organisation.
- Expliquer où les renseignements ont été obtenus.
- Expliquer comment les renseignements sont ou ont été utilisés et à qui ils ont été communiqués.
- Donner à la personne un accès gratuit ou à prix modique aux renseignements demandés, ou expliquer vos raisons pour ne pas lui donner accès. L'accès fourni peut prendre différentes formes. Par exemple, vous pouvez fournir une copie papier ou électronique des renseignements, ou permettre à la personne de voir les renseignements ou d'écouter un enregistrement des renseignements.
- Corriger ou modifier les renseignements personnels s'ils ne sont pas exacts ou exhaustifs.
- Consigner tous les différends liés au dossier et, le cas échéant, en informer les tierces parties.



Comment vous acquitter de vos responsabilités

- Donnez à toute personne qui en a besoin l'aide nécessaire pour formuler une demande d'accès à ses renseignements personnels. (Par exemple, votre organisation peut demander à la personne qui présente une demande d'accès de fournir suffisamment d'information pour qu'il vous soit possible de la renseigner sur l'endroit où ils se trouvent et la manière dont ils ont été utilisés ou communiqués.)
- Donnez suite à la demande le plus rapidement possible, au plus tard 30 jours après sa réception.
- Le délai habituel de traitement peut être prolongé d'une période maximale de 30 jours supplémentaires, dans les cas suivants :
 - » l'observation du délai initial de 30 jours nuirait gravement aux activités de votre organisation;
 - » votre organisation a besoin de plus de temps pour mener des consultations;
 - » votre organisation a besoin de plus de temps pour transférer les renseignements personnels sur un support de substitution.

- Si votre organisation prévoit qu'il lui faudra plus temps pour répondre à la demande, vous devez en informer l'auteur de la demande dans les 30 jours suivant la réception de cette dernière et lui indiquer qu'il a le droit de porter plainte auprès du Commissariat.
- Donnez à la personne un accès gratuit ou à prix modique aux renseignements demandés, et informez la personne des coûts approximatifs avant de traiter la demande. Vérifiez auprès d'elle si elle souhaite toujours aller de l'avant avec la demande.
- Veillez à ce que les renseignements fournis soient compréhensibles. Expliquez les acronymes, les abréviations et les codes.
- Si vous apportez des modifications, acheminez les renseignements modifiés à toute tierce partie ayant accès aux renseignements, s'il y a lieu.
- Communiquez par écrit avec toute personne dont la demande d'accès est refusée pour l'aviser de votre décision et lui exposer les motifs de votre refus et les recours possibles. Les recours comprennent la possibilité de déposer une plainte auprès du Commissariat.
- Si votre organisation ne détient pas de renseignements personnels sur le demandeur, en informer ce dernier.

Conseils

- Conservez un registre de l'endroit où les renseignements personnels sont conservés.
- Effectuez une recherche exhaustive pour retracer les renseignements personnels. Cela comprend tant des recherches physiques qu'électroniques.
- Ne communiquez jamais de renseignements personnels à moins d'être certain de l'identité du demandeur et de son droit d'accès.
- Consignez la date à laquelle vous avez reçu la demande d'accès aux renseignements.
- Assurez-vous que les membres de votre personnel connaissent la manière de traiter une demande d'accès.
- La norme juridique permettant de refuser de communiquer des renseignements pour le motif qu'il s'agit de « renseignements commerciaux confidentiels » est très stricte. Soyez prêt à justifier une telle déclaration avant de refuser un accès.

Liens connexes

- [Neuvième principe relatif à l'équité dans le traitement de l'information de la LPRPDE - Accès aux renseignements personnels](#)
- [Réponse aux demandes d'accès à l'information en vertu de la LPRPDE](#)

10 Recevez les plaintes à l'égard du non-respect des principes

Une personne doit être en mesure de remettre en question la conformité de votre organisation relativement aux principes relatifs à l'équité dans le traitement de l'information. Elle doit présenter sa plainte à la personne au sein de votre organisation chargée de la conformité à la LPRPDE.

Vos responsabilités

- Offrir un recours en élaborant des procédures simples de traitement des plaintes et d'enquête.
- Informer les plaignants des possibilités de recours qui s'offrent à eux. Cela comprend les procédures de traitement des plaintes au sein de votre organisation et celles des associations de l'industrie, des organismes de réglementation et du Commissariat.
- Mener des enquêtes sur toutes les plaintes reçues.
- Améliorer les pratiques et les politiques relatives au traitement des renseignements personnels qui posent problème.

Comment vous acquitter de vos responsabilités

- Consignez la date de réception et la nature de la plainte.
- Accusez réception de la plainte sans délai et, au besoin, communiquez avec le plaignant pour obtenir des précisions.
- Confiez le dossier à une personne possédant les compétences voulues pour l'examiner de manière équitable et impartiale. Permettez à cette personne de consulter tous les dossiers pertinents et tous les employés ou autres intervenants qui ont traité les renseignements personnels ou la demande d'accès.
- Informez clairement et rapidement le plaignant du résultat de l'examen de la plainte, et indiquez-lui les mesures qui ont été prises.
- Corrigez tout renseignement personnel inexact ou modifiez les politiques et les procédures à la lumière des conclusions de l'enquête sur la plainte. Assurez-vous que les employés de votre organisation sont au fait de tous les changements apportés à ces politiques et procédures.



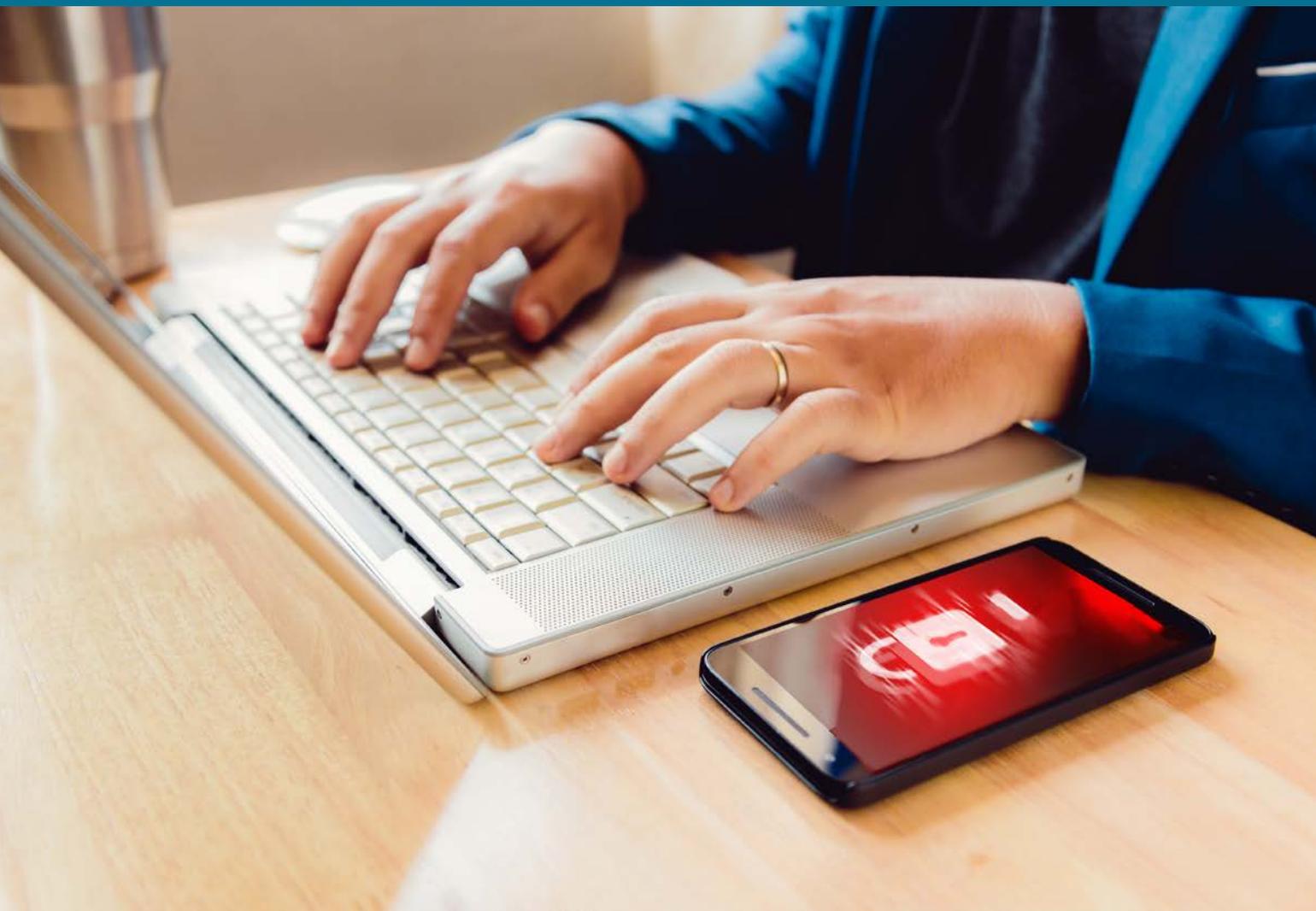
Conseils

- Le traitement équitable d'une plainte peut contribuer à préserver ou à restaurer la confiance de votre client envers votre organisation.
- Assurez-vous que les membres de votre personnel sont au fait des politiques et des procédures en matière de traitement des plaintes et qu'ils savent à qui transmettre les plaintes au sein de votre organisation.
- Consignez toutes vos décisions pour assurer une application uniforme.

Liens connexes

- [Dixième principe relatif à l'équité dans le traitement de l'information de la LPRPDE - Possibilité de porter plainte à l'égard du non-respect des principes](#)
- [Un programme de gestion de la protection de la vie privée : la clé de la responsabilité](#)
- [Dix conseils pour éviter les plaintes au Commissariat](#)

Gérer un cas d'atteinte



On parle d'atteinte aux mesures de sécurité en cas d'accès non autorisé à des renseignements personnels, d'utilisation ou de communication non autorisée de ces renseignements, ou de la perte de ceux-ci. La LPRPDE comprend des exigences en matière de déclaration obligatoire des atteintes.

Les organisations doivent :

- déclarer au Commissariat les atteintes aux mesures de sécurité présentant un risque réel de préjudice grave;
- aviser les personnes touchées et les tierces parties pertinentes de toute atteinte présentant un risque réel de préjudice grave;
- conserver un registre de toutes les atteintes, y compris celles qui ne comportent pas de risque réel de préjudice grave.

Risque réel de préjudice grave

Le risque réel de préjudice grave doit être établi au moyen d'une évaluation du degré de sensibilité du renseignement personnel touché, ainsi que de la probabilité que le renseignement personnel puisse être mal utilisé.

Les préjudices graves comprennent ce qui suit :

- lésion corporelle;
- humiliation, atteinte à la réputation ou détérioration des relations;
- perte d'un emploi, d'occasions d'affaires ou d'activités professionnelles;

- perte financière, vol d'identité, effet négatif sur le dossier de crédit;
- dommage à des biens ou perte de ces derniers.

Ce qui doit figurer dans votre rapport d'atteinte au Commissariat

Les déclarations d'atteinte aux mesures de sécurité présentées au CPVP doivent être consignées par écrit et doivent comprendre :

- une description des circonstances de l'atteinte et, si elle est connue, la cause;
- le moment où est survenue l'atteinte;
- dans la mesure du possible, une description des renseignements personnels visés lors de l'atteinte;
- le nombre ou le nombre approximatif de personnes touchées par l'atteinte;
- les mesures prises par l'organisation afin de réduire le risque de préjudice aux personnes touchées;
- les mesures que prend l'organisation, ou qu'elle prendra, pour aviser les personnes touchées;
- le nom et les coordonnées d'une personne-ressource.

Ce que doit contenir votre avis aux personnes touchées

- essentiellement la même information qui se trouve dans le rapport d'atteinte au Commissariat;
- les mesures que les personnes touchées peuvent prendre pour réduire le risque de préjudice (par exemple changer leurs mots de passe ou surveiller leurs comptes).

Ce que doivent contenir les dossiers dans votre propre registre des atteintes

Le Commissariat peut demander à avoir accès aux dossiers du registre des atteintes d'une organisation ou en demander une copie. Ces dossiers doivent contenir des détails suffisants pour lui permettre d'établir si l'organisation a correctement évalué le risque de préjudice et si elle a respecté ses obligations de déclaration et d'information au sujet d'une atteinte en particulier.

Les dossiers au registre n'ont pas à comprendre de renseignements personnels à moins qu'ils ne soient nécessaires pour expliquer la nature et le degré de sensibilité de l'atteinte, ou pour déterminer la probabilité que les renseignements personnels aient été utilisés à mauvais escient.

Vous êtes tenu par le Règlement sur les atteintes aux mesures de sécurité de conserver tous les dossiers du registre d'atteinte pendant deux ans. D'autres exigences légales pourraient nécessiter que vous les conserviez plus longtemps.

Lien connexe

- [Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité](#)



Plaintes adressées au commissaire à la protection de la vie privée du Canada



Toute personne peut déposer une plainte en vertu de la LPRPDE si elle est d'avis qu'une organisation a enfreint la loi.

Le commissaire à la protection de la vie privée peut également prendre lui-même l'initiative d'une plainte s'il a des motifs raisonnables de croire qu'une enquête devrait être menée.

Processus de plainte

Le commissaire adopte, le plus souvent possible dans ses enquêtes, une approche axée sur la collaboration et la conciliation. Le Commissariat encourage les parties à résoudre les plaintes entre elles, et peut utiliser d'autres méthodes de règlement des différends comme la médiation et la conciliation pour régler des questions à toute étape du processus d'enquête.

Le Commissariat examinera les plaintes et les traitera de l'une des trois manières suivantes :

- en tentant de les résoudre de manière informelle (connue sous le nom de règlement rapide);
- en refusant de procéder à une enquête;
- en décidant de procéder à une enquête.

Les principales étapes de chacun de ces processus sont énumérées ci-après et sont également expliquées dans le [graphique des plaintes et de l'application de la LPRPDE](#) sur notre site Web.

Prenez note que ce qui suit constitue une infraction à la LPRPDE :

- détruire les renseignements personnels demandés par une personne;
- exercer des mesures de représailles contre un employé qui a déposé une plainte auprès du Commissariat;
- nuire à la conduite d'une enquête ou d'une vérification menée par le commissaire ou son délégué.

Règlement rapide

Les plaintes qui peuvent être réglées de manière informelle sont traitées au moyen d'un processus de règlement rapide. Cela est notamment le cas dans les situations suivantes :

- il semble possible de traiter facilement des allégations de manière informelle;
- les parties consentent à régler la question de manière informelle.

À l'aide de ce processus, le Commissariat contribue à trouver une solution satisfaisante pour toutes les parties en l'absence d'une enquête officielle. Aucun rapport de conclusions n'est produit à l'égard des questions qui sont réglées de manière informelle.

Refus d'enquêter

Le Commissariat peut refuser d'enquêter sur une plainte lorsqu'il est d'avis que :

- le plaignant devrait d'abord épuiser les autres recours ou les procédures de grief qui sont à sa disposition;
- la plainte pourrait avantageusement être instruite selon des procédures différentes prévues par une loi fédérale ou provinciale (par exemple, un différend relatif à un contrat de location pourrait être mieux instruit auprès d'un tribunal propriétaire-locataire);
- la plainte n'a pas été déposée dans un délai raisonnable.

Lorsque le Commissariat refuse une plainte, il informe toutes les parties de sa décision et en précise les raisons. Un plaignant peut demander que la décision fasse l'objet d'un réexamen.

Si le Commissariat estime que, selon la demande de réexamen du plaignant, il existe des raisons impérieuses d'enquêter, il renverra l'affaire pour enquête.

Enquêtes

Le processus qui suit précise les étapes habituellement exécutées par le Commissariat pour faire enquête à l'égard de plaintes en matière d'atteinte à la vie privée contre des organisations.

1. Lorsque le Commissariat accepte une plainte pour enquête, il affecte un enquêteur au dossier.
2. Lorsque commence l'enquête, le Commissariat fournit un avis écrit à l'organisation visée expliquant la teneur de la plainte.

3. L'enquêteur communique avec le représentant désigné de l'organisation pour :
 - expliquer la manière dont se déroulera l'enquête;
 - dresser la liste de tous les registres qui doivent être examinés et de tous les membres du personnel à interviewer;
 - indiquer si des visites sur place seront nécessaires.
4. L'enquêteur obtient de l'information directement auprès de personnes qui connaissent bien la question à l'étude.
 - L'enquêteur peut demander à l'organisation de fournir des renseignements ou des documents qui sont pertinents pour l'enquête.
 - S'il procède à une visite des lieux, l'enquêteur peut examiner ou obtenir des copies ou des extraits de documents, y compris ceux qui sont stockés électroniquement, qui se trouvent sur place.
5. Avant la conclusion de l'enquête, les résultats peuvent être communiqués aux parties en cause. Cela peut être fait afin d'obtenir des déclarations supplémentaires, si les parties jugent approprié de les fournir, ou pour donner au répondant l'occasion de régler la question avant la finalisation du processus de plainte.

Remarque : Le Commissariat a le pouvoir de convoquer des témoins, de faire prêter serment et d'obliger des personnes et des organisations à produire des éléments de preuve, ainsi que d'effectuer des visites sur place.

6. En fonction des résultats de l'enquête, le commissaire ou son délégué produira un rapport à l'intention des parties. Le rapport comprend :

- les conclusions de son enquête;
 - toute entente conclue entre les parties;
 - toute recommandation, comme des modifications proposées aux pratiques de gestion des renseignements;
 - les mesures prises par l'organisation ou qui seront prises par celle-ci pour donner suite aux recommandations;
 - un avis de recours auprès de la Cour fédérale.
7. Le commissaire ou son délégué peut exiger qu'une organisation lui présente, dans un délai donné, les mesures qu'elle a prises ou qu'elle envisage de prendre pour donner suite aux recommandations du rapport, ou encore exiger que l'organisation explique pourquoi aucune mesure n'a été ou ne sera prise.
8. Le commissaire peut conclure un accord de conformité avec une organisation s'il a des motifs raisonnables de croire qu'une organisation a commis, ou s'apprête à commettre, ou qu'il est probable qu'elle commette, une infraction à la LPRPDE, ou si elle n'a pas donné suite à une recommandation liée aux dix principes relatifs à l'équité dans le traitement de l'information. En concluant un accord de conformité, une organisation s'engage à prendre certaines mesures en vue de la conformité. Cela empêcherait le commissaire à la protection de la vie privée



d'entreprendre ou de poursuivre une procédure judiciaire sous le régime de la LPRPDE à l'égard de toute question visée par l'accord. Toutefois, si une organisation n'a pas respecté les engagements pris en vertu d'un accord, le Commissariat pourrait, après lui avoir envoyé un avis de défaut, demander à la Cour une ordonnance enjoignant à l'organisation de se conformer aux conditions de l'accord de conformité, ou encore tenter ou rétablir une procédure judiciaire sous le régime de la LPRPDE, selon le cas.

Conclusions et décisions

Une plainte peut habituellement être traitée de l'une ou l'autre des façons suivantes.

1. Hors du champ d'application

À la lumière des renseignements recueillis, le Commissariat détermine que la LPRPDE ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte. Le Commissariat ne produit pas de rapport.



2. Refus d'enquêter

Le Commissariat peut refuser d'enquêter sur une plainte s'il est d'avis que :

- le plaignant devrait d'abord épuiser les autres recours ou les procédures de grief qui sont à sa disposition;
- la plainte pourrait avantageusement être instruite selon des procédures différentes prévues par une loi fédérale ou provinciale;
- la plainte n'a pas été déposée dans un délai raisonnable.

3. Abandonnée

L'enquête prend fin avant que toutes les allégations ne soient pleinement examinées. Le Commissariat peut mettre fin à une enquête s'il estime :

- qu'il n'existe pas suffisamment d'éléments de preuve pour poursuivre l'examen de la plainte;
- que la plainte est futile, vexatoire ou entachée de mauvaise foi;
- que l'organisation a apporté une réponse juste et équitable à la plainte;
- que la plainte fait déjà l'objet d'une enquête;

- qu'un rapport sur l'objet de la plainte a déjà été dressé par le commissaire;
- que la plainte a déjà été refusée.

4. Retirée

Le plaignant a retiré sa plainte volontairement ou n'a pu être joint. Le Commissariat ne produit pas de rapport.

5. Régulée rapidement et réglée en cours d'enquête

Les plaintes qui peuvent être réglées de manière informelle sont traitées au moyen d'un processus de règlement rapide. Cela est notamment le cas dans les situations suivantes :

- il semble possible de traiter facilement des allégations de manière informelle;
- les parties consentent à régler la question de manière informelle.

À l'aide de ce processus, le Commissariat contribue à trouver une solution satisfaisante pour toutes les parties en l'absence d'une enquête officielle. Aucun rapport de conclusions n'est produit à l'égard des questions qui sont réglées de manière informelle.

6. Non fondée

Le Commissariat a déterminé que l'organisation n'a pas contrevenu à la LPRPDE.

7. Fondée et conditionnellement résolue

Le Commissariat a déterminé qu'une organisation a contrevenu à la LPRPDE. L'organisation s'engage à mettre en œuvre les recommandations formulées par le Commissariat et à faire la démonstration de cette mise en œuvre dans les délais prescrits.

8. Fondée et résolue

Le Commissariat a déterminé qu'une organisation a contrevenu à une disposition de la LPRPDE. L'organisation démontre qu'elle a pris des mesures correctives satisfaisantes pour remédier à la situation, soit de sa propre initiative, soit à la suite de recommandations formulées par le Commissariat, au moment où la conclusion a été rendue.

9. Fondée et non résolue

Le Commissariat a déterminé qu'une organisation a contrevenu à une disposition de la LPRPDE, mais n'a pas été en mesure de régler les questions en suspens.

Accords de conformité

Une autre issue possible à la suite d'une plainte est que le commissaire à la protection de la vie privée ou son délégué conclut un accord de conformité avec une organisation afin de s'assurer qu'elle respecte la LPRPDE.

Dans un accord de conformité, une organisation accepte de prendre certaines mesures pour se conformer à la LPRPDE.

Si une organisation n'a pas respecté les engagements pris en vertu d'un accord de conformité, le Commissariat peut demander à la Cour une ordonnance enjoignant à l'organisation de se conformer aux conditions de l'accord, demander une audience ou réintroduire une instance, selon le cas.

Vérifications

La LPRPDE donne au Commissariat le pouvoir de [vérifier les pratiques d'une organisation en matière de protection de la vie privée](#) lorsque le Commissariat a des motifs raisonnables de croire que l'organisation ne s'acquitte pas de ses obligations en vertu de la [Partie 1](#) de la Loi, ou qu'elle ne respecte pas les recommandations de l'[Annexe 1](#).

Circonstances pouvant mener à une vérification

Les renseignements qui peuvent donner lieu à une vérification peuvent provenir de diverses sources, y compris :

- un groupe ou une série de plaintes à propos des pratiques d'une organisation donnée;
- des renseignements obtenus pendant une enquête;
- des renseignements fournis par une personne en vertu de la disposition relative à la dénonciation;
- toute question retenant l'attention du public.

Demander une audience à la Cour fédérale



Un plaignant peut demander une audience à la Cour fédérale dans certains cas, même s'il a été informé qu'une enquête a été abandonnée.

Le Commissariat peut également demander une audience en son propre nom ou au nom d'un plaignant dans certains cas.

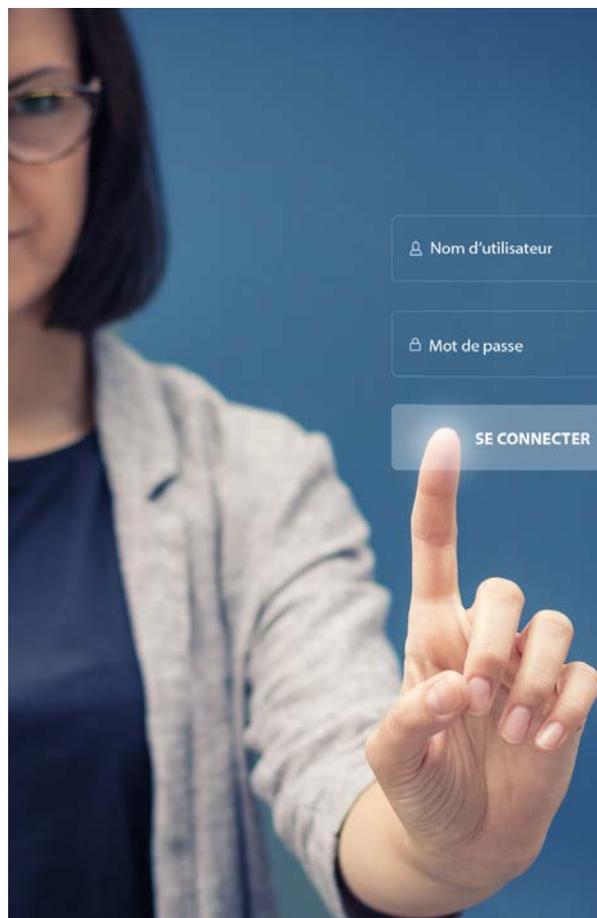
Toute demande d'audience doit être présentée dans un délai d'un an suivant la production du rapport de conclusions du Commissariat, ou suivant l'avis par le Commissariat qu'une plainte a été abandonnée, bien que la Cour puisse prolonger ce délai.

Les demandes d'audience devant la Cour peuvent seulement porter sur la question ayant fait l'objet d'une plainte ou sur une question qui est mentionnée dans le rapport produit par le Commissariat, et doivent se rapporter à l'une des dispositions énumérées à [l'article 14 de la Loi](#).

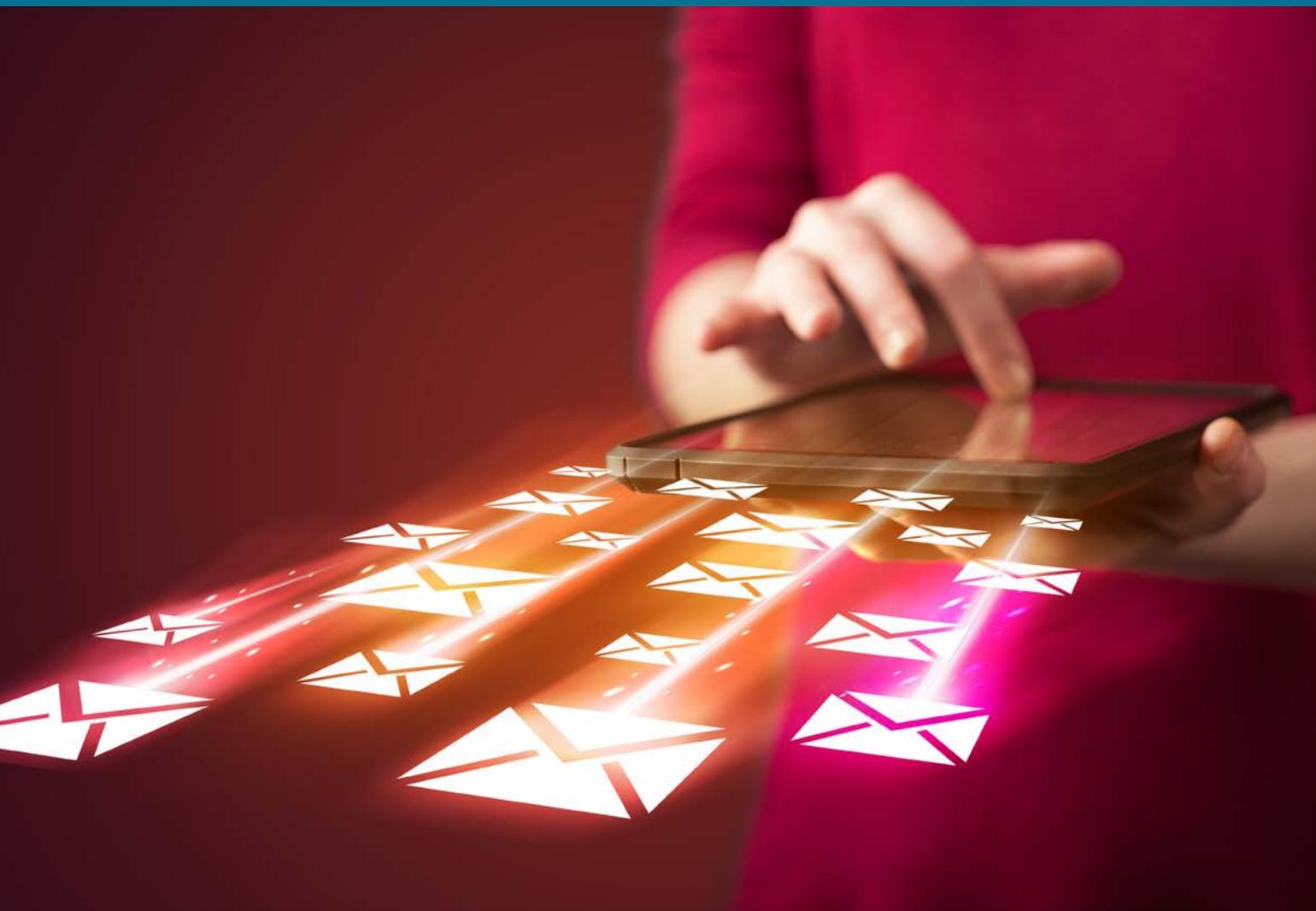
La Cour fédérale peut ordonner à une organisation de corriger des pratiques non conformes à la Loi. Elle peut aussi ordonner à une organisation de publier un avis faisant état des mesures prises ou envisagées pour corriger ces pratiques. Elle peut également accorder des dommages-intérêts au plaignant, notamment pour une humiliation subie.

Lien connexe

- [Demandes d'audience à la Cour fédérale en vertu de la LPRPDE](#)



La Loi canadienne anti-pourriel et la LPRPDE





La Loi canadienne anti-pourriel (LCAP) protège les consommateurs et les entreprises contre la mauvaise utilisation de la technologie numérique, y compris les pourriels et autres menaces électroniques. Elle vise à aider les entreprises à demeurer concurrentielles sur un marché mondial numérique.

La LCAP promeut les pratiques exemplaires en matière de marketing par courriel et cherche à lutter contre les pourriels et les problèmes connexes, comme le vol d'identité, l'hameçonnage et la propagation de logiciels malveillants comme les virus, les vers et les chevaux de Troie (malicieux).

Lorsque la LCAP est entrée en vigueur en 2014, elle a modifié la LPRPDE afin d'inclure de nouvelles restrictions relatives à la collecte d'adresses électroniques et de renseignements personnels à l'aide de logiciels espions.

Le Commissariat partage la responsabilité de l'application de la LCAP avec deux autres organismes : le Conseil de la radiodiffusion et des télécommunications canadiennes et le Bureau de la concurrence.

Les restrictions touchant la collecte d'adresses sont pertinentes pour les organisations de toute taille dans tous les secteurs.

Les organisations ont la responsabilité de s'assurer que toutes les personnes à qui elles envoient leurs messages électroniques ont donné leur consentement pour que leur adresse soit recueillie et utilisée à des fins de marketing ou à d'autres fins.

Afin d'assurer que votre organisation se conforme à la LCAP et pour savoir comment la protéger contre les cybermenaces, visitez combattrepourriel.gc.ca ou consultez notre site Web à l'adresse priv.gc.ca (recherchez « pourriel »).

Services-conseils aux entreprises



Une partie du rôle du Commissariat est d'aider les organisations à comprendre leurs obligations en matière de protection de la vie privée et à se conformer à la Loi. Nos services-conseils aux entreprises peuvent vous conseiller sur les incidences que peuvent avoir vos nouveaux programmes ou nouvelles initiatives sur la vie privée.

Nous pouvons également passer en revue la manière dont vous gérez la protection de la vie privée afin de cerner les bonnes pratiques et les risques potentiels, et vous fournir une orientation débouchant sur des mesures qui vous permettront d'assurer la conformité de vos pratiques à la LPRPDE.

Tous les services-conseils aux entreprises du Commissariat sont offerts sur une base volontaire et sans frais. Toutes les entreprises du Canada assujetties à la LPRPDE peuvent demander des conseils. Les services-conseils sont fournis en fonction de la capacité et de la disponibilité des ressources. Nous accordons la priorité aux projets comportant des risques plus élevés en matière de protection de la vie privée ou ayant d'importantes incidences sur les Canadiens.



Pour plus de renseignements, communiquez avec :
Commissariat à la protection de la vie privée du Canada
30, rue Victoria, 8^e étage
Gatineau (Québec) K1A 1H3

Téléphone : 819-994-5444

Sans frais : 1-800-282-1376

ATS : 819-994-6591

Pour plus de renseignements, consultez : priv.gc.ca/entreprise

Suivez-nous sur Twitter : [@priveepriacy](https://twitter.com/priveepriacy)

