

TROUSSE À OUTILS

CONFORMITÉ LOI 25

Liste des politiques et procédures obligatoires et recommandées :

(Attention, chaque organisation peut avoir des besoins différents. La consultation avec un avocat spécialisé en vie privée est fortement recommandée) :

Structuration d'un programme de protection des renseignements personnels (PRP) :

- ✓ Délégation écrite officielle du Responsable PRP (obligatoire)
- ✓ Détermination des rôles et responsabilités dans le cadre de la gestion du programme PRP (RACI / Responsable, approbateur, consulté et informé) (recommandé)
- ✓ Intégration du risque PRP dans l'organisation + établissement de la tolérance au risque PRP dans la documentation existante (ou documentation complémentaire)

Rédaction de documentation obligatoire détaillée (obligatoires) :

- ✓ Politique interne de gestion des renseignements personnels
- ✓ Gestion des renseignements personnels d'employés OU Modification du Manuel de l'employé, si existant
- ✓ Conservation et destruction des renseignements personnels
- ✓ Gestion des demandes d'individus (accès, rectification, etc.) et plaintes
- ✓ Révision de la politique de confidentialité web (« customer-facing », à être publiée en ligne) (obligatoire)
- ✓ Préparation d'un modèle d'Évaluation des facteurs relatifs à la vie privée (EFVP) (obligatoire)
- ✓ Ajout d'un Addenda de protection des renseignements personnels aux contrats actuels (obligatoire)
- ✓ Rédaction d'un processus de gestion des incidents de confidentialité OU ajouts nécessaires aux procédures actuelles
- ✓ Création d'un registre des incidents de confidentialité OU ajouts au registre existant, le cas échéant

Rédaction de documents facilitant les opérations (recommandé) :

- ✓ Rédaction d'un engagement à la confidentialité pour les employés (fortement recommandé)
- ✓ Création d'un processus « d'onboarding » de nouveaux fournisseurs de services (approvisionnement) (fortement recommandé)
- ✓ Création d'un registre des traitements des renseignements personnels (ROPA)
- ✓ Rédaction d'un processus de mise à jour des documents reliés à la vie privée (par ex. fréquence annuelle – processus d'approbation)

Programme de formation en protection des renseignements personnels (fortement recommandé) :

- ✓ Création d'un programme de formation continue en protection des renseignements personnels, incluant :
 - Formation de base complète à faire à l'embauche
 - Formation continue à faire annuellement
 - Formations spécifiques pour certains types de rôles

[Guide pratique sur l'application de la Loi 25 par CyberEco](#)

Gouvernance de données :

- Informations introductives sur la gouvernance de données :
<https://libeo.com/publications/comment-introduire-une-saine-gouvernance-des-donnees%E2%80%89/>
- Présentation sur la gouvernance des données de Synapse pour Événements Attractions Québec :
<https://evenementsattractions.quebec/satq/pdf/Accompagnement/Numerique/Guide3-Gouvernance-donnees-EAQ.pdf>
- Présentation de l'ISACA-Québec sur la gouvernance des données du 19 mai 2022 :
https://isaca-quebec.ca/assets/pdf/20220512_Pr%C3%A9sentation-Isaca-Qu%C3%A9bec-19-mai-2022_Intervention-Gouvernance-des-donn%C3%A9es_HJadi.pdf?_cchid=e949e97356a289765f7c7adac4567f71
- Cadre de la gouvernance des données de l'Université Concordia (de type politique) :
https://www.concordia.ca/content/dam/common/docs/politiques/PRVPA-4_Cadre.pdf
- Cadre de la gouvernance des données de la Défense Nationale (Canada) :
<https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/gouvernance-donnees.html> (complexe, mais ça vous donne une idée de ce que ça peut être à maturité)
- Marche à suivre : établissement d'un cadre de gouvernance de la donnée :
https://cippic.ca/sites/default/files/file/Explicatif_%C3%89tablissement_d%E2%80%99un_cadre_de_gouvernance_des_donn%C3%A9es.pdf

Cette formation est d'une durée de 7 heures et elle est donnée à distance par l'Université de Sherbrooke à quelques reprises dans une année :

<https://www.usherbrooke.ca/formation-continue/programmation/activite/introduction-a-la-gouvernance-donnees/845/>

Traitement des incidents de confidentialité :

- [Incidents de confidentialité et mesures de sécurité \(QC\)](#)
- [Comment réagir à une atteinte à la vie privée dans votre entreprise \(Fédéral\)](#)
- [Breach Notification Processing Changes under PIPA \(Alberta\)](#)
- [How to Notify the Commissioner of a Privacy Breach \(Alberta\)](#)
- [Privacy breaches: tools and resources for the private sector \(Colombie-Britannique\)](#)
- [Modèle d'avis à la personne concernée par un incident de confidentialité causant un préjudice sérieux \(Gouvernement du Québec\)](#)

Registre des incidents de confidentialité :

- Page d'information de la CAI : <https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/registre/>
- [Modèle de registre des incidents de l'Ordre des physiothérapeutes](#)
- [Modèle de registre des incidents de confidentialité de Cyberéco](#)
- [Modèle de registre des incidents de confidentialité du Gouvernement du Québec](#)

Demandes d'accès à l'information :

- Document de la CAI sur le repérage sérieux et complet dans le cadre des demandes d'accès :
https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FIC_DEM_Revision_Mesentente.pdf
- Procédure de traitement des demandes d'accès de l'Université d'Ottawa (bon départ, mais mériterait d'être un peu plus détaillé) : <https://www.uottawa.ca/notre-universite/politiques-reglements/methode-20-5-traitement-des-demandes-daccès-linformation> (ATTENTION! L'université d'Ottawa n'est pas soumise à la Loi 25 – il y a des différences entre les lois en ce qui concerne l'accès à l'information)
- Procédure de traitement des demandes d'accès pour les ministères et organismes fédéraux :
<https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=18310§ion=HTML>
(ATTENTION! Les organismes fédéraux ne sont pas soumis à la Loi 25 – il y a des différences entre les lois en ce qui concerne l'accès à l'information)

Comme il n'y a pas énormément de documents bien faits et pertinents disponibles en ligne, il pourrait être bon de se demander si vous ne souhaitez pas qu'un avocat vous fournisse une politique rédigée sur le sujet.

Évaluation des facteurs relatifs à la vie privée :

Voici des Guides d'accompagnement concernant les EFVP, qui peuvent vous être utiles pour créer votre propre EFVP et qui contiennent parfois un modèle à même le document:

- [Guide d'accompagnement de la Commission d'accès à l'information du Québec](#)
- <https://cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/responsable-protection-renseignements-personnels-entreprise#EFVP>
- [Privacy Impact Assessment for Organizations \(OIPC Colombie-Britannique\)](#)
- [Planning for Success : Privacy Impact Assessment Guide \(IPC Ontario\)](#)
**Attention, ce ne sont que les organisations du secteur de la santé qui sont pour le moment soumises aux PIAs en Ontario
- [Nos attentes : Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée](#) ** Attention, pour le moment ce guide ne s'adresse qu'aux organismes publics soumis à la LPRP au Fédéral. Cependant, on peut présumer que les attentes du Commissariat soit similaires ou les mêmes, lorsque le projet de loi C-27 sera adopté.

Délégation de fonctions au Responsable de la protection des renseignements personnels

- [Modèle de formulaire de délégation offert gratuitement par CyberEco](#)

Politique interne

- [Politique interne de l'Autorité des marchés financiers du Québec \(**ATTENTION, il s'agit d'un organisme public soumis à la Loi sur l'accès\)](#)

Politique de confidentialité (web)

- [Rédiger une politique de confidentialité \(CAI Qc\)](#)
- [Politique de confidentialité de CNC](#)

- [Modèle de politique de confidentialité à adapter fourni gratuitement en ligne par Synapse \(pas parfait mais très bien\)](#)

Addenda de protection des renseignements personnels

Comme il s'agit d'un ajout à vos contrats, nous vous recommandons de consulter un avocat pour cette portion de votre mise en conformité.

- [Annexe sur la gestion des tiers par CyberEco](#)

Certifications pour les Responsables de la protection des renseignements personnels :

- IAPP
- ISACA
- Exin Privacy & Data Protection
- DCSI
- TrustArc
- Identity Management Institute
- Privacy and Access Council of Canada

Où trouver des conseils et des informations sur les lois relatives à la protection de la vie privée au Canada ?

Fédéral - Commissariat à la protection de la vie privée du Canada

Le site web du Commissariat à la protection de la vie privée du Canada contient une multitude d'informations et de publications utiles. Voici celles qui nous semblent essentielles à la pratique d'un Responsable de la protection des renseignements personnels.

Bulletins d'interprétation (PIPEDA)

- ✓ [Renseignements sensibles \(mai 2022\)](#)
- ✓ [Accès aux renseignements personnels \(révisé : juin 2020\)](#)
- ✓ [Activité commerciale \(janvier 2017\)](#)
- ✓ [Transparence \(août 2015\)](#)
- ✓ [Mesures de sécurité \(juin 2015\)](#)
- ✓ [Information accessible au public \(mars 2014\)](#)
- ✓ [Forme de consentement \(mars 2014, actuellement en révision\)](#)
- ✓ [Renseignements personnels \(octobre 2013\)](#)
- ✓ [Exactitude \(mai 2013\)](#)
- ✓ [Responsabilité \(avril 2012\)](#)

Lignes directrices

- ✓ [Principes pour des technologies de l'intelligence artificielle \(IA\) générative responsables, dignes de confiance et respectueuses de la vie privée \(décembre 2023\)](#)
- ✓ [Document accompagnateur – Mettre l'intérêt supérieur des jeunes à l'avant-plan en matière de vie privée et d'accès aux renseignements personnels \(octobre 2023\)](#)
- ✓ [Déclaration commune sur l'extraction de données et la protection des renseignements personnels \(août 2023\)](#)
- ✓ [La protection des renseignements personnels au travail \(mai 2023\)](#)
- ✓ [Tenez compte des risques : transmission de renseignements personnels par télécopieur \(mars 2023\)](#)
- ✓ [Considérations en matière de vie privée dans le cadre d'activités d'embauche virtuelles \(février 2023\)](#)
- ✓ [Permettre aux entreprises et aux particuliers de se protéger contre les cyberattaques qui exploitent la réutilisation de mots de passe \(juin 2022\)](#)
- ✓ [Lignes directrices pour l'obtention d'un consentement valable \(révisé en août 2021\)](#)
- ✓ [Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne \(révisé en août 2021\)](#)
- ✓ [Position de principe sur la publicité comportementale en ligne \(révisé en août 2021\)](#)
- ✓ [Guide sur la protection de la vie privée à l'intention des entreprises \(révisé en octobre 2020\)](#)
- ✓ [Nos attentes : Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée](#)
- ✓ [Conseils utiles pour les entreprises œuvrant dans le domaine du cybermarketing \(avril 2015\)](#)
- ✓ [Foire aux questions en matière de consentement en ligne \(mai 2014\)](#)
- ✓ [Dix conseils aux professionnels des ressources humaines \(février 2012\)](#)
- ✓ [L'infonuagique et la protection de la vie privée \(octobre 2011\)](#)
- ✓ [Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée \(février 2011, en cours de révision\)](#)
- ✓ [Transfert transfrontalier de renseignements personnels \(janvier 2009\)](#)
- ✓ [Document d'orientation sur la surveillance vidéo secrète dans le secteur privé \(mai 2009\)](#)
- ✓ [Application de la Loi sur la protection des renseignements personnels et les documents électroniques aux dossiers du personnel \(mai 2004\)](#)

Québec – Commission d'accès à l'information (CAI)

Règlements

- ✓ [Règlement sur les incidents de confidentialité](#)

Lignes directrices

- ✓ [Lignes directrices sur les critères de validité du consentement](#)

La plupart des informations et des conseils disponibles sur le site web de la CAI ne sont publiés qu'en français.

- ✓ [Protection des renseignements personnels - Entreprises et organisations privées](#)
- ✓ [Qu'est-ce qu'un renseignement personnel ?](#)
- ✓ [Fonctions de la personne responsable de la protection des renseignements personnels](#)
- ✓ [Renseignements publics](#)
- ✓ [Utilisation et communication de renseignements personnels](#)
- ✓ [Conservation et destruction des renseignements personnels](#)
- ✓ [Consentement](#)
- ✓ [Cadre général d'application des sanctions administratives pécuniaires](#)

Alberta – Office of the Information Privacy Commissioner

- ✓ [Web buckets \(October 2020\)](#)
- ✓ [Work from Home: Transitioning Records \(April 2020\)](#)
- ✓ [Privacy Impact Assessments Requirements Guide](#)
- ✓ [Phishing \(mai 2019\)](#)
- ✓ [Guidelines for Managing Emails \(mars 2019\)](#)
- ✓ [Key Steps in Responding to Privacy Breaches \(mise à jour août 2018\)](#)
- ✓ [Reporting a Breach to the Commissioner \(août 2018\)](#)
- ✓ [Notifying Affected Individuals Under PIPA \(mise à jour août 2018\)](#)
- ✓ [OIPC Process for Determining Whether to Require Notification \(mise à jour août 2018\)](#)
- ✓ [Authorization to disregard Access Requests \(juin 2017\)](#)
- ✓ [Privilege practice note \(décembre 2016\)](#)
- ✓ [Guidelines for Social Media Background Checks \(December 2011\)](#)
- ✓ [Video Surveillance in the Private Sector \(March 2008\)](#)

Colombie-Britannique – Office of the Information Privacy Commissioner

Des webinaires intéressants sont mis à la disposition des organisations sur le site web de l'OIPC :

- ✓ [Guide to PIPA \(octobre 2015\)](#)
- ✓ [Reasonable security measures for personal information disclosures outside Canada \(mars 2022\)](#)
- ✓ [Guide for organizations collecting personal information online \(mai 2021\)](#)
- ✓ [Securing personal information: A self-assessment for public bodies and organizations \(octobre 2020\)](#)
- ✓ [Privacy Impact Assessments for the Private sector \(janvier 2020\)](#)
- ✓ [Responding to PIPA privacy complaints \(octobre 2019\)](#)
- ✓ [Disclosure of personal information of individuals in crisis \(septembre 2019\)](#)
- ✓ [Developing a privacy policy under PIPA \(mars 2019\)](#)
- ✓ [Competitive Advantage: Compliance with PIPA and the GDPR \(mars 2018\)](#)
- ✓ [Access to data for health research \(janvier 2018\)](#)
- ✓ [Employee Privacy Rights \(novembre 2017\)](#)
- ✓ [Guidance Document: Information Sharing Agreements \(septembre 2017\)](#)
- ✓ [Guide to OIPC Processes \(PIPA\) \(mai 2017\)](#)

- ✓ [IT Security and Employee Privacy: Tips and Guidance](#) (juin 2015)
- ✓ [Protecting Personal Information Away from the Office](#) (janvier 2015)
- ✓ [Practical Suggestions for your Organization's Website's Privacy Policy](#) (août 2018)

Des formations en ligne ont été créées par le SRIDAIL pour le Québec.

Elles s'adressent spécifiquement aux organismes publics, mais peuvent permettre aux entreprises privées et aux OSBL de mieux comprendre certains concepts de la Loi 25 :

- ✓ [Practical Suggestions for your Organization's Website's Privacy Policy](#) (août 2018)