

Se conformer à la Loi 25

Les obligations et les points importants
pour rédiger sa politique de confidentialité

Contenu

Les sujets traités

- Obligations
- Éléments essentiels
- Présentation des modèles
- Travailler sur vos politiques de confidentialité

LES OBLIGATIONS

Depuis septembre 2022 et jusqu'à septembre 2024, de nouvelles obligations sont mises en place annuellement.

Septembre 2022

Personne responsable

1. Le CA de l'organisme doit par **résolution** désigner une personne responsable de la protection des renseignements personnels.
2. Les coordonnées de cette personne doivent être affichées sur le **site web** de l'organisme.
3. La Commission d'accès à l'information du Québec doit également être avisée à l'aide de ce **formulaire**.

Registre d'incidents

Tenir un registre d'incidents. Puis, en cas de violation de la confidentialité :

- Prendre les mesures pour que la situation ne se reproduise pas;
- Avertir la Commission d'accès à l'information du Québec et la personne concernée (si préjudice);
- [Accéder à notre gabarit de registre ici](#)

Inventaire des renseignements

Faire l'inventaire des renseignements personnels que détient l'organisme et le tenir à jour.

- [Accéder à notre gabarit d'inventaire ici](#)

Septembre 2023

Politique

Établir une politique de gestion des renseignements personnels, la faire adopter par le CA et la publier.

- [Accéder à notre gabarit de politique ici](#)

Consentement

Respecter les nouvelles règles pour le consentement à la collecte et à l'utilisation des renseignements personnels.

Détruire ou anonymiser les renseignements personnels

Une fois la finalité des renseignements accomplie, ces derniers doivent être détruit ou anonymiser.

Septembre 2024

Portabilité

Être en mesure de communiquer et de rendre accessibles aux personnes (ou à un organisme autorisé par la Loi à les représenter) les renseignements personnels qui les concernent dans un délai de 30 jours.

LES ESSENTIELS

Les essentiels

1. Objectif de la politique
2. Définitions des données personnelles et confidentielles
3. Les raisons de la collecte de donnée et l'engagement à ce que leur usage se restreigne à ce qui est nécessaire
4. Gestion des témoins/cookies qui doivent être désactivés jusqu'à consentement
5. Gestion des renseignements
6. Gestion de l'accès aux renseignements
7. Gestion du partage à des tiers
8. Gestion de la confidentialité et d'incident qui y serait lié
9. Recours
10. Les annexes

Objectifs de la politique

Pour présenter à quoi elle sert, ça sert d'introduction (point 1).

Définitions

Il est essentiel de donner la définition de « renseignements personnels » :

Par « renseignements personnels », on entend tous les renseignements sur une personne identifiable ou permettant d'identifier une personne.

Il est possible d'ajouter plusieurs définitions qui peuvent aider à l'interprétation de la Politique (voir annexe 3).

Les façons de collecter de données

La façon dont les renseignements sont acquis, consentement manifeste, libre, éclairé, spécifique, granulaire, compréhensible, temporaire et distinct. (point 3)

Les raisons de la collecte de données

La politique doit inclure les raisons lié à la collecte des données et s'engager à en faire un usage qui se restreigne à ce qui a été consenti (point 4 et 5).

Gestion des témoins/cookies et autres technologies

Les sites web recueillent beaucoup d'informations sur les utilisateur·ices, il est donc important d'inclure les détails concernant les témoins et autres technologies comme Google Analytics. (point 6)

À noter : Sur votre site web, les témoins/cookies doivent être désactivés automatiquement, jusqu'à consentement.

La conservation des renseignements

La politique doit inclure les méthodes de conservation des données (lieu physique, lieu du serveur), prévoir leur sécurité et à leur destruction ou dépersonnalisation. (point 7)

Gestion de l'accès aux renseignements

La politique doit expliciter les mesures d'accès aux données, de modifications de celles-ci et la possibilité de les retirer sur demande (point 8).

Gestion du partage à des tiers

La politique doit inclure son mode de gestion de partage des données avec des tiers. Celui-ci doit absolument inclure le consentement de la personne (point 9).

Il est important de spécifier qu'il existe des raisons juridiques qui peuvent outrepasser le consentement.

Gestion de la confidentialité et d'incident qui y serait lié

La politique doit définir ce qu'est un « incident de confidentialité », les obligations liées à la confidentialité et la procédure lorsqu'il y a constatation (point 10, 11 et 12).

À noter que vous aviez également à créer un registre d'incident dont nous vous fournirons un modèle.

Les recours

La politique doit inclure les recours qui peuvent être pris :
plainte auprès de l'organisme, auprès du CA, plainte auprès de
la Commission d'accès à l'information, ainsi que les situations
justifiant leur usage (point 13).

Les annexes

1. Responsable de l'accès aux documents et de la protection des renseignements personnels
2. Déclaration relative à la confidentialité
3. Définitions
4. Évaluation du risque sérieux de préjudice

Avertissement

Selon le secteur d'activités de votre organisme, d'autres obligations pourraient s'ajouter; comme par exemples :

- Organismes qui travaille avec des personnes mineures (Loi sur la protection de la jeunesse)
- Organismes qui doit vérifier les antécédents judiciaires de son personnel permanent et/ou des bénévoles (Loi sur le casier judiciaire)
- D'autres obligations pourraient aussi s'ajouter par la Loi sur les services de santé et les services sociaux ou encore la Loi sur l'assurance maladie

NOS MODÈLES

- Modèle - Politique de confidentialité
 - Inclus les annexes présentés précédemment
- Modèle - Registre des incidents de confidentialité
- Modèle - Inventaire des renseignements personnels

Merci !

Écrivez-nous si vous avez des questions!



CDC
des Grandes Marées

Page de Ressources

- [Avis à la commission d'accès à l'information concernant un incident de confidentialité impliquant des renseignements personnels et qui présente un risque de préjudice sérieux](#)
- [Formulaire de désignation d'une personne responsable et délégation de responsabilités en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#)
- [Lignes directrices 2023-1 – Consentement : critères de validité](#) - Commission d'accès à l'information