



Aide-mémoire

Protection des renseignements personnels



Des questions à se poser pour se conformer à la loi : Avez-vous...



Désigné une personne RPRP?

La personne RPRP est, par défaut, celle qui a la plus grande autorité dans l'organisme. Il est possible de désigner une autre personne ou de déléguer certaines des responsabilités **par écrit**.

Vous devez publier les coordonnées de la personne RPRP sur votre site Web. Si vous n'avez pas de site Web, vous devez en informer le public par un autre moyen (courriel, annonce, etc.).



Adopté une politique interne de gouvernance?

Vous devez développer une politique qui explique les règles applicables concernant la collecte, la conservation et la destruction des renseignements; la répartition des responsabilités dans l'équipe et le processus de plainte.



Défini les paramètres de votre collecte?

Vous devez savoir quels renseignements vous souhaitez collecter, dans quel but et pour quelle durée. La collecte doit être **limitée aux renseignements nécessaires** pour votre but. Vous devez également savoir quels moyens seront utilisés pour faire la collecte.



Rendu disponible une politique de confidentialité?

Vous devez fournir aux personnes concernées une politique de confidentialité claire et accessible. Si vous avez un site Web, la politique doit y être publiée.

La politique explique comment votre organisme collecte, utilise et protège les renseignements personnels.



Obtenu un consentement valide?

Vous devez notamment expliquer aux personnes pourquoi leurs renseignements sont recueillis, comment ils sont recueillis et le fait qu'elles ont le droit de retirer leur consentement.

En pratique, ces informations se retrouvent généralement dans une **politique de confidentialité**.



Pris des mesures raisonnables pour protéger les renseignements personnels?

Plus vous détenez de renseignements personnels et plus leur gestion est risquée, plus les mesures de sécurité que vous devez mettre en place doivent être robustes.

Vous devez notamment faire une évaluation des facteurs relatifs à la vie privée (EFVP) et inclure des clauses sur la protection des renseignements personnels dans vos contrats de services lorsque nécessaire.



Après un incident de confidentialité : Avez-vous...

Un **incident de confidentialité** peut arriver lorsqu'une personne **consulte, utilise ou communique** un renseignement personnel **sans y être autorisée par la loi**, ou lorsqu'un renseignement personnel est **perdu**.

☐ Pris des mesures raisonnables pour limiter les conséquences?

Vous devez **immédiatement** prendre des mesures raisonnables pour limiter les conséquences d'un incident de confidentialité. Par exemple, ça peut vouloir dire :

- désactiver les accès compromis ou changer les mots de passe,
- demander la suppression des renseignements transmis par erreur.

Vous devez également prendre des mesures pour éviter que d'autres incidents similaires aient lieu.

☐ Évalué le niveau de risque?

Lorsqu'un incident a lieu, vous devez évaluer son niveau de risque pour les personnes concernées. Vous devez considérer, notamment :

- la sensibilité des renseignements concernés,
- les conséquences possibles de leur utilisation,
- la probabilité qu'ils soient utilisés de manière à leur nuire.

La personne RPRP de votre organisme doit être impliquée dans cette évaluation.

☐ Avisé les bonnes personnes?

Si vous jugez qu'un **risque de préjudice sérieux** existe, vous devez aviser la Commission de l'accès à l'information de l'incident de confidentialité.

Dans la majorité des cas, vous devez également aviser les personnes concernées. Cet avis doit contenir différentes informations, comme :

- une description des renseignements visés par l'incident,
- une description de l'incident, dont la date ou la période à laquelle l'incident a eu lieu,
- une description des mesures prises pour limiter les conséquences.

☐ Complété votre registre des incidents?

Vous devez compléter le registre chaque fois qu'un incident a lieu, peu importe la gravité de l'incident.

Chaque incident doit y être conservé pendant au moins cinq ans.

Un **préjudice sérieux** est un acte ou un événement qui peut causer une **conséquence négative non négligeable** à la personne concernée, à ses biens ou à ses intérêts. Il peut entraîner, par exemple :

- une atteinte à la réputation,
- une perte financière,
- un vol d'identité.