Procédure de gestion des incidents de confidentialité concernant des renseignements personnels

Adoptée le 23 octobre 2023

1. PRÉAMBULE

Comme le prévoit sa Politique de protection des renseignements personnels, l'Organisation accorde une importance à la protection des Renseignements personnels qu'elle détient. Ainsi, elle met en œuvre les moyens technologiques et administratifs nécessaires afin que ceux-ci soient correctement traités tout au long de leur Cycle de vie. Cependant, malgré les précautions prises, un Incident peut arriver. L'Organisation se dote donc de la présente procédure pour gérer les éventuels Incidents de confidentialité et en limiter les conséquences pour les Personnes concernées et l'Organisation.

2. OBJET

La présente procédure :

- Décrit les étapes à suivre lors d'un Incident de confidentialité;
- Rappelle l'obligation de notification et ses modalités;
- Définit les rôles et responsabilités des parties prenantes.

3. CADRE NORMATIF

La présente procédure s'inscrit dans un contexte régi notamment par les articles 3.5 à 3.8 de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

4. DÉFINITIONS

Aux fins de la présente procédure, on entend par :

Règlement : le *Règlement sur les incidents de confidentialité*.

Les sigles ou les autres termes commençant par une majuscule sont définis à la section 4 de la Politique de protection des renseignements personnels.

5. CHAMP D'APPLICATION

La présente procédure s'applique :

- À tous les membres du personnel de l'Organisation ayant connaissance d'un Incident de confidentialité concernant des Renseignements personnels détenus ou traités par l'Organisation;
- Aux tiers traitant des Renseignements personnels pour le compte de l'Organisation ou ayant accès à de tels renseignements et ayant connaissance d'un Incident de confidentialité relatif à ces renseignements.

6. PROCESSUS DE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

6.1 Signalement d'un Incident de confidentialité

Les membres du personnel de l'Organisation signalent sans délai au Comité tout Incident de confidentialité ou suspicion d'Incident de confidentialité dont ils ont connaissance.

Le Comité et les tiers signalent sans délai à la RPRP (rprp@upadi.ca, 514-715-1890) tout Incident de confidentialité ou suspicion d'Incident de confidentialité dont ils ont connaissance.

Lorsque possible, l'auteur du signalement prend sans tarder les mesures adéquates afin de contenir l'Incident de confidentialité et d'en limiter les effets.

6.2 Questions visant à déterminer s'il s'agit d'un Incident de confidentialité

La RPRP détermine si l'on est bien en présence d'un Incident de confidentialité.

Pour ce faire, elle répond aux deux questions suivantes :

1. Les informations qui font l'objet de l'Incident de confidentialité sont-elles des Renseignements personnels protégés par la Loi?
2. Ces Renseignements personnels ont-ils fait l'objet :
   - D'une consultation par une personne ou une entité non autorisée à en prendre connaissance?
   - D'une transmission à une personne ou une entité non autorisée à les recevoir?
   - D'une utilisation à des fins non autorisées par la Loi ou par la Personne concernée?
   - D'une perte ou d'un vol dans des circonstances qui mènent à croire qu'une des trois hypothèses mentionnées ci-dessus est plausible?

Si les réponses aux deux questions sont affirmatives, on poursuit le processus en remplissant le registre des Incidents de confidentialité. En revanche, si l'une des réponses aux deux questions est négative, il n'y a pas d'Incident de confidentialité.

6.3 Actions correctives et préventives

La RPRP donne instruction au Comité ou au tiers ayant signalé l'Incident de confidentialité pour la mise en place :

- De mesures correctrices nécessaires pour faire cesser l'Incident de confidentialité;
- De mesures préventives appropriées afin d'éviter qu'un tel Incident ne se reproduise.

6.4 Évaluation du risque de préjudice sérieux

Si elle conclut qu'un Incident de confidentialité imputable à l'Organisation est survenu, la RPRP évalue le risque pour la Personne concernée qui découle d'un tel Incident.

Pour ce faire, elle détermine :

1. Le niveau du préjudice, en considérant :
   - La criticité (objective) des Renseignements personnels concernés;
   - Les répercussions potentielles de l'Incident de confidentialité pour la Personne concernée, compte tenu de la sensibilité (subjective) des Renseignements personnels en cause.
2. La probabilité de survenance du préjudice, en analysant le contexte de l'Incident et en en déduisant :
   - Le niveau de vulnérabilité des Renseignements personnels en cause;
   - Le niveau de capacité et la volonté de nuisance d'une personne ou entité malintentionnée d'accéder et/ou d'exploiter les Renseignements personnels concernés.

La RPRP détermine si la Personne concernée s'expose à un risque plausible de préjudice sérieux.

6.5 Notification de l'Incident de confidentialité

6.5.1 En présence d'un risque plausible de préjudice sérieux

La RPRP doit aviser avec diligence de la survenance de l'Incident de confidentialité les personnes et entités suivantes :

6.5.1.1 La Commission d'accès à l'information du Québec

Cet avis doit être fait au moyen du formulaire publié par la Commission et en suivant la procédure qui y est indiquée.

6.5.1.2 La Personne concernée

Cet avis se fait directement à la Personne concernée par tout moyen adéquat, notamment par courriel ou par lettre postale. Il doit contenir tous les éléments exigés par le Règlement.

Toutefois, afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou afin d'atténuer un tel préjudice, l'Organisation peut procéder par avis public. Dans ce cas, par la suite, l'Organisation doit tout de même adresser un avis directement à la Personne concernée.

Si l'Organisation n'a pas les coordonnées de la Personne concernée, si la transmission de l'avis est excessivement difficile pour l'Organisation ou si la notification directe à la Personne concernée lui cause un préjudice trop élevé, il est possible de recourir à un avis public.

La Personne concernée n'a pas à être avisée de l'Incident de confidentialité tant que cette notification serait susceptible d'entraver une enquête menée par un organisme chargé de prévenir, de détecter ou de réprimer une infraction aux lois.

6.5.1.3 Les autres autorités compétentes

Dans les cas qui le requièrent, par exemple si l'Incident de confidentialité implique des Personnes concernées résidant hors du Québec, il est possible que la RPRP doive en informer une autre autorité régulatrice (au Canada ou à l'étranger).

Par ailleurs, si l'Incident de confidentialité constitue un crime, l'Organisation en avise le service de police compétent.

6.5.2 En l'absence d'un risque plausible de préjudice sérieux

L'Organisation détermine s'il est pertinent d'informer la Personne concernée de l'Incident de confidentialité. Elle peut choisir de le faire pour des raisons de transparence ou de gestion des affaires. Ces raisons sont documentées dans le registre des Incidents de confidentialité.

Par ailleurs, si l'Incident de confidentialité constitue un crime, l'Organisation en avise le service de police compétent.

7. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Le registre des Incidents de confidentialité documente tous les Incidents de confidentialité survenus. Ce registre permet de bonifier les plans de résilience, d'orienter l'offre de formation et de sensibilisation à la protection des Renseignements personnels et d'améliorer en continu la gestion des Incidents de confidentialité. Il joue également un rôle essentiel lors d'une éventuelle inspection.

Le registre contient pour chaque Incident de confidentialité :

- Sa nature;
- Sa date de survenance;
- La date à laquelle il a été découvert;
- Le type de Renseignements personnels visés;
- Le nombre des Personnes concernées;
- Les éléments qui amènent la RPRP à conclure qu'il existe ou non un risque plausible qu'un préjudice sérieux soit causé aux Personnes concernées;
- Les mesures prises pour remédier aux conséquences négatives de l'Incident de confidentialité, pour les atténuer ou pour les contenir et celles pour éviter qu'un tel Incident ne se reproduise;
- Les dates et moyens d'une notification de l'Incident de confidentialité.

Les Renseignements personnels contenus au registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date à laquelle l'Organisation a pris connaissance de l'Incident de confidentialité.

8. LA RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La RPRP décide, en fonction de la gravité de l'Incident de confidentialité, d'aviser le Conseil ou le Comité. Elle peut aussi tenir un exercice de retour sur un Incident de confidentialité majeur, avec les différentes parties prenantes.

9. MISE À JOUR

De manière à suivre l'évolution du cadre normatif applicable à l'Organisation en matière de protection des Renseignements personnels, la présente procédure pourra être mise à jour au besoin.

10. ENTRÉE EN VIGUEUR

La présente procédure entre en vigueur lors de son adoption par le Conseil.