Centre de services scolaire du Lac-Témiscamingue
Québec

DIRECTIVE

SG-02

SECRÉTARIAT GÉNÉRAL

DIRECTIVE SUR LA GESTION DES INCIDENTS DE CONFIDENTIALITÉ

RÉVISIONS DU DOCUMENT

No révision	Date	Résumé des changements apportés
# 1 Document initial	2024-03-18	Par Myriam Ramos - Directive découlant des modifications apportées à *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*
# 2	2024-08-12	Ajout de l'annexe 2 et changement de numérotation dans les annexes.

ANNEXE 1 : Schéma processus d'incident

ANNEXE 2 : Actions immédiates lorsqu'un incident de confidentialité survient

ANNEXE 3 : Extraits du Règlement sur les incidents de confidentialité

TABLE DES MATIÈRES

1. Cadre juridique 3
2. But et objectifs de la directive 3
3. Champ d'application 3
4. Définitions 3
5. Processus lors d'un incident de confidentialité 4
5. Toute autre atteinte à la protection d'un tel renseignement 4
6. Comité sur l'accès à l'information et la protection des renseignements personnels 7
7. Information et diffusion 7
8. Entrée en vigueur 7

Annexe 1 – Schéma du processus d'incident 8
Annexe 2 – Actions immédiates en cas d'incident de confidentialité 9
Annexe 3 – Extraits du règlement sur les incidents de confidentialité 10

1. CADRE JURIDIQUE

La présente directive découle des modifications apportées à *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, ci-après « LAI »).

La présente directive doit être lue en concordance avec les différents processus, formulaires et questionnaires d'évaluation existant au Centre de services scolaire du Lac-Témiscamingue, notamment, la directive relative aux règles encadrant la gouvernance du Centre de service scolaire du Lac-Témiscamingue à l'égard des renseignements personnels.

2. BUT ET OBJECTIFS DE LA DIRECTIVE

Le but de la directive est d'assurer la mise en œuvre des actions du Centre de services scolaire pour une meilleure prise en charge des incidents de confidentialité.

Les objectifs de la directive sont les suivants :

- Déterminer les rôles et responsabilités des personnes visées par la présente directive;
- Informer les membres du personnel et autres personnes du Centre sur les incidents de confidentialité et les actions à prendre.

3. CHAMP D'APPLICATION

La présente directive s'applique à l'ensemble du personnel du Centre. Elle s'applique également aux membres du conseil d'administration, aux membres des conseils d'établissements et aux membres des différents comités du CSSLT.

Cette directive s'applique également aux incidents de confidentialité impliquant des renseignements personnels confiés par le Centre à des tiers dans le cadre d'un mandat ou d'un contrat de service.

4. DÉFINITIONS

Les termes utilisés dans la présente directive sont ceux de la LAI et des autres encadrements légaux applicables, sauf indication contraire.

Pour faciliter la compréhension de la présente directive, on entend par :

Le Centre	Centre de service scolaire du Lac-Témiscamingue
Comité sur l'accès	Le comité sur l'accès à l'information et la protection des renseignements personnels du Centre de services scolaire
Déclarant	Personne qui a connaissance d'un possible incident de confidentialité
Incident de confidentialité	Désigne tout évènement intentionnel ou non dont : **1.** L'accès non autorisé par la loi à un renseignement personnel; **2.** L'utilisation non autorisée par la loi d'un renseignement personnel; **3.** La communication non autorisée par la loi d'un renseignement personnel; **4.** La perte d'un renseignement personnel; **5.** Toute autre atteinte à la protection d'un tel renseignement.

Personne	Une personne visée par le champ d'application de la présente directive agissant au nom du Centre de services scolaire ou dans le cadre de ses fonctions
Personne concernée	Personne dont les renseignements personnels ont été compromis par l'incident de confidentialité
Renseignement personnel	Renseignements qui concernent une personne physique et permettent directement ou indirectement de l'identifier
RPRP	Personne désignée comme Responsable de la protection des renseignements personnels du Centre de services scolaire.
COMSI	Coordonnateur organisationnel des mesures de sécurité de l'information

5. PROCESSUS LORS D'UN INCIDENT DE CONFIDENTIALITÉ

Toute personne qui constate un évènement pouvant s'apparenter à un incident de confidentialité doit en informer son gestionnaire immédiat pour en faire un signalement et ainsi démarrer le processus de gestion des incidents. Un incident de confidentialité se produit lorsqu'un évènement peut être associé à l'une des **cinq** catégories suivantes :

Catégorie	Explication
1. L'accès non autorisé par la loi à un renseignement personnel	Un accès non autorisé peut être réalisé par un acteur externe ou un acteur interne dont la nécessité d'accès aux renseignements personnels ne peut être démontrée
2. L'utilisation non autorisée par la loi d'un renseignement personnel	L'utilisation non autorisée comprend les utilisations explicitement proscrites ainsi que les utilisations sans un consentement adéquat.
3. La communication non autorisée par la loi d'un renseignement personnel	La communication non autorisée peut être réalisée par un acteur externe via l'exfiltration de données ou un acteur interne en transmettant des renseignements personnels intentionnellement ou accidentellement à une personne non autorisée
4. La perte d'un renseignement personnel	La perte inclut les formes électroniques comme une clé USB et physiques comme les boîtes de documents.
5. Toute autre atteinte à la protection d'un tel renseignement	Tout autre évènement ne pouvant être clairement identifié à une des catégories précédentes, mais qui représentent un risque de préjudice pour la personne concernée.

En cas de doute, il est toujours préférable d'en faire le signalement.

5.1. Signalement d'un incident de confidentialité

5.1.1. La personne doit, dans le délai le plus court, informer la direction de son unité administrative (école, centre, service) de l'évènement dont il a été témoin.

5.1.2. Le Déclarant et la direction doivent, dès que possible, poser les gestes nécessaires qui diminueraient les risques qu'un préjudicie soit causé (rappel d'un courriel; téléphone, mettre en lieu sûr des documents, etc.)

5.1.3. Dans la mesure du possible, le Déclarant fournit les informations suivantes relativement à l'incident de confidentialité au COMSI via l'outil de billetterie prévu à cet effet :

5.1.3.1. Le contexte et les circonstances entourant l'évènement (Date, description des faits survenus, etc.);

5.1.3.2. La nature des renseignements personnels concernés (par exemple : noms, adresse, courriel, code permanent, etc.);

5.1.3.3. Le fait que ces renseignements étaient ou non protégés par un mot de passe ou un code d'accès, par exemple;

5.1.3.4. Le nombre de personnes concernées par les renseignements personnels;

5.1.3.5. L'identité et le nombre de personnes ou l'organisme qui ont reçu les renseignements personnels, le cas échéant;

5.1.3.6. Les mesures immédiates prises, le cas échéant;

5.1.3.7. Toute autre information pertinente.

5.2. Analyse de la situation et confinement de l'incident

5.2.1. Suite à la prise en charge du billet, le COMSI procède à une analyse préliminaire de la situation.

5.2.2. Au besoin, il obtient des informations supplémentaires et pose des actions de confinement supplémentaire.

5.2.3. Il statue sur la présence de renseignements personnels et transmet le dossier au Responsable de la protection des renseignements personnels. En cas de doute, le COMSI peut référer au Responsable. Dans l'éventualité d'un incident non avéré, le billet est fermé et transformé en incident de cybersécurité.

5.2.4. Le Responsable de la protection des renseignements personnels analyse l'incident et détermine s'il s'agit bien d'un incident de confidentialité.

5.2.5. S'il détermine qu'il ne s'agit pas d'un incident de confidentialité, mais qu'il juge qu'une intervention est tout de même nécessaire auprès des personnes impliquées dans l'évènement, il communique avec la direction afin qu'elle pose, le cas échéant, les gestes appropriés.

5.3. Prise en charge d'un incident de confidentialité

5.3.1. Le Responsable de la protection des renseignements personnels s'assure que les gestes ou les mesures, qui sont susceptibles de diminuer les risques qu'un préjudicie soit causé aux personnes dont les renseignements personnels sont concernés par l'incident de confidentialité, soient mis en œuvre en tenant compte de ceux qui ont été posés par le Déclarant ou le COMSI.

5.4. Évaluation du risque de préjudice

5.4.1. Le Responsable de la protection des renseignements personnels évalue le risque de préjudice sérieux de l'incident de confidentialité en considérant notamment la sensibilité du renseignement, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. À cette fin, il ajoute au dossier la grille d'évaluation du risque de préjudice complété.

5.4.2. Si l'incident de confidentialité présente un risque préjudice sérieux, le Responsable de la protection des renseignements personnels doit :

5.4.2.1. Aviser toute personne dont les renseignements personnels sont concernés par l'incident de confidentialité de la manière et en fournissant les informations requises par le règlement applicable (voir annexe);

5.4.2.2. Aucun avis aux personnes visées n'est nécessaire si un tel avis avait pour effet d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois;

5.4.2.3. Aviser toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux (ministère, police, etc.) en ne communiquant que les renseignements personnels nécessaires à cette fin et inscrire cette communication au registre des communications en vertu de la LAI.

5.5. Déclaration à commission d'accès à l'information

5.5.1. Si l'incident de confidentialité présente un risque de préjudice sérieux, le Responsable de la protection des renseignements personnels doit :

5.5.1.1. Aviser la commission d'accès à l'information avec diligence, de la manière et en fournissant les informations requises par le règlement applicable (voir annexe);

5.6. Déclaration au registre des incidents de confidentialité

5.6.1. Le Responsable de la protection des renseignements personnels inscrit l'incident avéré au registre des incidents de confidentialité dans tous les cas.

5.7. Bilan et mesures à prendre pour éviter qu'un incident de confidentialité de même nature se reproduise

5.7.1. Une fois les mesures immédiates accomplies, le Responsable de la protection des renseignements personnels détermine si d'autres mesures devraient être appliquées pour éviter que d'autres incidents de même nature ne se reproduisent. Au besoin, il consulte les autres directions. À titre d'exemples voici des mesures pouvant être proposées :

5.7.1.1. La modification des accès informatiques;

5.7.1.2. La suppression de renseignements personnels;

5.7.1.3. La mise en place de formation ou autres mesures de sensibilisation;

5.7.1.4. La révision de processus internes (logiciels, destruction, etc.).

6. COMITÉ SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

6.1. Le responsable de la protection des renseignements personnels peut en tout temps consulter le comité sur l'accès à l'information du centre dans l'analyse et le traitement d'une situation pouvant être un incident de confidentialité.

6.2. Le responsable de la protection des renseignements fait rapport annuellement au comité sur l'accès à l'information des incidents de confidentialité survenus et des mesures mises en place.

6.3. Le responsable de la protection des renseignements personnels transmet au comité sur l'accès à l'information les recommandations de la commission d'accès à l'information, le cas échéant.

7. INFORMATION ET DIFFUSION

7.1. Le responsable s'assure de la diffusion de la présente directive auprès des différentes unités administratives.

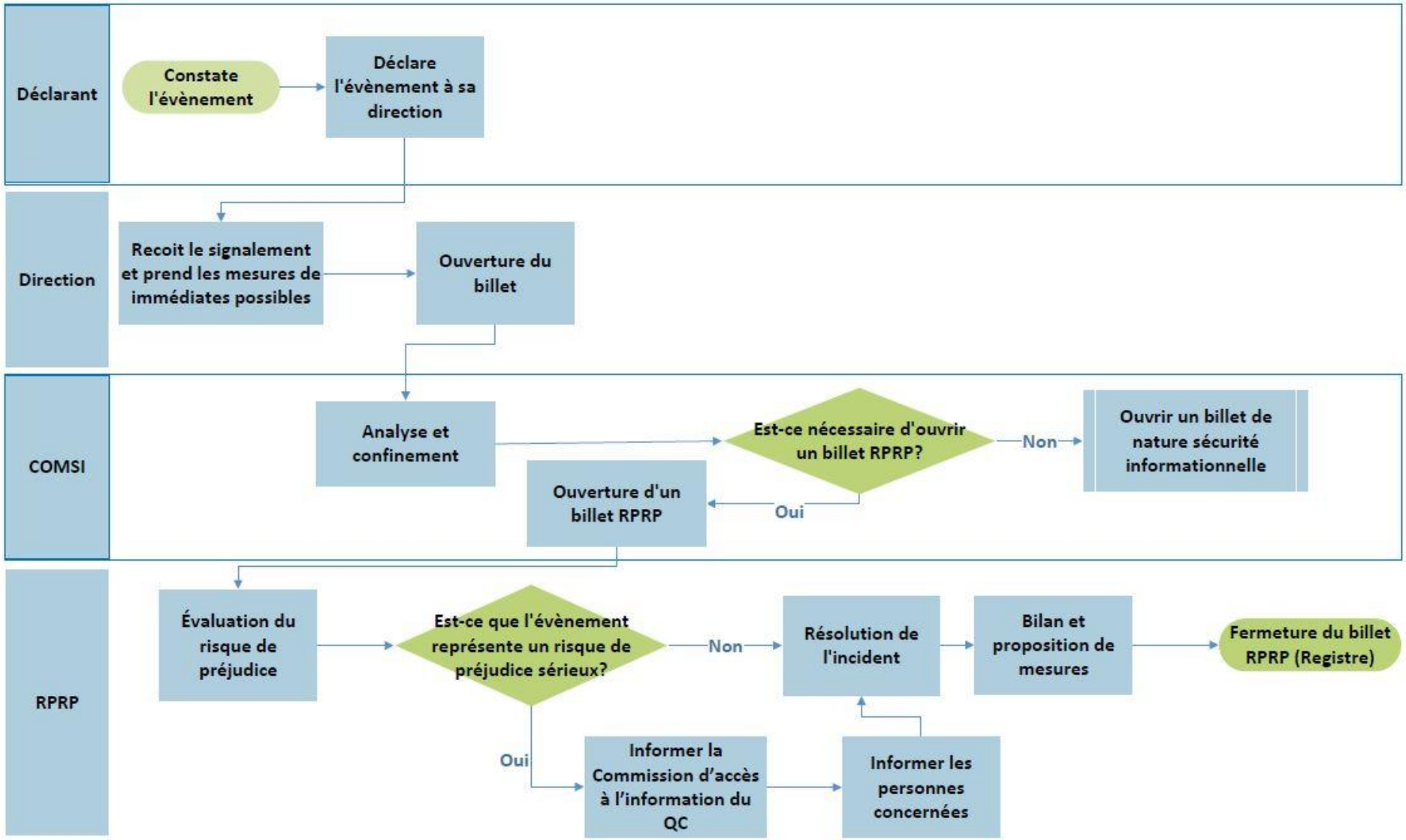
7.2. Au besoin, en collaboration avec les directions, le responsable s'assure qu'une formation adéquate soit disponible et offerte aux membres du personnel.

8. ENTRÉE EN VIGUEUR

La présente directive entre en vigueur le 18 mars 2024.

MR/sm

ANNEXE 1 – Schéma du processus d'incident



ANNEXE 2 – Actions immédiates en cas d'incident de confidentialité

Lors d'un incident de confidentialité, il est demandé au déclarant de prendre toutes mesures raisonnables, et ce dans la mesure de ses moyens et connaissances afin de réduire le plus rapidement possible le risque de préjudice pour les personnes concernées. À titre d'exemple, voici une liste de mesures qui pourraient être prises rapidement lors d'un évènement.

Évènement de nature physique

- Documents physiques non sécurisés :
  - Verrouiller le local;
  - Verrouiller le classeur;
  - Déplacer temporairement les documents dans un local pouvant être verrouillé;
  - Ouvrir une demande de service pour réparer les serrures et cadenas.

- Transmission d'un document au mauvais destinataire :
  - Contacter le mauvais destinataire et demander de ne pas ouvrir le document;
  - Physiquement, récupérer le document lorsque possible;
  - Obtenir et conserver les reçus de livraison.

Évènement de nature électronique

- Transmission d'un document au mauvais destinataire :
  - Si le document a été transmis à l'interne, rappeler le courriel;
  - Contacter le mauvais destinataire et demander de ne pas ouvrir le document;
  - Demander au destinataire la destruction du courriel.

- Partage des fichiers non autorisés :
  - Retirer tous les membres du partage qui sont non essentiels;
  - Retirer les documents des partages communs.

Autres évènements - virus- formulaire d'hameçonnage

  - Si un mot de passe a été transmis, modifier le mot de passe de la personne concernée;
  - Ne pas transmettre les courriels potentiellement malicieux à moins d'avis contraire et signaler les courriels malicieux selon la procédure;
  - Déconnecter l'appareil potentiellement compromis du réseau filaire/Wifi.

ANNEXE 3 – Extraits du règlement sur les incidents de confidentialité

Extraits du Règlement sur les incidents de confidentialité, publié dans le Décret 1761-2022 du 30 novembre 2022, dans la Gazette officielle du Québec du 14 décembre 2022, 154e année, no 50, p. 6819.

AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

3. L'avis à la Commission d'accès à l'information qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, donné en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) ou du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1), est fait par écrit et doit contenir les renseignements suivants:

1° le nom de l'organisation ayant fait l'objet de l'incident de confidentialité et, le cas échéant, le numéro d'entreprise du Québec qui lui est attribué en vertu de la Loi sur la publicité légale des entreprises (chapitre P-44.1);

2° le nom et les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident;

3° une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

4° une brève description des circonstances de l'incident et, si elle est connue, sa cause;

5° la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

6° la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;

7° le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;

8° une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

9° les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ou du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;

10° les mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que la date ou la période où les mesures ont été prises ou le délai d'exécution envisagé;

11° le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

4. L'organisation doit transmettre à la Commission d'accès à l'information tout renseignement énoncé à l'article 3 dont elle prend connaissance après lui avoir transmis l'avis qui y est visé. L'information complémentaire doit alors être transmise avec diligence à compter de cette connaissance.

CONTENU DE L'AVIS À LA PERSONNE DONT UN RENSEIGNEMENT PERSONNEL EST CONCERNÉ

1. L'avis à la personne dont un renseignement personnel est concerné par un incident qui présente un risque qu'un préjudice sérieux soit causé, donné en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) ou du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1), doit contenir les renseignements suivants:

1° une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

2° une brève description des circonstances de l'incident;

3° la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

4° une brève description des mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

5° les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;

6° les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

CIRCONSTANCES SELON LESQUELLES L'AVIS À LA PERSONNE EST TRANSMIS PAR AVIS PUBLIC

6. L'avis visé à l'article 5 est transmis à la personne concernée par l'incident de confidentialité.

Malgré le premier alinéa, l'avis visé à l'article 5 est donné au moyen d'un avis public dans l'une ou l'autre des circonstances suivantes:

1° lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;

2° lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisation;

3° lorsque l'organisation n'a pas les coordonnées de la personne concernée.

Par ailleurs, afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou afin d'atténuer un tel préjudice, l'avis visé à l'article 5 peut également être donné au moyen d'un avis public. Dans ce cas, l'organisation demeure toutefois tenue de transmettre, avec diligence, un avis à la personne concernée, à moins que l'une des circonstances énoncées au deuxième alinéa ne s'applique à sa situation.

En application du présent article, un avis public peut être fait par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée.