



L'Observatoire de l'ACA

par et pour l'action
communautaire autonome

Politique de confidentialité et de protection des données personnelles

Portée : toutes les personnes qui fournissent, collectent ou conservent des données personnelles dans le cadre des activités et de la vie associative de l'Observatoire de l'ACA

Numéro : RH-2026-1

Date d'effet : 26 mars 2026

À l'Observatoire de l'action communautaire autonome, la vie associative est au fondement de la recherche pour coproduire des savoirs et mobiliser des connaissances. La confiance est au cœur de nos relations avec toutes les personnes qui contribuent de près ou de loin au fonctionnement de l'organisme, à ses activités et à ses publications.

Nous accordons une grande importance au respect de la vie privée et à l'intégrité de toutes et de tous. Cette politique de confidentialité reflète notre engagement à traiter vos renseignements personnels avec le plus grand soin et à les utiliser uniquement comme prévu lors de leur collecte. En règle générale, les renseignements confidentiels sont disponibles seulement aux personnes qui doivent y avoir accès dans l'exercice de leurs fonctions au sein de l'Observatoire de l'ACA.

Dans un contexte où les renseignements personnels sont de plus en plus accessibles et parfois traités comme une marchandise, nous souhaitons que cette politique soit intégrante. Elle vise à soutenir des pratiques évolutives, permettant à chaque personne de s'éduquer, de se protéger et d'exercer ses droits.

Cette politique s'inspire des travaux effectués par la COCQ-SIDA.



Table des matières

I — Politique de confidentialité relative aux renseignements personnels	3
1. Définition	3
2. Obligation de confidentialité	4
3. Photographie ou enregistrement	4
4. Témoins de connexion et technologies similaires	5
II — Encadrement applicable à la collecte, à la conservation et à la destruction des renseignements personnels	5
5. Collecte des renseignements confidentiels	5
6. Gestion des renseignements confidentiels	5
7. Conservation des renseignements confidentiels	6
8. Destruction ou anonymisation des renseignements personnels	6
9. Divulgence volontaire d'un renseignement à une tierce personne	7
10. Communication de renseignements confidentiels à la personne concernée	7
11. Manquement à l'obligation de confidentialité	8
12. En cas d'incident de confidentialité	8
13. Recours	8
14. Mise à jour de la politique	9
Annexe A — Incident de confidentialité : Plan de réponse	10
Annexe B — Incident de confidentialité : Questionnaire d'évaluation du risque sérieux de préjudice grave	12
Annexe C — Incident de confidentialité : Contenu de la communication aux personnes concernées	14
Annexe D — Rôles et responsabilités de la personne responsable des données personnelles	15

I — Politique de confidentialité relative aux renseignements personnels

1. Définition

1.1. Corps collaboratif

Le corps collaboratif désigne les individus qui contribuent au fonctionnement de l'observatoire de l'ACA, rémunérés ou non, incluant la direction, les administratrices et administrateurs, les bénévoles et les stagiaires.

1.2. Événement

Un événement comprend tout événement ou activité que l'Observatoire de l'ACA mène, gère ou organise, incluant les projets de recherche.

1.3. Formulaire de signalement

Le formulaire de signalement est le formulaire qui sert au corps collaboratif pour informer la personne responsable des renseignements personnels lorsqu'un incident de confidentialité est constaté.

1.4. Incident de confidentialité

Un incident de confidentialité est un accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que la perte d'un renseignement personnel ou toute autre forme d'atteinte à sa protection.

1.5. Participant-e

Un-e participant-e est un individu qui fournit des renseignements confidentiels à l'Observatoire de l'ACA en lien avec son adhésion à l'organisme, à sa participation à un événement, **une activité de recherche** ou à la création d'une publication.

1.6. Personne responsable des renseignements personnels

La personne responsable des renseignements personnels est l'individu désigné pour assurer la protection des données personnelles détenues par l'Observatoire de l'ACA et pour veiller à l'application de la présente politique.

1.7. Publication

Une publication est une production de l'Observatoire de l'ACA, ou à laquelle il contribue, quelle que soit sa forme : écrit, visuel, audio, vidéo ou autre.

1.8. Registre des incidents de confidentialité

Le registre des incidents de confidentialité consigne l'ensemble des renseignements sur les incidents de confidentialités déclarés. Il comprend les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises

en réaction à l'incident. Les dates pertinentes y figurent aussi : date de l'incident, de sa détection, de la transmission des avis, etc.

1.9. Risque sérieux de préjudices

Il y a un risque sérieux de préjudice lorsque la divulgation ou la perte de renseignements confidentiels pourrait entraîner des conséquences importantes pour l'individu concerné. Le risque dépend de la sensibilité des renseignements concernés, des conséquences possibles de leur utilisation et de la probabilité qu'ils soient utilisés à des fins préjudiciables.

1.10. Renseignement confidentiel

Un renseignement confidentiel est une information personnelle transmise à l'Observatoire de l'ACA de quelque manière que ce soit (verbale, écrite, audio, vidéo, informatisée ou autre) qui peut être utilisée pour identifier un·e participant·e ou un·e membre du corps collaboratif. Cela comprend, entre autres, son nom, son numéro de téléphone, son adresse, son courriel, le fait qu'elle ait été ou soit un·e participant·e ou un·e participant·e potentiel·le, son genre, son orientation sexuelle et toute information concernant sa santé.

- Les renseignements professionnels ou nécessaires à la représentation de l'Observatoire de l'ACA ne sont pas des renseignements confidentiels.
- Les renseignements qui ne permettent pas d'identifier un individu dans le cadre d'un témoignage ne sont pas des renseignements confidentiels.
- Les données statistiques ne sont pas des renseignements confidentiels, puisqu'elles ne permettent pas d'identifier un individu.
- Les photographies ou enregistrements qui ne permettent pas d'identifier un individu ne constituent pas un renseignement confidentiel.

2. Obligation de confidentialité

- 2.1. Avant d'exercer ses fonctions ou d'exécuter son mandat à l'Observatoire de l'ACA, chaque membre du corps collaboratif est tenu de signer un engagement comprenant une entente de confidentialité.
- 2.2. L'obligation de confidentialité s'applique tout au long de la relation avec l'Observatoire de l'ACA et perdure au-delà de la fin de la relation.

3. Photographie ou enregistrement

- 3.1. Tout individu a le choix d'être photographié ou non, ou d'être enregistré (audio/vidéo) ou non.
- 3.2. Une photographie ou un enregistrement qui permet d'identifier un·e membre du corps collaboratif n'est pas un renseignement confidentiel.

4. Témoins de connexion et technologies similaires

- 4.1. L'Observatoire de l'ACA peut utiliser des témoins de connexion (« cookies »), des balises internet, des pixels invisibles, des fichiers journaux ou d'autres technologies pour collecter certains renseignements confidentiels lors de la visite de son site web.
- 4.2. Le site web de l'Observatoire de l'ACA peut contenir des liens ou des renvois vers des sites tiers. La présente politique cesse de s'appliquer au moment de quitter le site web de l'Observatoire de l'ACA, qui n'est pas responsable de la collecte ou du traitement de renseignements personnels par ces sites tiers ou sources externes.

II — Encadrement applicable à la collecte, à la conservation et à la destruction des renseignements personnels

5. Collecte des renseignements confidentiels

- 5.1. L'Observatoire de l'ACA peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels sur les membres du corps collaboratif. La constitution de tels dossiers sert à :
 - maintenir les coordonnées à jour ;
 - documenter des situations de travail ou de bénévolat ;
 - réaliser des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.).
- 5.2. L'Observatoire de l'ACA peut constituer un ou des dossiers contenant des renseignements confidentiels concernant les participant·e·s. La constitution de tels dossiers sert aux évènements et aux publications.
- 5.3. L'Observatoire de l'ACA peut seulement recueillir les renseignements confidentiels dont il a besoin pour son administration, ses évènements et ses publications.
- 5.4. Les renseignements confidentiels peuvent seulement être recueillis auprès de la personne concernée, à moins que celle-ci consente à ce que la cueillette soit faite auprès d'une autre personne ou que la loi l'autorise.

6. Gestion des renseignements confidentiels

- 6.1. La personne responsable des renseignements personnels est l'individu qui exerce la plus haute autorité dans l'organisme. Si l'Observatoire de l'ACA ne compte aucune employé·e, cette fonction revient à la présidence du conseil d'administration. Cette fonction peut être déléguée par écrit, en tout ou en partie. La personne responsable

doit être clairement identifiée sur le site web de l'Observatoire de l'ACA avec la mention « responsable de la protection des renseignements personnels ». Le moyen de la joindre doit être indiqué.

- 6.2. La direction de l'Observatoire de l'ACA est autorisée à accéder à tout renseignement confidentiel détenu par l'organisme. Les autres membres du corps collaboratif sont autorisé·e·s à accéder aux renseignements confidentiels lorsque c'est utile à leurs tâches ou fonctions.

7. Conservation des renseignements confidentiels

- 7.1. Les personnes qui ont accès aux données confidentielles ont des obligations :
 - S'assurer que les renseignements confidentiels sont gardés à l'abri de tout dommage physique et tout accès non autorisé ;
 - S'assurer que tous les documents électroniques comportant des renseignements confidentiels, incluant les copies de sauvegarde, sont chiffrés et protégés par mot de passe ;
 - Modifier les mots de passe qui protègent ces données au moins deux fois par année, et chaque fois qu'une personne connaissant le mot de passe n'est plus autorisée à accéder à ces renseignements confidentiels ;
 - En dehors des heures ou périodes de travail, garder les renseignements confidentiels en format papier à un endroit qui n'est pas accessible aux personnes non autorisées à y accéder.
- 7.2. Lorsqu'un·e membre du corps collaboratif est également un·e participant·e, les renseignements confidentiels relatifs à chacun de ces statuts sont conservés dans des dossiers distincts.
- 7.3. Les dossiers comportant des données confidentielles sont la propriété de l'Observatoire de l'ACA, qui en assure la conservation et la protection.
- 7.4. L'Observatoire de l'ACA accorde la plus grande importance à la sécurité des renseignements confidentiels et s'engage à les utiliser uniquement pour les fins pour lesquelles ils sont recueillis. Toutefois, aucune transmission de données par internet n'est entièrement sécurisée. Les participant·e·s qui transmettent des renseignements confidentiels par voie électronique le font en connaissance de ces limites.

8. Destruction ou anonymisation des renseignements personnels

- 8.1. Les dossiers concernant le corps collaboratif sont conservés par l'Observatoire de l'ACA conformément aux obligations légales applicables.
- 8.2. Les autres renseignements confidentiels sont conservés le temps nécessaire à leur usage prévu lors de leur collecte, sauf si la personne concernée a consenti à une

conservation plus longue.

- 8.3. Les renseignements confidentiels doivent être supprimés ou anonymisés dès qu'ils n'ont plus d'utilité pour l'Observatoire de l'ACA.
- 8.4. L'anonymisation doit garantir que les renseignements conservés ne peuvent pas permettre d'identifier la personne concernée.
- 8.5. Les renseignements confidentiels qui n'ont plus lieu d'être conservés sont détruits de manière à empêcher toute reconstitution des données.

9. Divulgence volontaire d'un renseignement à une tierce personne

- 9.1. Sauf disposition légale contraire et sous réserve des autres articles de la présente politique, l'Observatoire de l'ACA ne peut divulguer des renseignements confidentiels à une tierce personne que si l'individu concerné y a consenti par écrit, de manière claire, libre et éclairée. Ce consentement ne peut être donné que pour une fin déterminée et pour la durée nécessaire à la réalisation de cette fin.
- 9.2. Les renseignements confidentiels peuvent être divulgués sans le consentement de l'individu concerné lorsque sa vie, sa santé ou sa sécurité est gravement menacée. Dans un tel cas, la divulgation doit être limitée aux renseignements nécessaires et effectuée de la manière la moins préjudiciable possible.
- 9.3. Comme permis par la loi, l'Observatoire de l'ACA peut divulguer les renseignements confidentiels nécessaires à sa défense ou à celle de son corps collaboratif contre toute réclamation ou poursuite intentée contre l'organisme ou son corps collaboratif, y compris celles émanant d'un assureur.
- 9.4. L'Observatoire de l'ACA s'engage à ne pas vendre, louer ou autrement aliéner les renseignements confidentiels à une tierce partie.

10. Communication de renseignements confidentiels à la personne concernée

- 10.1. Sous réserve de l'article 10.2, tout individu a le droit de connaître les renseignements confidentiels que l'Observatoire de l'ACA a reçus, recueillis et conservés à son sujet, d'y avoir accès et de demander, au besoin, que des rectifications y soient apportées.
- 10.2. L'Observatoire de l'ACA doit restreindre l'accès aux renseignements personnels lorsque la loi l'exige ou lorsque leur divulgation risque de révéler des renseignements confidentiels concernant une tierce personne.
- 10.3. Les demandes d'accès ou de rectification aux renseignements confidentiels sont

traitées dans un délai maximal de 30 jours, conformément à la loi.

11. Manquement à l'obligation de confidentialité

11.1. Un·e membre du corps collaboratif manque à son obligation de confidentialité lorsqu'il ou elle :

- communique des renseignements confidentiels à des personnes non autorisées à y avoir accès ;
- discute de renseignements confidentiels alors que des personnes non autorisées à y avoir accès sont susceptibles de les entendre ;
- laisse des renseignements confidentiels sur papier ou support informatique à la vue de personnes non autorisées à y avoir accès ;
- ne respecte pas les dispositions de la présente politique.

11.2. Un·e membre du corps collaboratif qui manque à son obligation de confidentialité fait face à des mesures disciplinaires appropriées qui peuvent aller jusqu'au congédiement ou à la résiliation de toute relation de collaboration avec l'Observatoire de l'ACA. Des mesures correctives peuvent également être mises en place afin de prévenir la répétition d'un tel manquement.

12. En cas d'incident de confidentialité

12.1. La personne qui constate un incident de confidentialité doit remplir le plus rapidement possible le formulaire de signalement et, le cas échéant, le transmettre à la personne responsable des renseignements personnels.

12.2. Dès que la personne responsable prend connaissance d'un incident de confidentialité, elle doit mettre en œuvre le plan de réponse (annexe A). Ce plan vise à analyser et réduire le risque de préjudice, ainsi qu'à mettre en place des mesures correctives.

12.3. En cas de risque sérieux de préjudice, les personnes concernées et la Commission d'accès à l'information en sont informées.

12.4. La personne responsable détermine les mesures raisonnables pour réduire le risque de préjudice et pour prévenir de nouveaux incidents.

12.5. La personne responsable met à jour le registre des incidents de confidentialité. Les informations suivantes doivent y être conservées durant 5 ans.

13. Recours

13.1. Si des données personnelles ont été utilisées ou transmises d'une façon contraire à la présente politique, l'individu lésé peut déposer une plainte auprès de la personne responsable des renseignements personnels ou, dans le cas d'une plainte concernant la direction, auprès du conseil d'administration de l'Observatoire de l'ACA.

- 13.2. Conformément à la loi, tout individu à qui l'accès ou la rectification de renseignements confidentiels le concernant a été refusé peut déposer une plainte auprès de la Commission d'accès à l'information dans les 30 jours suivant le refus ou l'expiration du délai pour répondre à sa demande.

14. Mise à jour de la politique

- 14.1. L'Observatoire de l'ACA se réserve le droit de mettre à jour la présente politique en tout temps. Si les modifications apportées touchent les droits du corps collaboratif ou des participant·e·s, les personnes concernées en seront informées par le moyen jugé le plus approprié.
- 14.2. Les questions ou les commentaires sur la présente politique doivent être adressés à la personne responsable des renseignements personnels.

Annexe A — Incident de confidentialité : Plan de réponse

Ce plan de réponse doit être mis en œuvre par la personne responsable des renseignements personnels dès qu'elle a connaissance d'un incident de confidentialité.

(Article 12.2)

1. Mettre en place des mesures raisonnables pour réduire le risque de préjudice.
(Article 12.2)
2. Procéder à une première analyse du risque de préjudice ([annexe B](#)). (Article 12.2)
 - a) Si l'incident ne présente pas un risque sérieux de préjudice, il est rapporté au conseil d'administration lors de la réunion régulière qui suit. Le conseil d'administration peut décider de faire une nouvelle analyse.
 - b) Si l'incident présente un risque sérieux de préjudice ou si la personne responsable souhaite l'avis du conseil d'administration, les administrateurs et administratrices disponibles sont consulté·e·s le plus rapidement possible.

Si le risque de préjudice est sérieux est confirmé par le conseil d'administration :

3. Prévenir par écrit et sans délai toutes les personnes dont les renseignements confidentiels ont été exposés en incluant les informations requises ([annexe C](#)).
(Article 12.3)
4. Prévenir sans délai la [Commission d'accès à l'information](#) en utilisant le formulaire [Avis à la commission d'accès à l'information concernant un incident de confidentialité impliquant des renseignements personnels et présentant un risque de préjudice sérieux](#) (coordonnées incluses dans le formulaire). (Article 12.3)

Quelle que soit la conclusion de l'analyse du risque de préjudice :

5. Déterminer les mesures raisonnables pour prévenir de nouveaux incidents.
(Article 12.7)
6. Mettre à jour le registre des incidents de confidentialité (dossier 2400). (Article 12.4)
 - a) La description des renseignements confidentiels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir cette description ;
 - b) Une brève description des circonstances de l'incident ;
 - c) La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;

- d) La date à laquelle la personne responsable des renseignements personnels a eu connaissance de l'incident ;
- e) Le nombre d'individus concernés par l'incident (ou une approximation si cette information n'est pas connue) ;
- f) Le résultat de l'analyse de risque de préjudice ;
- g) La date et le moyen utilisé pour informer les personnes concernées ;
- h) La date de transmission du formulaire à la Commission d'accès à l'information ;
- i) Les mesures prises pour réduire le risque de préjudice ;
- j) Les mesures prises pour éviter qu'un incident de confidentialité se reproduise.

Annexe B — Incident de confidentialité : Questionnaire d'évaluation du risque sérieux de préjudice grave

Évaluation si l'incident présente un risque de préjudice sérieux

Pour tout incident de confidentialité, l'Observatoire de l'ACA doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, il doit considérer :

- Quelle est la sensibilité des renseignements concernés ?
- Quelles sont les conséquences appréhendées de leur utilisation ?
- Quelle est la probabilité qu'ils soient utilisés à des fins préjudiciables ?

Renseignements sensibles

- Les documents financiers
- Les dossiers médicaux
- Les renseignements personnels qui sont communiqués de manière courante ne sont généralement pas considérés comme sensibles (nom, adresse postale, adresse courriel)

Préjudice grave

Les exemples suivants sont considérés comme des préjudices graves :

- Humiliation
- Dommage à la réputation ou aux relations
- Perte de possibilité d'emploi ou d'occasion d'affaires ou d'activités professionnelles
- Perte financière
- Vol d'identité
- Effet négatif sur le dossier de crédit
- Dommage aux biens ou perte des biens

Évaluation de la probabilité d'un mauvais usage

Pour déterminer la probabilité d'un mauvais usage, il faut se poser les questions suivantes :

- Qu'est-il arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'exposition de ces renseignements confidentiels ?
- Qui a eu accès aux renseignements personnels ou aurait pu y avoir accès ?
- Combien de temps les renseignements personnels ont-ils été exposés ?
- A-t-on constaté un mauvais usage de ces renseignements ?
- L'intention malveillante a-t-elle été démontrée (vol, piratage) ?
- Les renseignements ont-ils été exposés à des personnes ou à des entités susceptibles d'en faire un usage préjudiciable ou de porter atteinte à la réputation des personnes concernées ?

Si l'analyse fait ressortir un risque de préjudice sérieux, l'organisation doit aviser la Commission et les personnes concernées de l'incident. Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques qu'un incident de même nature se produise à nouveau.

Note : le Commissariat à la protection de la vie privée du Canada a produit une vidéo d'aide à l'évaluation : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-lesentreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/atteinte_101/atteinte_risques/

Annexe C — Incident de confidentialité : Contenu de la communication aux personnes concernées

Quand

L'Observatoire de l'ACA doit aviser directement, par écrit et dès que possible, toutes les personnes qui sont à risque de subir un préjudice sérieux à cause de l'exposition de leurs renseignements personnels (article 12.3). Toutefois, le [Règlement sur les incidents de confidentialité](#) prévoit des situations où la communication peut se faire exceptionnellement par le biais d'un avis public si le fait de transmettre l'avis directement aux personnes concernées est susceptible de représenter une difficulté excessive ou d'augmenter le préjudice causé.

Contenu

L'avis écrit aux personnes concernées doit contenir les éléments suivants :

- Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description.
- Une brève description des circonstances de l'incident.
- La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue).
- Une brève description des mesures que l'Observatoire de l'ACA a prises ou envisage de prendre suivant l'incident dans le but de réduire les risques de préjudice.
- Les mesures que l'Observatoire de l'ACA suggère à la personne concernée de prendre dans le but de réduire les risques de préjudice.
- Les coordonnées de la personne auprès de laquelle la personne concernée peut obtenir de plus amples renseignements à propos de l'incident.

Annexe D — Rôles et responsabilités de la personne responsable des données personnelles

La personne responsable des renseignements personnels est l'individu désigné pour assurer la protection des données personnelles détenues par l'Observatoire de l'ACA et pour veiller à l'application de la présente politique. (Article 1.6)

La personne responsable des renseignements personnels est l'individu qui exerce la plus haute autorité dans l'organisme. Si l'Observatoire de l'ACA ne compte aucune employé-e, cette fonction revient à la présidence du conseil d'administration. Cette fonction peut être déléguée par écrit, en tout ou en partie. (Article 6.1)

Prévenir des risques d'incidents de confidentialité

7. Prendre connaissance de l'intégralité de la politique de confidentialité et de protection des données personnelles de l'Observatoire de l'ACA.
8. Informer toute nouvelle personne qui intègre le corps collaboratif de l'Observatoire de l'ACA sur ses responsabilités concernant la confidentialité des données personnelles et leur faire signer le formulaire d'engagement. (Article 2.1)
9. Conserver les données confidentielles dans des lieux physiques ou virtuels sécurisés. (Article 7.1)
10. Modifier les mots de passe qui protègent ces données : (Article 7.1)
 - a) Au moins deux fois par année ;
 - b) Dès qu'une personne qui connaissait le mot de passe n'a plus le droit d'y accéder.
11. Supprimer ou anonymiser les données confidentielles dès qu'ils n'ont plus d'utilité pour l'Observatoire de l'ACA. (Article 8.3)
12. Faire approuver par le conseil d'administration et appliquer les mesures disciplinaires contre un-e membre du corps collaboratif qui a manqué à son obligation de confidentialité. (Article 11.2)
13. Mettre en place des mesures correctives à la suite d'un incident de confidentialité, si applicable. (Article 12.4)
14. Répondre aux questions concernant la présente politique et recevoir les commentaires. (Article 14.2)
15. Mettre à jour la présente politique au besoin. (Article 14.1).

Gérer les données confidentielles

16. Ne donner l'accès aux données confidentielles qu'aux membres du corps collaboratif qui en ont besoin dans le cadre de leurs fonctions au sein de l'Observatoire de l'ACA. (Article 6.2)
17. Répondre aux demandes d'accès aux informations personnelles par les personnes concernées dans un délai de 30 jours. (Articles 10.1 et 10.3)
18. Répondre aux demandes de modification des informations personnelles par les personnes concernées dans un délai de 30 jours. (Articles 10.1 et 10.3)

Servir de pivot en cas d'incident de confidentialité

19. Recevoir les plaintes des personnes lésées par l'utilisation ou la transmission de leurs données personnelles, sauf si la plainte concerne la direction. (Article 13.1)
20. Recevoir les formulaires de signalement interne des incidents de confidentialité. (Article 12.1)
21. Mettre en œuvre le plan de réponse ([annexe A](#)) dès qu'un incident de confidentialité est signalé.

Tenir à jour le registre des incidents de confidentialité

22. Inscrire dans le registre tous les incidents de confidentialité, incluant (Articles 12.2 et 12.5)
 - a) les conclusions de l'analyse
 - b) les moyens pris pour éviter les préjudices sérieux
 - c) les mesures correctives
23. Supprimer du registre toutes informations relatives aux incidents de plus de 5 ans. (Article 12.2)
24. Sur demande de la Commission d'accès à l'information, lui transmettre une copie du registre.