Plan de gestion des incidents de confidentialité

FONDATION POUR LA BIODIVERSITÉ ET LA FAUNE DU QUÉBEC

Date : 28 mars 2024
Mise à jour :

Plan de gestion des incidents de confidentialité au sein de la Fondation pour la biodiversité et la faune du Québec

1. Objectif et cadre juridique

1.1. Le présent plan d'intervention a pour objectif d'identifier les intervenants, les étapes, les démarches et les actions requises en vue de s'assurer que les incidents impliquant des renseignements personnels détenus par la Fondation pour la biodiversité et la faune du Québec (ci-après : l'« **Organisme** ») soient traités de manière coordonnée, efficiente et rapide, afin d'atténuer les risques susceptibles d'en découler et d'apporter les correctifs nécessaires.

1.2. Il vise tous les renseignements personnels détenus par l'Organisme dans le cadre de ses activités au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1] ainsi que des autres lois et règlements applicables en matière de protection des renseignements personnels et celles applicables au domaine d'activités de l'Organisme (collectivement désignés, la « **Loi** »), notamment ceux relatifs à l'identité, à la santé, à la situation sociale ou familiale, à l'emploi, aux renseignements scolaires ou à ceux de nature financière, à la formation, au travail ou à l'éducation des individus concernés (ci-après : un « **Renseignement personnel** »).

2. Incident de confidentialité

2.1. Constitue un incident de confidentialité :

2.1.1. L'accès non autorisé par la Loi à un Renseignement personnel;
2.1.2. L'utilisation non autorisée par la Loi à un Renseignement personnel;
2.1.3. La communication non autorisée par la Loi à un Renseignement personnel;
2.1.4. La perte d'un Renseignement personnel ou toute autre atteinte à la protection d'un Renseignement personnel.

2.2. Un incident de confidentialité peut résulter d'une atteinte dont la source est à l'interne (c'est-à-dire, provenant d'un employé de l'Organisme) ou à l'externe (c'est-à-dire, provenant d'une entité ou personne distincte de l'Organisme).

2.3. Advenant un incident de confidentialité ou en cas de doute sur la survenance d'un tel incident, l'Organisme respecte le présent Plan de gestion des incidents de confidentialité, afin de prendre les moyens pour protéger les Renseignements personnels impliqués, mitiger les risques de préjudice et d'en limiter les conséquences.

3. Signalement d'un incident de confidentialité

3.1. L'Organisme compte sur la collaboration de l'ensemble des membres de sa direction et de son personnel pour signaler les événements qui correspondent à un incident de confidentialité au responsable de la protection des Renseignements personnels au sein de l'Organisme, à savoir :

Nom : Mylène Bergeron, directrice des communications et de la collecte de fonds
Adresse : 1175, avenue Lavigerie, bureau 420, Québec (Québec) G1V 4P1
Courriel : mylene.bergeron@fbfq.ca

(Ci-après : le « **Responsable de la protection des renseignements personnels** »)

[1] RLRQ c. A -2.1.

3.2. La personne qui constate ou qui doute de la survenance d'un incident de confidentialité doit le signaler, avec empressement, *via* le formulaire prévu à cette fin en Annexe A ou par tout autre moyen de communication mis en place par l'Organisme par celle-ci (ci-après : le « **Signalement** »);

3.3. Le Signalement est adressé au Responsable de la protection des renseignements personnels et précise, si possible, et selon les informations connues au moment du Signalement, les Renseignements personnels visés par l'incident, les circonstances de l'incident, le nombre de personnes visées et les dates pertinentes, à savoir, la date ou la période de la survenance ainsi que la date de la détection de l'incident. Si certains éléments ne sont pas connus lors du Signalement, ils pourront être transmis au Responsable de la protection des renseignements personnels ultérieurement, dès leur connaissance;

3.4. La personne, incluant tout client ou employé, qui croit que ses Renseignements personnels ont fait l'objet d'un incident de confidentialité, est invitée à formuler sa plainte par écrit au Responsable de la protection des renseignements personnels en conformité avec la procédure de traitement des plaintes.

4. Étapes et démarches en cas d'incident de confidentialité

4.1. Avec empressement et diligence, lors d'un Signalement, les étapes ci-dessous doivent être réalisées. À noter que le délai où les mesures ont été prises ou le délai d'exécution envisagé sont importants et pourront être considérés par la Commission d'accès à l'information :

4.1.1. **Rassembler l'équipe d'intervention** : Le Responsable de la protection des renseignements personnels devra s'adjoindre d'une ou de plusieurs personnes pour évaluer l'incident de confidentialité. Par exemple, un responsable de la sécurité informatique, de la gestion des risques ou des communications est des ressources qui peuvent être impliquées à l'interne. Ensemble, ils forment l'équipe d'intervention. Au besoin, des conseillers externes, tels que des conseillers juridiques ou des experts en cybersécurité, pourront être appelés pour accompagner l'Organisme à gérer et à analyser l'incident de confidentialité;

4.1.2. **Évaluation de l'incident de confidentialité** : Si l'Organisme a des raisons de croire qu'il s'est produit un incident de confidentialité, elle doit, au meilleur de sa connaissance lors de cette étape, établir :

4.1.2.1. La cause et l'origine de l'incident ;
4.1.2.2. Les renseignements visés (personnels ou non) ainsi que leur nombre ;
4.1.2.3. Les personnes visées, le cas échéant, et leur emplacement géographique ;
4.1.2.4. Le risque de préjudice pour les personnes concernées selon la grille d'analyse du préjudice.

4.1.3. **Mitiger les risques :** Des mesures correctives et préventives afin de limiter les conséquences de l'incident de confidentialité doivent être prises, en s'assurant de mettre fin à la pratique non conforme et d'en limiter les conséquences. Agir rapidement pour faire cesser la pratique non autorisée, récupérer ou exiger la destruction des Renseignements personnels impliqués ou encore, corriger les lacunes informatiques ou autres ayant contribué à l'incident de confidentialité sont des mesures qui doivent être prises, si possible, pour diminuer les risques de préjudice et prévenir la récurrence d'un incident de confidentialité similaire.

4.1.3.1. À cette étape, l'établissement pourra notamment considérer les éléments suivants :

4.1.3.1.1. Contenir la menace par le confinement / isolement des composants affectés
4.1.3.1.2. Modifier (révoquer) les accès et mots de passe si requis
4.1.3.1.3. Identifier, localiser et préserver les renseignements visés par l'incident
4.1.3.1.4. Protéger la confidentialité des renseignements personnels visés
4.1.3.1.5. Récupérer les renseignements personnels / les supports – obtenir une confirmation de destruction / de non-diffusion du responsable de l'incident
4.1.3.1.6. Empêcher la diffusion / la divulgation des renseignements – chiffrement, blocage des accès
4.1.3.1.7. Conserver tous les documents en place au moment de l'incident sans les modifier, notamment pour préserver la preuve

4.1.4. **Gérer les communications :** Aucune communication à l'externe, par exemple aux partenaires ou au grand public, notamment sur les médias sociaux, ne devrait être effectuée sans l'accord du responsable des communications de l'Organisme ou, à défaut, d'un expert en communication. Les courriels à l'interne, par exemple aux gestionnaires et à tous les employés, devront également être approuvés par ce responsable afin de gérer le message communiqué par l'Organisme qui aura un effet sur sa réputation.

5. Classification de l'incident de confidentialité

5.1. Dès que possible, suivant la réception d'un Signalement, le Responsable de la protection des renseignements personnels classifie l'incident de confidentialité.

5.2. La classification d'un incident est une activité subjective. L'équipe d'intervention doit tenir compte de différents facteurs reliés à l'incident qu'elle consignera éventuellement au registre (voir article 7 relatif au registre), notamment :

5.2.1. des préjudices réels ou éventuels en découlant;
5.2.2. de son étendue et de sa durée (criticité);
5.2.3. de sa cause principale;
5.2.4. de la nature délicate ou non de l'information touchée (sensibilité);

5.3. L'équipe d'intervention revoit et valide l'exactitude des éléments consignés divulgués lors du Signalement, le cas échéant.

6. Évaluation du préjudice et avis

6.1. Le Responsable de la protection des renseignements personnels devra évaluer le préjudice potentiel relié à l'incident de confidentialité. En effet, la gravité du risque de préjudice auquel sont exposées les personnes concernées devra être étudiée et, pour ce faire, les éléments suivants seront notamment considérés.

6.2. **Les Renseignements personnels concernés et leur sensibilité.** Le Responsable de la protection des renseignements personnels doit être en mesure de faire une description des Renseignements personnels visés par l'incident de confidentialité. Il doit prendre les moyens pour que l'Organisme soit au courant de l'identité des personnes concernées par les Renseignements personnels impliqués, par exemple, des clients ou des employés. La sensibilité des Renseignements personnels impliqués dans l'incident de confidentialité est également importante. En effet, certains renseignements sont sensibles par leur nature (par exemple, s'ils sont médicaux ou autrement intimes) ou selon le contexte de leur utilisation. Si les Renseignements personnels impliqués dans l'incident de confidentialité sont sensibles, cela favorisera la qualification du préjudice comme étant « sérieux ». À noter qu'en cas d'avis à la Commission d'accès à l'information, l'Organisme devrait être en mesure de justifier la raison pour laquelle elle se trouve dans l'impossibilité de fournir la description des Renseignements personnels impliqués, si cette information ne peut être fournie ou si elle n'est pas connue.

6.3. **Les conséquences appréhendées de leur utilisation.** Si les Renseignements personnels impliqués dans l'incident de confidentialité sont susceptibles d'être utilisés pour commettre une fraude ou un vol d'identité, ou si une atteinte importante à la vie privée peut résulter de leur utilisation, il est probable que le préjudice soit qualifié de « sérieux ». L'intention des personnes impliquées à la source même de l'incident de confidentialité, s'il y en a, est un facteur déterminant.

6.4. **Analyse du préjudice.** De façon générale, un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts, de manière non négligeable. Il peut conduire, par exemple, à l'humiliation, à une atteinte à la réputation, à une perte financière, à des conséquences négatives sur un dossier de crédit ou à une perte d'emploi. Par exemple, s'il est déjà connu que les Renseignements personnels seront utilisés sur le Dark web, le risque de préjudice « sérieux » est réel.

6.5. Si l'incident présente un risque de préjudice sérieux, l'Organisme avise, avec diligence, toute personne dont un Renseignement personnel est concerné par l'incident, sauf si l'avis est susceptible d'entraver une enquête au sens de la Loi. Dans ce cas, l'Organisme doit aussi déclarer, avec diligence, l'incident qui présente un risque de préjudice sérieux à la Commission d'accès à l'information ainsi qu'à toute personne susceptible de diminuer le risque de préjudice sérieux, sous réserve de certaines conditions prévues par la Loi à respecter.

6.6. La grille d'évaluation du préjudice est jointe en Annexe B et le contenu des avis à la Commission d'accès à l'information et aux personnes concernées est joint en Annexe C.

6.7. Il est également possible que l'Organisme doive aviser d'autres personnes en vertu des diverses ententes contractuelles auxquelles elle est partie, et ce, même si le préjudice potentiel n'est pas sérieux.

7. Tenue d'un registre

7.1. Dès qu'un incident de confidentialité est porté à l'attention du Responsable de la protection des renseignements personnels, l'incident doit être consigné au registre des incidents de confidentialité de l'Organisme, et ce, même s'il ne comporte pas de risque de préjudice sérieux et même si aucun avis n'a été transmis à la personne concernée ou à la Commission d'accès à l'information le concernant;

7.2. Ce registre des incidents de confidentialité doit comprendre certaines informations, dont notamment, le Signalement, les Renseignements personnels visés par l'incident, les dates de survenance de l'incident, ainsi que celles relatives à la détection par l'Organisme et de transmission des avis, s'il y a lieu.

7.3. Le registre collige également les informations sur les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice, les mesures prises par l'Organisme, en réaction à l'incident;

7.4. L'Organisme doit tenir le registre des incidents de confidentialité à jour et le conserver pour une période de cinq (5) ans après sa connaissance de l'incident.

7.5. Le contenu du registre est joint en Annexe D.

8. Évaluation approfondie, changements et mise en place de mesures correctives

8.1. Dans un délai raisonnable suivant le Signalement, le Responsable de la protection des Renseignement personnels analyse, avec diligence, la situation qui a conduit à l'incident de confidentialité et détermine si les normes, politiques ou directives internes de l'Organisme, au moment de l'incident, ont été suivies;

8.2. Dans la négative, il identifie les raisons pour lesquelles ces règles de mises en place et élaborées par l'Organisme n'ont pas été suivies, le cas échéant, et il voit à la mise en place de mesures préventives, pour éviter qu'un tel incident ne survienne à nouveau;

8.3. Si le responsable est d'avis qu'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les processus doivent être adaptés pour éviter qu'un tel incident de confidentialité ne survienne à nouveau;

8.4. Dans tous les cas, la sensibilisation des ressources de l'Organisme peut être renforcée en lien avec la survenance de l'incident de confidentialité.

9. Mise en place de mesures préventives

9.1. Le Responsable de la protection des renseignements personnels devra mettre en place des mesures raisonnables ayant pour objectif d'éviter qu'un incident de même nature se produise à nouveau. Il peut, entre autres :

9.1.1. Mettre en place des contrôles systématisés à l'attention du personnel de direction ou d'utilisateurs spécifiques ayant accès aux Renseignements personnels au sein de l'Organisme;
9.1.2. Ajouter des politiques, procédures, normes ou directives dont certaines relatives à l'identification supplémentaires ou l'accès, afin de minimiser les risques reliés à toute utilisation ou communication inadéquate des Renseignements personnels;
9.1.3. Mandater des spécialistes afin de procéder à une enquête approfondie sur les processus opérationnels de l'Organisme ou les mesures de protection mises en place par l'Organisme;
9.1.4. Revoir les ententes et les processus opérationnels liés aux fournisseurs de services qui ont accès à des Renseignements personnels collectés par l'Organisme ou à qui ces renseignements sont communiqués;
9.1.5. Offrir des formations ponctuelles à des ressources ciblées ou encore, dispenser de la formation et des ateliers de sensibilisation en matière de protection des Renseignements personnels à l'ensemble du personnel de l'Organisme ou à certaines ressources davantage concernées.

10. Recommandations et solutions

10.1. Le Responsable de la protection des Renseignements personnels émet des recommandations relatives aux solutions à moyen et à long terme.

ANNEXE A

Signalement d'un incident de confidentialité des renseignements personnels

Date de survenance de l'incident	Date de détection par l'organisation	Renseignements personnels visés par l'incident	Circonstances de l'incident	Nombre de personnes visées

ANNEXE B

Grille d'analyse concernant l'évaluation du préjudice en cas d'incident de confidentialité des renseignements personnels.

Cette grille vous permet d'évaluer le préjudice lorsqu'un incident de confidentialité se produit au sein de l'Organisme.

Date ou période de l'événement :

Type d'incident / cause de l'incident :
☐ Accès non autorisé
☐ Utilisation non autorisée
☐ Communication non autorisée
☐ Perte ou autre atteinte à la protection des renseignements personnels
☐ Autre. Préciser : _____

Quels renseignements personnels sont concernés :
☐ Renseignements d'identification *(Ex. : Nom, coordonnées (adresse postale, courriel, numéro de téléphone), numéro d'assurance sociale / maladie, permis de conduire, code permanent, codes d'utilisateur, mot de passe, etc.)* ☐ Renseignements démographiques *(Ex. : Date de naissance, origines ethniques, orientation sexuelle, identité de genre, religion, état matrimonial, niveau d'instruction, etc.)* ☐ Renseignements de nature financière *(Ex. : Numéro de carte de crédit, de compte bancaire, information sur le soutien financier ou l'accommodation financière fournie par un établissement à un élève / un employé, salaire, conditions d'emploi, etc.* ☐ Renseignements de nature médicale *(Ex. Âge, taille, poids, dossiers médicaux, groupe sanguin, etc.)* ☐ Autre. Préciser : _____ *(Ex. Antécédents judiciaires, dossier d'employé, etc.)*

Les renseignements personnels concernés sont-ils sensibles ? *(Note : certains renseignements sont sensibles par leur nature (par exemple, s'ils sont médicaux ou autrement intimes) ou selon le contexte de leur utilisation)*
☐ Oui
☐ Non

Quelles sont les conséquences appréhendées de l'utilisation du renseignement personnel visé par l'incident de confidentialité ?
☐ Vol d'identité
☐ Fraude financière / Impact sur le dossier de crédit
☐ Diffusion des renseignements personnels, notamment sensibles
☐ Répercussion sur la santé physique ou psychologique
☐ Perte d'emploi
☐ Perte financière
☐ Humiliation, atteinte à la réputation, à la vie privée
☐ Impact sur les relations professionnelles ou d'affaires
☐ Autre. Préciser : _____

Quelles sont les probabilités de l'utilisation du renseignement personnel visé par l'incident de confidentialité à des fins préjudiciables : *(Note : l'intention des personnes impliquées à la source même de l'incident de confidentialité, s'il y en a, est un facteur déterminant)*
☐ Faibles ☐ Moyennes ☐ Élevées ☐ Inconnues

En fonction de cette évaluation (niveau du préjudice, du type de renseignements personnels visés, des mesures prises, de la probabilité que les conséquences appréhendées se réalisent), le risque de préjudice est jugé : *(Note : de façon générale, un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts, de manière non négligeable.)*
☐ Négligeable ☐ Modéré ☐ Sérieux

En fonction de cette évaluation (niveau du préjudice, du type de renseignements personnels visés, des mesures prises, de la probabilité que les conséquences appréhendées se réalisent), l'incident de confidentialité doit : *Plus d'un choix peut s'appliquer.* *(Note : Si l'incident présente un risque de préjudice sérieux, l'Organisme avise, avec diligence, toute personne dont le renseignement personnel est concerné par l'incident, sauf si l'avis est susceptible d'entraver une enquête, de même que la CAI et toute personne susceptible de diminuer le risque de préjudice sérieux. Dès qu'un incident de confidentialité est porté à l'attention du Responsable de la protection des renseignements personnels, l'incident doit être consigné au registre des incidents de confidentialité de l'Organisme, et ce, même s'il ne comporte pas de risque de préjudice sérieux.)*
☐ Être inscrit au registre des incidents de confidentialité ☐ Être déclaré avec diligence à la Commission d'accès à l'information ☐ Être déclaré aux personnes concernées

Signature de la personne ayant fait l'évaluation	**Responsable de la protection des renseignements personnels**
Nom :	Nom :

ANNEXE C

CONTENU DES AVIS

L'avis écrit à la Commission d'accès à l'information (« CAI ») doit contenir les informations suivantes :

1. Le nom de l'organisation concernée par l'incident de confidentialité ainsi que son numéro d'entreprise du Québec;
2. Les coordonnées d'une personne au sein de l'Organisme qui peut répondre à des questions au sujet de l'incident;
3. Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison pour laquelle il est impossible de fournir une telle description;
4. Un sommaire descriptif des causes et circonstances de l'incident, si elles sont connues;
5. La date de l'incident et la période durant laquelle il a eu lieu (ou une approximation si cette information n'est pas connue);
6. La date ou période durant laquelle l'Organisme a découvert l'incident;
7. Le nombre de personnes concernées par l'incident et le nombre de personnes concernées par l'incident qui résident au Québec (ou une approximation si cette information n'est pas connue);
8. Une description des éléments qui ont permis de conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées;
9. Les mesures que l'Organisme a prises ou qu'elle entend prendre pour aviser les personnes concernées de l'atteinte;
10. Les mesures prises ou prévues par l'Organisme après l'incident, y compris celles visant à réduire/atténuer le risque de préjudice et à éviter que de tels incidents ne se reproduisent à l'avenir;
11. La démonstration que d'autres organismes de protection des renseignements personnels ont été informés de l'incident, le cas échéant.

L'avis aux personnes concernées par l'incident de confidentialité est le suivant :

« Avis à la personne concernée par un incident de confidentialité causant un préjudice sérieux

Dans le respect des obligations auxquelles [elle ou il] est [tenue ou tenu] en application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* [la ou le nom de l'organisme public] souhaite vous informer de la survenance récente d'un incident de confidentialité qui concerne vos renseignements personnels. [Décrire les renseignements personnels visés par l'incident (ex. : Les renseignements personnels visés dans cet incident sont…) ou, si cette information n'est pas connue, la raison qui justifie l'impossibilité de les mentionner].

En effet [insérer une brève description des circonstances de l'incident]. Cet incident est survenu [inscrire la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période].

Soyez [assurée ou assuré] que [la ou le nom de l'organisme public] met actuellement en œuvre des mesures afin de diminuer les risques qu'un préjudice vous soit causé. À cet égard [inscrire une brève description des mesures que l'organisme public a prises ou qu'il entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé].

De plus, afin d'optimiser la protection de vos renseignements personnels, nous vous suggérons [décrire les mesures que l'organisme public suggère à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer un tel préjudice].

Pour toute question ou précision complémentaire en lien avec cet incident en particulier, nous vous invitons à communiquer avec [inscrire les coordonnées qui permettront aux personnes concernées d'obtenir des informations supplémentaires relativement à l'incident]. »

ANNEXE D

CONTENU DU REGISTRE DES INCIDENTS :

1. 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;

2. Une brève description des circonstances de l'incident;

3. La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue);

4. La date ou la période à laquelle l'Organisme s'est aperçu de l'incident;

5. Le nombre de personnes concernées par l'incident (ou une approximation si cette information n'est pas connue);

6. La description des éléments qui ont mené à la conclusion que les personnes concernées sont à risque d'un préjudice sérieux;

7. Si l'incident présente un risque de préjudice sérieux, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées. Le registre doit aussi indiquer si un avis public a été nécessaire, et

8. Une brève description des mesures prises par l'Organisme ou qu'elle prévoit de prendre suivant l'incident dans le but de réduire les risques de préjudice.