SODEC Québec

PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL

Approbation comité de direction : 2022-12-12
Dernière révision : 2023-09-28

Table des matières

PRÉAMBULE

La Société de développement des entreprises culturelles (la « **SODEC** ») est responsable de la protection des renseignements personnels qu'elle détient, que leur conservation soit assurée à l'interne ou par un tiers. Les renseignements personnels sont confidentiels, sauf dans la mesure prévue par la législation. Toute personne qui, dans le cadre de ses fonctions, a accès à un renseignement personnel détenu par la SODEC doit prendre les moyens nécessaires pour en assurer la protection et la confidentialité. Néanmoins, des incidents de confidentialité impliquant un renseignement personnel détenu par la SODEC peuvent survenir, et c'est pourquoi la SODEC a choisi de se doter de la présente Procédure de gestion des incidents de confidentialité impliquant un renseignement personnel (la « **Procédure** »).

La Procédure met en place un cadre de gestion des incidents de confidentialité conforme aux obligations en matière de protection des renseignements personnels suivant l'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*.

1. OBJECTIF ET CADRE NORMATIF

La Procédure a pour but de gérer les incidents de confidentialité et limiter leurs éventuelles conséquences négatives pour les personnes concernées et la SODEC. Elle établit la démarche à suivre en cas d'incident de confidentialité impliquant un renseignement personnel détenu par la SODEC, précise les rôles et les responsabilités des intervenants en cas d'incident, détermine les modalités de la tenue d'un registre des incidents et rappelle l'obligation d'effectuer les déclarations obligatoires requises en cas d'incident de confidentialité impliquant un renseignement personnel.

Le cadre normatif de cette Procédure comprend principalement :

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, telle que modifiée par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, RLRQ, c. 25 (la « **Loi sur l'accès** »);
- Règlement sur les incidents de confidentialité;
- Politique de sécurité de l'information;
- Politique de confidentialité.

2. CHAMP D'APPLICATION

La Procédure s'applique à tous les employés de la SODEC et à tous les tiers auxquels la SODEC communique des renseignements personnels, y compris tous les fournisseurs ou partenaires, ainsi que les sous-traitants (ci-après un « **tiers** ») ayant connaissance d'un incident de confidentialité en lien avec les renseignements personnels communiqués.

3. DÉFINITIONS

Dans le cadre de la Procédure, les termes ci-dessous ont les définitions données en annexe. Ils peuvent être complétés par toute autre politique, directive ou procédure y faisant référence.

4. SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

Dès qu'une personne, employé ou tiers, a des motifs de croire que s'est produit un incident de confidentialité, elle doit signaler l'incident en remplissant une déclaration d'incident de confidentialité.

4.1 Déclaration d'incident de confidentialité

Pour les employés, la déclaration s'effectue par c2Atom. Pour toute personne qui n'est pas un employé de la SODEC, cette déclaration peut être faite à l'aide de l'adresse courriel suivante : incident.confidentialite@sodec.gouv.qc.ca.

4.2 Avis au gestionnaire

En plus de remplir la déclaration d'incident, les employés doivent également aviser leur gestionnaire sans délai.

L'employé, sa ou les directions concernées de même que tout tiers signalant l'incident doivent collaborer à l'analyse de l'incident.

La déclaration de l'incident est reçue par le Responsable AIPRP de même que par le directeur des technologies de l'information.

5. DÉTECTION ET ÉVALUATION PRÉLIMINAIRE

Le responsable AIPRP prend connaissance de la déclaration d'incident et effectue une évaluation préliminaire de la situation. S'il détermine que cette dernière correspond à un incident de confidentialité, il transmet son évaluation préliminaire et la déclaration d'incident aux membres du comité AIPRP.

6. ÉVALUATION DU RISQUE ET MESURES À PRENDRE

À la suite de la réception de la déclaration d'incident et de l'évaluation préliminaire du Responsable AIPRP, le Comité AIPRP se réunit afin que celui-ci :

a. procède à une évaluation du risque qu'un préjudice sérieux soit causé à une personne;
b. s'assure que les mesures préventives et correctrices raisonnables existantes sont adéquates pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Dans le cas contraire, le Comité AIPRP détermine les mesures devant être prises pour les corriger.

Le Comité AIPRP doit se réunir aussi souvent que requis, selon la gravité de l'incident. Il peut convoquer tout membre du personnel jugé utile et doit documenter ses travaux, en répondant aux questions prévues à l'annexe 2. En fonction de la gravité de l'incident de confidentialité, le Comité AIPRP peut également demander à des parties externes telles qu'un fournisseur de sécurité de l'information d'effectuer des enquêtes criminalistiques numériques ou à une agence de communication externe d'aider la Société lors de communications en situation de crise, etc.

7. MESURES URGENTES POUR LIMITER L'ATTEINTE À LA VIE PRIVÉE

En cas d'incident de confidentialité, la ou les directions concernées, de même que la direction des technologies de l'information, au besoin, doivent prendre toute mesure urgente requise pour limiter les conséquences pour les personnes concernées, notamment la possibilité d'utilisation malveillante des renseignements personnels, l'usurpation ou le vol d'identité.

8. DÉCLARATION DE L'INCIDENT

Si l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes concernées par les renseignements personnels, le responsable AIPRP doit, avec diligence, transmettre un avis à la Commission et aux personnes concernées par les renseignements personnels, si nécessaire. Le contenu de ces avis doit être conforme aux dispositions du Règlement sur les incidents de confidentialité, tel que détaillé à l'annexe 3 des présentes. Le Responsable AIPRP doit également aviser la personne concernée de l'incident, s'il existe un risque probable de préjudice sérieux. Cet avis, qui doit être transmis sans délai, doit être rédigé dans un langage clair et simple, et contenir les informations exigées suivant les dispositions du Règlement sur les incidents de confidentialité, telles que détaillées à l'annexe 3 des présentes.

Lorsque l'incident de confidentialité constitue un crime ou peut être qualifié de criminel, le Responsable AIPRP doit aviser les services de police compétents.

Le Responsable AIPRP peut également aviser toute personne ou tout organisme susceptibles de diminuer ce risque, et ce, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée.

Finalement, le responsable PRP avise, avec diligence, la personne responsable des contacts avec les assureurs, le cas échéant.

9. ÉVALUATION APPROFONDIE DE LA SITUATION ET PRÉVENTION

Le responsable AIPRP et le Comité AIPRP doivent effectuer une évaluation approfondie de l'incident afin d'éviter que de nouveaux incidents de même nature ne se produisent. Cette évaluation approfondie doit être documentée et contenir notamment les informations prévues à l'annexe 4.

L'évaluation approfondie doit être transmise sur demande au président-directeur général lorsqu'elle est terminée. Ce dernier peut également la transmettre au conseil d'administration de la SODEC s'il juge pertinent de le faire.

10. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Le responsable AIPRP doit tenir un registre des incidents de confidentialité conforme au Règlement sur les incidents de confidentialité. Le Responsable AIPRP doit y consigner tout incident de confidentialité indifféremment de sa gravité et de l'existence ou non d'un risque de préjudice sérieux. Une copie du registre doit être transmise à la Commission sur demande.

Les renseignements contenus dans le registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle la SODEC a pris connaissance de l'incident.

11. RESPONSABLE DE LA PROCÉDURE

Le Responsable AIPRP est responsable de l'application de la présente Procédure.

12. ENTRÉE EN VIGUEUR

La présente Procédure entre en vigueur le 12 décembre 2022.

ANNEXE 1 : DÉFINITIONS

Dans le cadre de la présente Procédure, les termes et expressions ci-dessous ont les définitions suivantes. Ils peuvent être complétés par toute autre politique, directive ou procédure y faisant référence.

Comité AIPRP : Comité sur l'accès à l'information et sur la protection des renseignements personnels;

Commission : Commission d'accès à l'information du Québec;

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

En voici quelques exemples :

- Un membre du personnel consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions;
- Un pirate informatique s'infiltre dans un système;
- Une personne utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne;
- Une communication est effectuée par erreur à la mauvaise personne, contenant des renseignements personnels;
- Une personne perd ou se fait voler des documents contenant des renseignements personnels;
- Une personne s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

Personne concernée : personne physique dont les renseignements personnels sont exposés à un risque en raison de la survenance d'un incident de confidentialité.

Renseignement personnel (RP) : tout renseignement qui concerne une personne physique et qui permet de l'identifier directement ou indirectement. Le nom d'une personne, pris isolément, n'est pas un renseignement personnel. Cependant, lorsque ce nom est associé ou jumelé à un autre renseignement visant cette même personne, il devient alors un renseignement personnel.

Voici des exemples de renseignements personnels :

- Le nom d'une personne et sa date de naissance;
- Un numéro d'assurance sociale;
- Un numéro de carte de crédit;
- Un numéro d'assurance maladie;
- Un renseignement de nature médicale ou financière;
- Le nom d'une personne et son numéro de téléphone personnel;
- Le nom d'une personne et l'adresse de son domicile.

Responsable AIPRP : le président-directeur général ou la personne désignée par celui-ci par délégation de compétence conformément aux dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;

ANNEXE 2 : ÉVALUATION DU RISQUE ET MESURES À PRENDRE

Le Comité AIPRP doit procéder à une évaluation du risque et déterminer si des mesures doivent être prises.

ÉVALUATION DU RISQUE
Quelle est la sensibilité des RP? Considérez la nature et la quantité des RP en cause, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.
Cliquez ici pour entrer du texte.
Quelles sont les personnes concernées par l'incident? S'agit-il d'employés, de membres ou de partenaires d'affaires? Qui peut avoir eu accès aux renseignements personnels? Combien de personnes sont touchées par l'incident? Considérez la portée de l'incident de confidentialité. Se référer à la déclaration d'incident de confidentialité.
Cliquez ici pour entrer du texte.
Est-ce que les RP étaient chiffrés ou cryptés? Précisez le type de chiffrement en inscrivant, le cas échéant, la méthode, la norme ou les standards retenus. Précisez les mesures prises pour préserver la confidentialité de la clé de chiffrement et éviter le déchiffrement des données.
Cliquez ici pour entrer du texte.
Quelles sont les causes de l'incident? Se référer à la déclaration d'incident de confidentialité.
Cliquez ici pour entrer du texte.
Est-ce que les RP pourraient être exploités par des personnes malveillantes et quel est le type de préjudice pouvant être causé aux personnes concernées par l'incident? Précisez les types d'utilisation malveillante possibles des RP et les répercussions ou les conséquences négatives qui pourraient en résulter. Par exemple : dommage économique ou social (vol et usurpation d'identité ou fraude, perte liée aux affaires, perte d'occasions d'emploi), répercussions sur la santé physique ou psychologique (stress), dommages moraux (atteinte à la réputation, humiliation, diffamation, discrimination).
Cliquez ici pour entrer du texte.
Quel est le niveau de préjudice que pourraient subir les personnes concernées? Précisez : faible, moyen ou élevé en indiquant les faits qui vous amènent à établir ce niveau de préjudice.
Cliquez ici pour entrer du texte.
Est-ce que la situation a un caractère réversible? Par exemple, est-il possible de récupérer les renseignements personnels?
Cliquez ici pour entrer du texte.
Est-ce que des mesures de protection des RP et de sécurité prises immédiatement après la découverte de l'incident ont permis de réduire les risques de préjudices aux personnes concernées et d'atténuer les éventuels effets négatifs de cet incident?
Cliquez ici pour entrer du texte.

Quand a eu lieu l'incident? Quel est le délai écoulé entre la découverte de l'incident et les mesures prises? Se référer à la déclaration d'incident de confidentialité.
Cliquez ici pour entrer du texte.
MESURES À PRENDRE
Est-ce que d'autres mesures doivent être prises pour réduire les effets de l'incident sur les personnes concernées et les préjudices potentiels pour celles-ci ainsi que pour éviter que ce type d'incident se reproduise? Déterminez les priorités et les mesures à prendre à partir des résultats de l'évaluation des risques.
Cliquez ici pour entrer du texte.

ANNEXE 3 : CONTENU DES AVIS

Conformément au Règlement sur les incidents de confidentialité :

1. Avis aux personnes concernées

L'avis aux personnes concernées doit contenir les renseignements suivants :

a. 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;
b. Une brève description des circonstances de l'incident;
c. La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de la période;
d. 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;
e. 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;
f. Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

L'avis est transmis à la personne concernée par l'incident de confidentialité. Toutefois, l'avis est donné au moyen d'un avis public dans l'une ou l'autre des circonstances suivantes :

a. Lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;
b. Lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour la SODEC;
c. Lorsque la SODEC n'a pas les coordonnées de la personne concernée.

2. Avis à la Commission

L'avis à la Commission doit contenir les renseignements suivants :

a. Le nom de la SODEC et le numéro d'entreprise du Québec qui lui est attribué en vertu de la *Loi sur la publicité légale des entreprises*;
b. Le nom et les coordonnées de la personne à contacter à l'interne relativement à l'incident;
c. 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;
d. Une brève description des circonstances de l'incident et, si elle est connue, sa cause;
e. La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de la période;

f. La date ou la période au cours de laquelle la SODEC a pris connaissance de l'incident;
g. 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;
h. Une description des éléments qui amènent la SODEC à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que 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;
i. Les mesures que la SODEC a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;
j. Les mesures que la SODEC 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 des incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé;
k. 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 à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

L'avis à la Commission peut également être transmis en remplissant le formulaire accessible sur le site Web de la Commission au https://www.cai.gouv.qc.ca/documents/CAI_FO_avis_incident_confidentialite.pdf.

ANNEXE 4 : ÉVALUATION APPROFONDIE DE L'INCIDENT DE CONFIDENTIALITÉ ET PRÉVENTION

Dans son évaluation approfondie de l'incident de confidentialité, le Comité AIPRP doit notamment :

- au besoin, approfondir l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuer une description chronologique des événements et des mesures prises face à cet incident, y compris les dates et les intervenants concernés;

- vérifier si les normes, politiques ou directives internes en vigueur au moment de l'incident, tant sur le plan de la sécurité de l'information que sur celui de la protection des renseignements personnels, ont été suivies par les personnes impliquées – déterminer 1) les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant, et 2) si celles-ci doivent être bonifiées à la lumière de l'incident survenu;

- s'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;

- au besoin, formuler des recommandations relatives aux solutions à moyen et long terme, et aux stratégies de prévention;

- s'assurer de la réelle nécessité, pour l'organisme ou l'entreprise, de la collecte des renseignements personnels concernés;

- le cas échéant, prévoir le suivi devant être accordé.

ANNEXE 5 : SCHÉMA SUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL