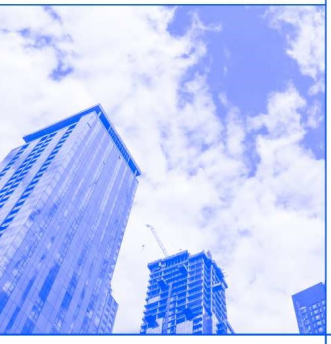
ÉA

ORDRE DES ÉVALUATEURS AGRÉÉS DU QUÉBEC



Procédure de gestion d’un incident de confidentialité

Table des matières

Classification de la politique	Politique de gouvernance
Adoption	Conseil d'administration Version 01 – 28 septembre 2023 (2324-CA-042)
Entrée en vigueur	Version 01 – 28 septembre 2023
Responsable de l'élaboration et de la révision de la politique	Comité de gouvernance, éthique et ressources humaines
Responsable de l'application de la politique	Directeur et général et secrétaire
Révision de la politique	Au minimum trois ans

Tél. : 514 281-9888 / 1-800-982-5387
Téléc. : 514 281-0120

www.oeaq.qc.ca

Procédure de gestion d'un incident de confidentialité

L'Ordre des évaluateurs agréés du Québec (ci-après « Ordre », « Nous ») reconnaît l'importance d'assurer la protection des renseignements personnels qu'il recueille auprès des candidats à la profession, de ses détenteurs de permis, de ses employés et de toute autre personne avec qui il est appelé à interagir dans le cadre de ses activités. À ce titre, l'Ordre est responsable de la protection des renseignements personnels qu'il détient ou qu'il confie, le cas échéant, à un tiers et ce, tout au long du cycle de vie de ces renseignements.

L'Ordre prend les moyens nécessaires pour assurer la protection des renseignements personnels. Néanmoins, des incidents de confidentialité impliquant des renseignements personnels peuvent survenir. L'Ordre s'est doté de la présente procédure pour être en mesure de diminuer et de répondre adéquatement en cas d'incident de confidentialité.

1. Objectif et Cadre juridique

La présente procédure a pour objectif d'établir les démarches à suivre lorsque l'Ordre a des motifs de croire que s'est produit un incident de confidentialité impliquant des renseignements personnels qu'il détient ou qu'il a confié à un tiers.

2. Cadre juridique

La présente procédure tient compte du cadre juridique applicable à l'Ordre en matière de protection des renseignements personnels, notamment :

- *Code des professions* (RLRQ, c. C-26)
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels lorsque les renseignements personnels* (RLRQ, c. A-2.1) sont détenus dans le cadre du contrôle de l'exercice de la profession
- *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1) lorsque les renseignements personnels sont détenus dans le cadre de ses autres fonctions et activités
- *Règlement sur les incidents de confidentialité* (RLRQ, c. A-2.1, r. 3.1)

3. Champ d'application

La présente procédure s'applique aux employés, membres d'un comité, administrateurs de l'Ordre mais aussi aux tiers auxquels l'Ordre communique des

renseignements personnels, aux fournisseurs ou partenaires de l'Ordre, incluant les sous-traitant.

4. Définition

Aux fins de la présente procédure, on entend par :

- **Incident de confidentialité** : tout accès, utilisation ou communication non autorisée par la loi d'un Renseignement personnel, ou toute perte ou autre atteinte à la protection de ce renseignement.
    - *Exemples d'accès non autorisé par la loi :*
        - *Consultation non autorisée / non nécessaire à l'exercice des fonctions des renseignements personnels par un employé ou par un fournisseur de service ;*
        - *Intrusion d'un tiers dans le système informatique de l'entreprise : hameçonnage, rançongiciel, etc. ;*
        - *Etc.*
    - *Exemples d'utilisation non autorisée par la loi :*
        - *Membre du personnel qui 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 ;*
        - *Consultation / extraction non autorisée de renseignements personnels ;*
        - *Etc.*
    - *Exemples de communication non autorisée par la loi :*
        - *Communication de renseignements personnels à la mauvaise personne ;*
        - *Etc.*

- **Personne concernée** : toute personne dont les Renseignements personnels sont visés par un Incident de confidentialité.

- **Personne liée** : employés, membres d'un comité, administrateurs de l'Ordre, tiers auxquels l'Ordre communique des renseignements personnels, fournisseurs ou partenaires de l'Ordre, incluant les sous-traitants.

- **Préjudice sérieux** : Acte ou évènement susceptible de porter atteinte à la Personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.

- **Renseignement personnel** : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

- **Responsable de la protection des renseignements personnels** : personne veillant à assurer le respect et la mise en œuvre du cadre juridique applicable à la protection des renseignements personnels au sein de l'Ordre.

5. Procédure à suivre

5.1. Signalement

Si une personne liée à l'Ordre a des raisons de croire qu'un incident de confidentialité impliquant des renseignements personnels s'est produit, elle doit en aviser, sans délai, le Responsable de la protection des renseignements personnels de l'Ordre et lui fournir toute information pertinente.

5.2. Évaluer la situation

Le Responsable de la protection des renseignements personnels doit :

- **Examiner** le signalement afin de **déterminer** s'il s'agit d'un incident de confidentialité impliquant des renseignements personnels.
    - *Exemples de questions à se poser :*
        - *Les informations visées par l'incident sont-elles des Renseignements personnels ?*
        - *Les Renseignements personnels ont-ils fait l'objet d'un accès, d'une utilisation ou d'une communication non autorisée par la loi ? ont-ils fait l'objet d'une perte ou de toute autre atteinte à leur protection ?*

- **Aviser** les intervenants concernés à l'interne afin d'identifier, de circonscrire, d'enquêter et de corriger la situation liée à l'incident de confidentialité.

    - Directeur général et secrétaire, employés, administrateurs, membres de comités, etc.

    - *Exemples de questions à se poser :*
        - *Quelle est la cause de l'incident ?*
        - *Quelles est la date ou la période visée par l'incident ?*
        - *Quelles sont les renseignements personnels visés ?*
        - *Étaient-ils chiffrés / protégés par un mot de passe ?*
        - *Ont-ils été récupérés ou détruits ?*
        - *Qui sont les personnes concernées par l'incident ? Quel est leur nombre ?*
        - *Quelles sont les mesures de sécurité en place au moment de l'incident ?*

- **Aviser** la haute direction et, selon la gravité de l'incident, le conseil d'administration.

5.3. Diminuer les risques – Limiter les atteintes à la vie privée

Le Responsable de la protection des renseignements personnels doit prendre rapidement les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

- *Exemples de mesures à prendre :*
    - *Récupérer ou exiger la destruction des Renseignements personnels impliqués ;*
    - *Révoquer ou modifier les mots de passe ;*
    - *Cesser la pratique non autorisée ;*
    - *Corriger les lacunes des systèmes informatiques ;*
    - *Contacter les personnes ou organismes à l'externe susceptibles de diminuer le risque de préjudice.*

5.4. Identifier le risque de préjudice

Afin de déterminer si le préjudice est sérieux, le Responsable de la protection des renseignements personnels doit identifier le risque de préjudice en tenant compte :

- de la **sensibilité** des Renseignements personnels
    - Renseignement de nature financière (Numéro de carte de crédit, de compte, de transit, information sur le soutien financier fourni par un ordre ou sur l'accommodation financière accordée, salaire, conditions d'emploi) ;
    - Renseignement de nature médicale ;
    - Renseignement d'identification (Numéro d'assurance sociale / maladie, permis de conduire) ;
    - Renseignement sur les origines ethniques, l'orientation sexuelle, l'identité de genre ;
    - Renseignement génétique ou biométrique ;
    - Etc.

- des **conséquences appréhendées** de l'utilisation des Renseignements
    - Vol d'identité ;
    - Fraude financière / Impact sur le dossier de crédit ;
    - Diffusion des renseignements personnels, notamment sensibles ;
    - Permanence / Perpétuation de l'atteinte ;
    - Répercussion sur la santé physique ou psychologique ;
    - Perte d'emploi ;
    - Humiliation, atteinte à la réputation, à la vie privée ;
    - Impact sur les relations professionnelles ou d'affaires ;
    - Etc.

- de la **probabilité** que les Renseignements soient utilisés à des fins préjudiciables.

5.5. Aviser les autorités compétentes et les personnes concernées

Le Responsable de la protection des renseignements personnels doit :

- **Aviser la CAI**, avec diligence, en cas de préjudice sérieux
    - L'avis à la CAI doit être fait par écrit et contenir les éléments suivants (possible de remplir le formulaire prévu à cet effet sur le site de la CAI) :
        - le nom de l'Ordre ;
        - le nom et les coordonnées de la personne à contacter au sein de l'Ordre relativement à l'incident ;
        - 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 ;
        - une brève description des circonstances de l'incident et, si elle est connue, sa cause ;
        - la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période ;
        - la date ou la période au cours de laquelle l'Ordre a pris connaissance de l'incident ;
        - 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 ;
        - une description des éléments qui amènent l'Ordre 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 ;
        - les mesures que l'Ordre 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 ;
        - les mesures que l'Ordre 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 ;
        - 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.

- **Aviser les personnes** dont les Renseignements personnels sont visés par l'incident de confidentialité.

    - L'avis à doit contenir les éléments suivants :
        - Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description ;
        - Une brève description des circonstances de l'incident ;
        - La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue ;
        - Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident ;
        - Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci ;
        - Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

    - Cet avis n'a pas à être transmis aux personnes concernées tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

    - Cet avis peut être fait au moyen d'un avis public dans l'une ou l'autre des circonstances suivantes :
        - lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée ;
        - lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'Ordre ;
        - lorsque l'Ordre n'a pas les coordonnées de la personne concernée.

      Un tel avis public peut aussi être rendu afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou pour l'atténuer.

- **Aviser les services de police**

- **Aviser les assureurs de l'Ordre**

- **Aviser les conseillers juridiques** pour obtenir des conseils relativement à la préservation de la preuve et aux risques juridiques associés aux mesures déployées

- Contacter les **personnes ou organismes à l'externe** susceptibles de diminuer le risque de préjudice. Si tel est le cas :
    - Ne communiquer que les renseignements personnels à cette fin ;
    - Enregistrer la communication.

5.6. Tenir un registre des incidents de confidentialité

Le Responsable de la protection des renseignements personnels doit tenir un registre qui contient l'ensemble des incidents de confidentialité et ce, peu importe que le risque ait été qualifié de sérieux ou non.

Le registre doit contenir les éléments suivants :

- Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'Ordre doit inscrire la raison justifiant l'impossibilité de fournir cette description ;
- Une brève description des circonstances de l'incident ;
- La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue ;
- La date ou la période au cours de laquelle l'Ordre a pris connaissance de l'incident ;
- Le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre ;
- Une description des éléments qui amènent l'Ordre à conclure qu'il y a, ou non, risque qu'un préjudice sérieux soit causé aux personnes concernées, comme :
    - la sensibilité des renseignements personnels concernés ;
    - les utilisations malveillantes possibles des renseignements ;
    - les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables ;
- Les dates de transmission des avis à la Commission et aux personnes concernées, quand l'incident présente le risque de préjudice sérieux. L'Ordre doit aussi préciser si elle a donné des avis publics et la raison de ceux-ci ;
- Une brève description des mesures prises par l'Ordre à la suite de l'incident, pour diminuer les risques qu'un préjudice soit causé.

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de 5 ans après la date ou la période au cours de laquelle l'Ordre a pris connaissance de l'incident.

5.7. Faire un suivi / un bilan de l'incident

Afin de tirer les leçons de l'incident de confidentialité, le Responsable de la protection des renseignements personnels doit :

- Approfondir l'analyse des circonstances de l'incident ;

- Documenter – de manière chronologique – les actions prises en lien avec l'incident ;
- Réviser les procédures en place et, le cas échéant, en adopter de nouvelles ;
- Sensibiliser les personnes liées à l'Ordre des mesures prises.

ÉA

ORDRE DES
ÉVALUATEURS
AGRÉÉS DU
QUÉBEC

1460-1050, côte du Beaver Hall
14e étage
Montréal Québec
H2Z 0A5

Courriel : oeaq@oeaq.qc.ca
Tél. : (514) 281-9888
Tél. : 1 800 9VALEUR
Fax : (514) 281-0120