EX AEQUO
Pour une égalité sans détour

POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

ADOPTÉ LE 28 MARS 2024

TABLE DES MATIÈRES

INTRODUCTION

Ex aequo s’engage à respecter le droit à la vie privée de chaque individu et à protéger la confidentialité des renseignements personnels recueillis auprès de toutE participantE, professionnelLE externe ou employéE. Les renseignements personnels sont disponibles seulement aux personnes qui doivent y avoir accès dans l’exercice de leurs mandats pour Ex aequo.

1 DÉFINITIONS

1.1 EmployéE

Toute personne qui travaille pour Ex aequo moyennant rémunération, incluant la direction, ainsi que toutes personnes non rémunérées (bénévole, stagiaire).

1.2 Événement

Tout événement qu'Ex aequo gère ou organise.

1.3 Formulaire de signalement d'un incident de confidentialité

Le formulaire mis à la disposition de tout·et toute employéE ou participantE afin d'informer la personne responsable des renseignements personnels de l'incident de confidentialité.

1.4 Incident de confidentialité

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

1.5 Membre

Toute personne physique ou toute personne morale qui s'intéresse à la mission et aux objectifs de l'organisation et qui adhère à ceux-ci. Pour ce faire, elle doit satisfaire aux conditions générales d'admission prévues aux règlements généraux de l'organisation.

1.6 ParticipantE

Tout individu qui fournit des renseignements confidentiels à Ex aequo en lien avec la tenue d'un événement, la diffusion d'une publication, la participation à une activité ou à l'obtention d'un service.

1.7 Publication

Toute publication produite par Ex aequo ou à laquelle il contribue sous quelques formes que ce soit (verbale, écrite, audio, vidéo, informatisée ou autre).

1.8 Registre des incidents de confidentialité

L'ensemble des renseignements consignés sur des incidents déclarés et concernant les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises suite à l'incident. Les dates pertinentes y figurent aussi : survenance de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.

1.9 Risque sérieux de préjudices

Le risque évalué à la suite d'un incident de confidentialité qui pourrait porter préjudice aux personnes concernées. Ce risque est analysé par la personne responsable des renseignements personnels. Pour tout incident de confidentialité, la personne responsable évalue la gravité du risque de préjudice pour les personnes concernées en estimant **«** la sensibilité des renseignements concernés **»**, **«** les conséquences appréhendées de leur utilisation **»** et **«** la probabilité qu'ils soient utilisés à des fins préjudiciables **»**.

1.10 Renseignements personnels

Tout renseignement fourni ou communiqué à Ex aequo sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre) qui concerne un·ou une participante ou un ou une employée et qui peut être utilisé pour l'identifier, y compris : son nom, son numéro de téléphone, son adresse, son courriel, son genre, son orientation sexuelle et toute information concernant sa santé. Pour plus de certitude :

- 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 relatif à cet individu.

1.11 Service ou activité

Tout service qu'Ex aequo rend à un individu à la demande de celui-ci, ou toute activité qu'Ex aequo organise à laquelle l'individu participe.

2 PHOTOGRAPHIES ET ENREGISTREMENTS

2.1 Tout individu a le choix d'être photographié ou non, ou d'être enregistré (audio/vidéo) ou non.

2.2 Les photographies ou enregistrements qui permettent d'identifier un individu comme employé d'Ex aequo ne constituent pas un renseignement confidentiel relatif à cet individu.

3 OBLIGATION DE CONFIDENTIALITÉ

3.1 Les employéEs sont tenuEs de signer la présente entente de confidentialité (Annexe A) avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès d'Ex aequo.

3.2 L'obligation de confidentialité s'applique à la durée du bénévolat d'une personne, d'un stage, d'un contrat avec unE professionnelLE ou du lien d'emploi d'unE employéE avec Ex aequo. Cette obligation demeure même après la fin du bénévolat de la personne, de la fin du stage, de la fin du contrat ou du lien d'emploi avec Ex aequo.

4 COLLECTE ET USAGE DES RENSEIGNEMENTS PERSONNELS

4.1 Ex aequo peut, au besoin, constituer un ou des dossiers contenant des renseignements personnels concernant les employéEs. La constitution de tels dossiers a pour objet de :

- maintenir les coordonnées à jour ;
- documenter des situations de travail ou de bénévolat ;
- permettre, dans le cas des employéEs rémunéréEs, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.).

4.2 Ex aequo recueille des renseignements personnels pour chacun de ses membres afin d'établir leur profil. La consultation de ces renseignements sera faite seulement par les personnes pour qu'elles puissent réaliser leurs mandats.

4.3 Ex aequo peut, au besoin, constituer un ou des dossiers contenant des renseignements personnels concernant les participantEs. La constitution de tels dossiers a pour objet de permettre à Ex aequo de réaliser un événement, une publication, une activité ou de fournir un service.

4.4 Ex aequo peut seulement recueillir les renseignements personnels qui sont nécessaires aux fins du dossier et peut utiliser les renseignements personnels seulement à ces fins.

4.5 Les renseignements confidentiels peuvent seulement être recueillis auprès de la personne concernée, à moins que celle-ci consente à ce que la cueillette soit réalisée auprès d'autrui ou que la loi l'autorise.

5 GESTION DES RENSEIGNEMENTS PERSONNELS

5.1 La personne à la direction générale est mandatée par le conseil d'administration pour être la personne responsable d'assurer la protection des renseignements personnels. Sur le site web d'Ex aequo, il doit être indiqué que la personne à la direction générale est également la « personne responsable de la protection des renseignements personnels » ainsi que le moyen de la joindre.

La personne responsable de la protection des renseignements personnels s'assure également de la tenue d'un Registre des incidents de confidentialité.

5.2 Sous réserve de l'article 5.3, la personne à la direction générale est autorisée à accéder à tout renseignement personnel que détient Ex aequo. Les autres employéEs sont autoriséEs à accéder aux renseignements personnels dans la mesure où cet accès est nécessaire à la réalisation d'une tâche dans l'exercice de leurs fonctions.

5.3 Pour l'application des lois, un **incident de confidentialité** correspond à tout accès, utilisation ou communication non autorisé par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

5.4 Lorsqu'unE employéE ou participantE constate un incident de confidentialité, il ou elle doit informer avec diligence la personne responsable de la protection des renseignements personnels afin qu'il ou qu'elle soit inscrite au Registre des incidents de confidentialité. L'employéE ou le participantE doit, pour ce faire, compléter un formulaire de signalement et l'acheminer ensuite à la personne responsable de la protection des renseignements personnels.

Le registre doit conserver les informations sur un incident de confidentialité pour une période de cinq ans.

Doit être colligé dans le formulaire de signalement :

- 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) ;
- La date ou la période à laquelle l'organisation s'est aperçue de l'incident ;
- Le nombre de personnes concernées par l'incident (ou une approximation si cette information n'est pas connue).

5.5 La personne responsable de la protection des renseignements personnels évalue si l'incident présente un « risque sérieux de préjudice ». Les renseignements ainsi que les mesures à prendre afin de diminuer le risque qu'un préjudice sérieux soit causé aux personnes concernées sont versés au Registre des incidents de confidentialité.

Si l'incident présente un risque sérieux de préjudice, la personne responsable de la protection des renseignements confidentiels avise la Commission d'accès à l'information et les personnes concernées de tout incident présentant un risque sérieux de préjudice à l'aide du formulaire approprié.

5.6 Lors d'un accompagnement individualisé, seule la personne réalisant l'accompagnement est autorisée à accéder aux renseignements confidentiels que détient Ex aequo dans le cadre de cette activité ou de ce service. La direction générale peut toutefois y accéder dans la mesure où cela est nécessaire et convenu dans les documents balisant l'activité ou le service individualisé.

6 CONSERVATION DES RENSEIGNEMENTS CONFIDENTIELS

6.1 Les employéEs ayant accès aux dossiers en vertu des articles de la section 5 s'obligent à :

- S'assurer que les renseignements personnels soient gardés dans un lieu approprié et à l'abri de tout accès non autorisé ;
- S'assurer que tous les documents électroniques comportant des renseignements confidentiels, incluant ceux copiés sur un appareil de stockage portatif, soient cryptés et protégés par des mots de passe. La gestion des mots de passe se fera selon une méthode éprouvée;
- Garder les renseignements confidentiels en format papier dans des classeurs pouvant être verrouillés et s'assurer que les classeurs soient verrouillés à la fin de chaque journée de travail. Les clés des classeurs doivent être gardées dans des endroits sûrs.

6.2 Lorsqu'unE employéE peut également, à certains égards, être qualifiéE de participantE, les renseignements confidentiels concernant chaque titre seront conservés séparément.

6.3 Les dossiers constitués en vertu de cette politique sont la propriété d'Ex aequo.

7 DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

7.1 Sous réserve de l'article 7.2, les renseignements confidentiels sont conservés tant et aussi longtemps que l'objet pour lequel ils ont été recueillis n'a pas été accompli, à moins que l'individu concerné ait consenti à ce qu'il en soit autrement. Ces renseignements confidentiels sont ensuite détruits de façon à ce que les données y figurant ne puissent plus être reconstituées.

7.2 Les dossiers concernant les employéEs sont conservés par Ex aequo. Ceux-ci sont détruits 7 ans après la fin du lien d'emploi.

7.3 Le profil du membre est immédiatement détruit lorsqu'il décède.

7.4 Pour plus de certitude, les renseignements confidentiels concernant un individu ayant offert un témoignage, tels que son nom et ses coordonnées, sont détruits une fois le témoignage publié ou diffusé, à moins que l'individu ait préalablement consenti à ce que les renseignements confidentiels le concernant soient conservés pour permettre à Ex aequo de l'utiliser dans le futur. Pour plus de certitude, chaque utilisation du témoignage d'une personne doit être approuvée par celle-ci.

8 DIVULGATION DE RENSEIGNEMENTS PERSONNELS À UN TIERS

8.1 Autre que dans les situations où la loi le requiert et sous réserve des autres dispositions du présent article 8, les renseignements personnels ne peuvent être divulgués à un tiers qu'après l'obtention du consentement verbal ou écrit, manifeste, libre et éclairé de la personne concernée. Un tel consentement ne peut être donné que pour une fin spécifique et pour la durée nécessaire à la réalisation de cette dernière.

8.2 Les renseignements personnels peuvent être divulgués sans le consentement de la personne concernée si la vie, la santé ou la sécurité de celle-ci est gravement menacée. La divulgation doit alors être effectuée de la façon la moins préjudiciable pour la personne concernée.

8.3 Tel que permis par la loi, Ex aequo peut divulguer des renseignements personnels nécessaires à sa défense ou celle de ses employéEs contre toute réclamation ou poursuite intentée contre Ex aequo ou ses employéEs, par ou de la part d'unE participantE, d'unE employéE, ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'unE participantE ou d'unE employéE.

9 COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À LA PERSONNE CONCERNÉE

9.1 Sous réserve de l'article 9.2, les participantEs et employéEs ont le droit de connaître les renseignements personnels qu'Ex aequo a reçus, recueillis et conservent à leur sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci.

9.2 Ex aequo doit restreindre l'accès aux renseignements personnels lorsque la loi le requiert ou lorsque la divulgation révélerait vraisemblablement des renseignements confidentiels au sujet d'un tiers.

9.3 Une demande d'unE participantE ou d'unE employéE en lien avec l'article 9.1 doit être traitée dans un délai maximal de 30 jours.

10 MANQUEMENT À L'OBLIGATION DE CONFIDENTIALITÉ

10.1 UnE employéE manque à son obligation de confidentialité lorsqu'il ou elle :

- communique des renseignements personnels à des individus n'étant pas autorisés à y avoir accès ;
- discute de renseignements personnels à l'intérieur ou à l'extérieur des locaux d'Ex aequo alors que des individus n'étant pas autorisés à y avoir accès sont susceptibles de les entendre ;
- laisse des renseignements personnels sur papier ou support informatique à la vue dans un endroit où des individus n'étant pas autorisés à y avoir accès sont susceptibles de les voir ;
- fait défaut de suivre les dispositions de cette politique.

10.2 Advenant un manquement à l'obligation de confidentialité, des mesures disciplinaires appropriées, pouvant aller jusqu'à la résiliation du lien d'emploi ou de toute autre relation avec Ex aequo, seront prises à l'égard de la partie contrevenante et des mesures seront adoptées au besoin afin de prévenir qu'un tel scénario ne se reproduise.

11 RECOURS

11.1 S'il s'avère que les renseignements personnels d'une personne ont été utilisés de façon contraire à une disposition de cette politique, cette personne peut déposer une plainte auprès de la personne à la direction générale ou du conseil d'administration d'Ex aequo si la plainte concerne la personne à la direction générale.

11.2 Comme prévu par la loi, la personne s'étant vu refuser l'accès ou la rectification des renseignements personnels la concernant peut déposer sa plainte auprès de la Commission d'accès à l'information pour l'examen du désaccord dans les 30 jours du refus d'Ex aequo d'accéder à sa demande ou de l'expiration du délai pour y répondre.

ANNEXE A : FORMULAIRE DE SIGNALEMENT

Comme prévu dans la Politique de protection des renseignements personnels, vous devez remplir ce formulaire de signalement aussitôt que vous constatez un incident de confidentialité et le remettre à la direction générale.

Les informations colligées seront versées au registre des incidents sur la confidentialité. À partir de ces informations, la direction générale décide si l'incident présente « un risque de préjudice sérieux » pour les personnes concernées et remplit une déclaration à la Commission de l'accès à l'information, si nécessaire. Des mesures pour contrôler et prévenir le type d'incident déclaré seront ensuite déployées.

Un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

Par exemple, un incident de confidentialité pourrait se produire lorsque:

- un membre de l'équipe consulte un renseignement personnel sans autorisation;
- un membre de l'équipe communique des renseignements personnels au mauvais destinataire;
- l'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

FORMULAIRE DE SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ (DOCUMENT INTERNE)

1. Date et période de l'incident de confidentialité

Date de l'incident :

Date de la découverte de l'incident :

L'incident a eu lieu sur une période de :

2. Type d'incident de confidentialité (identifier avec un "x" le type d'incident) :

☐ Accès non autorisé par la loi à un renseignement personnel

☐ Utilisation non autorisée par la loi d'un renseignement personnel

☐ Communication non autorisée par la loi d'un renseignement personnel

☐ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

3. Causes et circonstances de l'incident (identifier avec un "x" les causes ou circonstances) :

☐ Altération délibérée

☐ Communication accidentelle

☐ Communication délibérée sans autorisation

☐ Consultation non autorisée

☐ Cyberattaque (virus, logiciel espion, etc.)

☐ Défaillance technique

☐ Destruction accidentelle

☐ Destruction volontaire sans autorisation

☐ Divulgation accidentelle

☐ Divulgation délibérée sans autorisation

☐ Erreur humaine

☐ Hameçonnage (phishing)

☐ Ingénierie sociale (technique de manipulation pour obtenir des rens. pers.)

☐ Perte d'accès aux renseignements

☐ Perte de renseignements

☐ Rançongiciel

☐ Utilisation incompatible

☐ Vol de renseignements

☐ Autre, précisez :

4. Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident ?

☐ Ordinateur du bureau

☐ Ordinateur du domicile

☐ Dispositif amovible électronique

☐ Papier

☐ Clé USB

☐ Serveur

☐ CD

☐ Bande sonore

☐ Téléphone portable

☐ Infonuagique (cloud)

☐ Tablette

☐ Vidéosurveillance

☐ Ordinateur portable

☐ Photo

☐ Autre, précisez :

5. Identification des renseignements personnels visés par l'incident de confidentialité (identifier avec un x pour chaque renseignement).

☐ Nom

☐ Prénom

☐ Adresse du domicile

☐ Date de naissance

☐ Numéro de téléphone au domicile

☐ Numéro du cellulaire

☐ Adresse courriel personnelle

☐ Numéro de permis de conduire

☐ Numéro d'assurance sociale

- ☐ Numéro d’assurance maladie
- ☐ Numéro de passeport
- ☐ Salaire Fonction / occupation
- ☐ Renseignements sur des employés, ou bénéficiaires
- ☐ Renseignements médicaux
- ☐ Renseignements génétiques
- ☐ Renseignements scolaires / académiques
- ☐ Renseignements bancaires / numéro de compte / institution / placements / hypothèque
- ☐ Numéro de carte de crédit
- ☐ Numéro d’identification personnel (NIP)
- ☐ Nom du détenteur
- ☐ Code de sécurité à trois chiffres
- ☐ Numéro de carte de débit
- ☐ Numéro d’identification personnel (NIP)
- ☐ Nom du détenteur
- ☐ Autres renseignements personnels, précisez :
- ☐ Impossible de fournir une description des renseignements personnels visés

  Expliquez :

6. Personnes concernées par l’incident de confidentialité

Nombre de personnes concernées par l’incident :

Nombre de personnes concernées par l’incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l’incident selon leur lien avec l’organisation, qu’il s’agisse d’employéEs, de clientEs, autogestionnaires, partenaires, préposéEs à domicile, d’étudiantEs, d’usagers et d’usagères, de membres, de bénévoles, de fournisseurs, etc., actuelLEs ou ancienNEs :

7. Personne déclarant l’incident

Prénom, nom de la personne :

Fonction :
Moyen de communication (courriel et / ou téléphone)

ANNEXE B: DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

Je, soussignéE déclare avoir lu la Politique de protection des renseignements personnels d'Ex aequo et je m'engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité demeure même après que le lien d'emploi, de stage ou de bénévolat avec Ex aequo soit rompu.

Signé à [inscrivez le lieu] le : [inscrivez la date]

Nom en lettres moulées :

Signature :

ANNEXE C : INCIDENT DE CONFIDENTIALITÉ : PLAN DE RÉPONSE

Démarches à effectuer

Lorsqu'unE employéE ou participantE constate un incident de confidentialité, il ou elle communique avec la personne responsable de la protection des renseignements personnels par le biais d'un formulaire de signalement prévu à cette fin.

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

La personne responsable évalue si l'incident présente un risque de préjudice sérieux, selon la définition présentée à l'annexe D.

Dans le cas où l'incident présente un risque de préjudice sérieux, la direction prévient sans délai la Commission d'accès à l'information (CAI) via le formulaire prévu à cette fin et toute personne dont les renseignements personnels sont affectés.

La personne responsable tient un registre de tous les incidents.

La direction répond à la demande de la CAI d'avoir une copie du registre, le cas échéant.

ANNEXE D : INCIDENT DE CONFIDENTIALITÉ : CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES

Quand

Tel qu'indiqué à l'article 5.5 de la présente politique, un organisme doit aviser « avec diligence » toutes les personnes dont les renseignements personnels ont été touchés par un incident de confidentialité. Cet avis doit être envoyé directement aux personnes concernées. 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.

Contenu

Comme c'est le cas pour l'avis écrit à la CAI, 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'organisme a prises ou entend prendre suivant l'incident dans le but de réduire les risques de préjudice ;
- Les mesures que l'organisme suggère à la personne concernée de prendre dans le but de réduire/atténuer 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 E : INCIDENT DE CONFIDENTIALITÉ : QUESTIONNAIRE D'ÉVALUATION DU « RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »

Évaluer si l'incident présente un risque de préjudice sérieux[1]

Pour tout incident de confidentialité, l'organisation doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, entre autres :

- 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 ?**

1. Renseignements sensibles

- Documents financiers ;
- Dossiers médicaux ;
- Les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles ;
- Sauf si le contexte en fait des renseignements sensibles : nom, adresses associéES à des périodiques spécialisés ou à des activités qui les identifient.

2 Préjudice grave

- 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 ;

---

[1] [1] Le questionnaire respecte le **Règlement sur les incidents de confidentialité**

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-les- entreprises/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/

- Effet négatif sur le dossier de crédit ;
- Dommage aux biens ou leur perte ;

3 Pour déterminer la probabilité d'un mauvais usage

- Qu'est-il arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'atteinte ?
- 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 des renseignements ?
- L'intention malveillante a-t-elle été démontrée (vol, piratage) ?
- Les renseignements ont-ils été exposés à des entités ou à des personnes susceptibles de les utiliser pour causer un préjudice ou qui représentent un risque pour la réputation de la ou des personnes touchées ?

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 et éviter qu'un incident de même nature se produise à nouveau.

ANNEXE F : REGISTRE DES INCIDENTS DE CONFIDENTIALITE

Incident

Date de l’incidence

Date détection de l’incident par l’organisation

Date de transmission du formulaire de signalement

Circonstance de l’incident

Nombre de personnes visées

Évaluation de la gravité du risque de préjudice

Mesures prises en réaction de l’incident