

Politique de confidentialité

Information alimentaire populaire Centre-Sud (IAPCS) ou La Dépanne alimentaire Centre-Sud respecte le droit à la vie privée de chaque individu et s'engage à protéger la confidentialité des renseignements confidentiels recueillis auprès de tout·e participant·e ou employé·e. 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 IAPCS.



Table des matières

- DÉFINITIONS3
 - « Employé·e »3
 - « Événement »3
 - « Formulaire de rapport d'incident »3
 - « Incident de confidentialité »3
 - « Participant·e »3
 - « Publication »3
 - « Registre des incidents »3
 - « Risque sérieux de préjudices »3
 - « Renseignement confidentiel »3
 - « Service ou activité»4
- PHOTOGRAPHIES ET ENREGISTREMENTS4
- OBLIGATION DE CONFIDENTIALITÉ4
- COLLECTE ET USAGE DES RENSEIGNEMENTS CONFIDENTIELS4
- GESTION DES RENSEIGNEMENTS CONFIDENTIELS4
- CONSERVATION DES RENSEIGNEMENTS CONFIDENTIELS5
- DESTRUCTION DES RENSEIGNEMENTS CONFIDENTIELS6
- DIVULGATION DE RENSEIGNEMENTS CONFIDENTIELS À UN TIERS6
- COMMUNICATION DE RENSEIGNEMENTS CONFIDENTIELS À LA PERSONNE CONCERNÉE6
- MANQUEMENT À L'OBLIGATION DE CONFIDENTIALITÉ7
- RECOURS7
- Annexe A: CODE DE CONDUITE POUR EMPLOYÉ·E8
- Annexe B9
- INCIDENT DE CONFIDENTIALITÉ : PLAN DE RÉPONSE9
- Annexe C10
- INCIDENT DE CONFIDENTIALITÉ : CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES10
- Annexe D11
- INCIDENT DE CONFIDENTIALITÉ : QUESTIONNAIRE D'ÉVALUATION DU11
- « RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »11

DÉFINITIONS

« Employé·e »

Toute personne qui travaille pour IAPCS moyennant rémunération, incluant les codirectrices, ainsi que toutes personnes non rémunérées (bénévole, stagiaire).

« Événement »

Tout événement que IAPCS gère ou organise.

« Formulaire de rapport d'incident »

Le formulaire mis à la disposition de tout·e employé·e ou participant·e afin d'informer la personne responsable des renseignements personnels.

« 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.

« Participant·e »

Tout individu qui fournit des renseignements confidentiels à IAPCS en lien avec la réalisation d'un Événement, la création d'une Publication, la participation à une activité ou avec l'obtention d'un Service.

« Publication »

Toute publication produite par IAPCS ou à laquelle IAPCS contribue, sous quelque forme que ce soit (verbale, écrite, audio, vidéo, informatisée ou autre).

« Registre des incidents »

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 en réaction à l'incident. Les dates pertinentes y figurent aussi : arrivée de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.

« 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 ».

« Renseignement confidentiel »

Tout renseignement fourni ou communiqué à IAPCS sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre) qui concerne un·e participant·e ou un·e employé·e et qui peut être utilisé pour l'identifier, y compris : son nom, son numéro de téléphone, son adresse, son courriel, le lien entre la personne et l'organisme, 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 les enregistrements qui ne permettent pas d'identifier un individu ne constituent pas un renseignement confidentiel relatif à cet individu.

« Service ou activité »

Tout service que IAPCS rend à un individu à la demande de celui-ci, ou toute activité à laquelle il participe.

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 les enregistrements qui permettent d'identifier un individu comme employé-e de IAPCS ne constituent pas un renseignement confidentiel relatif à cet individu.

OBLIGATION DE CONFIDENTIALITÉ

3.1

Les employé-es sont tenu-es de signer la présente politique de confidentialité avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès de IAPCS.

3.2

L'obligation de confidentialité s'applique à la durée de la relation d'un-e employé-e avec IAPCS. L'obligation de confidentialité survit à la cessation de la relation, comme il se doit.

COLLECTE ET USAGE DES RENSEIGNEMENTS CONFIDENTIELS

4.1

IAPCS peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels concernant les employé-es. 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 employé-es rémunéré-es, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.).

4.2

IAPCS peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels concernant les participant-es. La constitution de tels dossiers a pour objet de permettre à IAPCS de réaliser un Événement, une Publication, de réaliser une activité, d'analyser ses statistiques, ou de fournir un Service.

4.3

IAPCS peut seulement recueillir les renseignements confidentiels qui sont nécessaires aux fins du dossier et peut utiliser les renseignements confidentiels seulement à ces fins.

4.4

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

GESTION DES RENSEIGNEMENTS CONFIDENTIELS

5.1

La direction générale est responsable d'assurer la protection des renseignements confidentiels. La direction peut déléguer cette responsabilité en la constatant par écrit. Sur le site web principal de IAPCS, doit être indiqué sous le titre de la personne responsable, « responsable de la protection des renseignements personnels » ainsi que le moyen de la joindre.

La direction ou la personne responsable s'assure de la tenue d'un Registre des incidents de confidentialité.

5.2

Sous réserve de l'article 5.3, la direction est autorisée à accéder à tout renseignement confidentiel que détient IAPCS. Les autres employé-es sont autorisé-es à accéder aux renseignements confidentiels 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-es 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'un-e employé-e ou un-e participant-e constate un incident de confidentialité, il ou elle doit informer avec diligence la direction ou la personne responsable des renseignements personnels afin qu'il soit inscrit au Registre d'incidents. L'employé-e ou le ou la participant-e doit, pour ce faire, compléter le Formulaire de rapport d'incident, qui sera automatiquement dirigé à la direction ou à la personne responsable.

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

Doit être colligé dans le Formulaire de rapport d'incident :

- 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 direction ou la personne responsable juge 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.

Si l'incident présente un risque sérieux de préjudice, la direction ou la personne responsable 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.

CONSERVATION DES RENSEIGNEMENTS CONFIDENTIELS

6.1

Les employé-es ayant accès aux dossiers en vertu de l'article 5 s'obligent à :

- S'assurer que les renseignements confidentiels soient gardés à l'abri de tout dommage physique ou

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. Ces mots de passe doivent être modifiés deux fois par année, ainsi qu'à chaque fois que les personnes ayant accès aux dossiers concernés sont remplacées ;
- 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 l'armoire à clé à combinaison du bureau.

6.2

Lorsqu'un-e employé-e peut également, à certains égards, être qualifié-e de participant-e, les renseignements confidentiels concernant chaque titre seront conservés séparément.

6.3

Les dossiers constitués en vertu de cette politique sont la propriété du IAPCS.

DESTRUCTION DES RENSEIGNEMENTS CONFIDENTIELS

7.1

Sous réserve de l'article 7.2, les renseignements confidentiels ne sont conservés que 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 employé-es sont conservés par IAPCS.

7.3

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 IAPCS de le recontacter dans le futur. Pour plus de certitude, chaque utilisation du témoignage d'une personne doit être approuvée par celle-ci.

DIVULGATION DE RENSEIGNEMENTS CONFIDENTIELS 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 confidentiels ne peuvent être divulgués à un tiers qu'après l'obtention du consentement 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 confidentiels 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, IAPCS peut divulguer des renseignements confidentiels nécessaires à sa défense ou celle de ses employé-es contre toute réclamation ou poursuite intentée contre la IAPCS ou ses employé-es, par ou de la part d'un-e participant-e, d'un-e employé-e, ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'un-e participant-e ou d'un-e

employé-e.

COMMUNICATION DE RENSEIGNEMENTS CONFIDENTIELS À LA PERSONNE CONCERNÉE

9.1

Sous réserve de l'article 9.2, les participant-es et employé-es ont le droit de connaître les renseignements confidentiels que IAPCS a reçus, recueillis et conservés à leur sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci.

9.2

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

9.3

Une demande d'un-e participant-e ou d'un-e employé-e en lien avec l'article 9.1 doit être traitée dans un délai maximal de 30 jours.

MANQUEMENT À L'OBLIGATION DE CONFIDENTIALITÉ

10.1

Un-e employé-e manque à son obligation de confidentialité lorsque cette personne :

- communique des renseignements confidentiels à des individus n'étant pas autorisés à y avoir accès ;
- discute de renseignements confidentiels à l'intérieur ou à l'extérieur de IAPCS alors que des individus n'étant pas autorisés à y avoir accès sont susceptibles de les entendre ;
- laisse des renseignements confidentiels 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 contrat de travail ou de toute autre relation avec IAPCS, seront prises à l'égard de la partie contrevenante et des mesures correctives seront adoptées au besoin afin de prévenir qu'un tel scénario ne se reproduise.

RECOURS

11.1

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

11.2

Comme prévu par la loi, la personne s'étant vu refuser l'accès ou la rectification des renseignements confidentiels 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 de IAPCS d'accéder à sa demande ou de l'expiration du délai pour y répondre.

Annexe A

INCIDENT DE CONFIDENTIALITÉ : PLAN DE RÉPONSE

Démarches à effectuer

Lorsqu'un·e employé·e ou participant·e constate un incident de confidentialité, il ou elle communique avec la codirection ou la personne responsable par le biais d'un Formulaire de rapport d'incident prévu à cette fin.

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

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

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

La direction ou la personne responsable tient un registre de tous les incidents.

La direction ou la personne responsable répond à la demande de la Commission d'accès à l'information d'avoir une copie du registre, le cas échéant.

Annexe B

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, dont lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisme ou d'accroître le préjudice causé aux personnes concernées.

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 C

INCIDENT DE CONFIDENTIALITÉ : QUESTIONNAIRE D'ÉVALUATION DU « RISQUE SÉRIEUR 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, notamment :

1. Quelle est la **sensibilité** des renseignements concernés ?
2. Quelles sont les **conséquences appréhendées** de leur utilisation ?
3. 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 (nom, adresse) ;
 - Sauf si le contexte en fait des renseignements sensibles, ou
 - Des dates de naissance (incluant l'année) en combinaison avec le reste des coordonnées.

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 ;
- 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 d'accès à l'information 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.

¹ ¹ Le questionnaire respecte le [Règlement sur les incidents de confidentialité](#)