Groupe Inter-Action Travail

POLITIQUE DE CONFIDENTIALITÉ

Cadre d’application de la Loi 25

22 SEPTEMBRE 2023

TABLE DES MATIERES

DÉFINITIONS

« Employé(e) »
Toute personne qui travaille pour le Groupe Inter-Action Travail (**GIAT**) moyennant une rémunération, incluant la direction, ainsi que toutes les personnes non rémunérées (bénévole, stagiaire).

« Événement »
Tout événement organisé et / ou géré par le GIAT.

« Formulaire de d'évènement (signalement) »
Le formulaire mis à la disposition des membres du personnel ou des participants 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 au GIAT en lien avec la prestation d'un service, la participation à un évènement ou à une activité, qui peut être pris en considération pour la création d'une publication.

« Publication »
Toute publication produite par le GIAT ou à laquelle cette même organisation contribue, sous quelque forme que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre).

« 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 en réaction 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.

« 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 au GIAT 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, son genre, son orientation sexuelle et toute information concernant sa santé.

De façon plus précise :

- 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.

« Service ou activité »
Tout service que le GIAT 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 enregistrements qui permettent d'identifier un individu comme employé(e) du GIAT ne constituent pas un renseignement confidentiel relatif à cet individu.

OBLIGATION DE CONFIDENTIALITÉ

3.1
Les employé(e)s sont tenus de signer les présentes ententes de confidentialité (Annexe A) avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès du GIAT.

3.2
L'obligation de confidentialité s'applique à la durée de la relation d'un(e) employé(e) avec le GIAT et survit à la fin de cette relation.

COLLECTE ET USAGE DES RENSEIGNEMENTS CONFIDENTIELS

4.1
Le GIAT peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels concernant les employés(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(e)s rémunérés, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.).

4.2
Le GIAT peut, au besoin, constituer un ou des dossiers contenant des renseignements confidentiels concernant les participants(es). La constitution de tels dossiers a pour objet de permettre au GIAT de réaliser un événement, une publication, une activité ou de fournir un service.

4.3
Le GIAT 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. Dans ce cas précis, un consentement verbal ou écrit doit avoir été obtenu au préalable par la personne concernée.

GESTION DES RENSEIGNEMENTS CONFIDENTIELS

5.1
La direction, comme personne exerçant la plus haute autorité dans l'organisation, est la personne responsable d'assurer la protection des renseignements personnels. La direction peut déléguer cette responsabilité en la constatant par écrit. Sur le principal site web du GIAT doit être indiqué, sous l'onglet « Nous joindre », une personne responsable de la protection des renseignements personnels (RPRP) ainsi que les coordonnées pour 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 le GIAT. Les autres employé(e)s sont autorisés 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 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.

5.4
Lorsqu'une personne (membre du personnel ou non) constate un incident de confidentialité, elle doit informer avec diligence la direction ou la personne responsable de la protection des renseignements confidentiels afin qu'il soit inscrit au registre. L'employé(e) ou le ou la participant(e) doit, pour ce faire, compléter un formulaire de signalement et l'acheminer ensuite 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 consolidé 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 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.

5.6
Seule la personne responsable du dossier de défense individuelle est autorisée à accéder aux renseignements confidentiels que le GIAT détient dans le cadre de ce service. La direction de GIAT peut toutefois y accéder dans la mesure où cela est nécessaire et convenu dans les documents balisant le service individualisé.

CONSERVATION DES RENSEIGNEMENTS CONFIDENTIELS

6.1
Les employé(e)s 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 et dans un lieu où l'accès est 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 des endroits sûrs.

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 Groupe Inter-Action Travail.

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 que les données y figurant ne puissent plus être reconstituées.

7.2
Les dossiers concernant les employés(es) sont conservés par le GIAT.

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 au GIAT 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 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 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, le GIAT peut divulguer des renseignements confidentiels nécessaires à sa défense ou celle de ses employé(e)s contre toute réclamation ou poursuite intentée contre le GIAT ou ses employé(e)s, 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(e)s et employé(e)s ont le droit de connaître les renseignements confidentiels que le GIAT a reçus, recueillis et conserve à leur sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci. Il se pourrait que dans une telle situation, une demande par écrite soit requise.

9.2
Le GIAT 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 membre du personnel 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 du GIAT 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 le GIAT, 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 GIAT, ou du conseil d'administration de ce dernier, si la plainte concerne la direction générale.

11.2
Comme prévu par la loi, la personne s'étant vu refuser l'accès ou la rectification des renseignements confidentiels la concernant après avoir fait sa demande en règle par écrit, 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 GIAT d'accéder à sa demande ou de l'expiration du délai pour y répondre.

CONCLUSION

Le Groupe Inter-Action Travail (GIAT) respecte le droit à la vie privée de chaque personne et s'engage à protéger la confidentialité des renseignements confidentiels recueillis auprès de tout individu qu'il soit employé, prestataire d'un ou plusieurs services, partenaire, collaborateur ou autre. 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 GIAT. La rédaction de ce document a été réalisée avec minutie, en consultant des documents fournis et / ou partagés par d'autres organisations, partenaires, collaborateurs, regroupements et autres. La Politique de confidentialité de GIAT a pour but de garantir la protection de la vie privée des individus et de se conformer aux obligations légales en matière de protection des renseignements personnels.

Adoptée par le Conseil d'administration du Groupe Inter-Action Travail le 25 septembre 2023

Résolution : 25/09/2023/266

Annexe A : DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

Je déclare avoir lu la Politique de confidentialité du GIAT et je comprends l'importance d'assurer la protection des renseignements personnels auxquels j'ai accès dans le cadre de mon travail. Je m'engage à en respecter les termes.

Nom : _____

Signé à Alma, le _____ / _____ / 20_____

Signature

Annexe B **:** INCIDENT DE CONFIDENTIALITÉ

PROCÉDURE DE GESTION DES INCIDENTS DE SÉCURITÉ ET VIOLATION DES RENSEIGNEMENTS PERSONNELS

Démarches à effectuer

Lorsqu'un employé(e) ou participant(e) constate un incident de confidentialité, il ou elle communique avec la direction ou la personne responsable par le biais d'un formulaire d'incident 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 ou la personne responsable, 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 ou la personne responsable répond à la demande de la CAI d'avoir une copie du registre, le cas échéant.

Annexe C **:** 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, entre autres, 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 D **:** INCIDENT DE CONFIDENTIALITÉ

QUESTIONNAIRE D'ÉVALUATION DU « RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »

Évaluer si l'incident présente un risque de préjudice sérieux

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 : nom, adresses associées à des périodiques spécialisés ou à des activités qui les identifient.

2. Préjudice grave

- 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 ;
- Humiliation.

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 E : PROCÉDURE DE CONSERVATION ET DE DESTRUCTION

PROCÉDURE DE CONSERVATION, DE DESTRUCTION ET D'ANONYMISATION DES RENSEIGNEMENTS PERSONNELS

1.Aperçu

Un fichier contenant l'inventaire des renseignements personnels a été mis en place afin de répertorier convenablement l'éventail de tous les renseignements personnels détenus par l'organisation. Ce fichier détaillé se divise :

- **En trois groupes d'individus**
  - Équipe de travail-membres du personnel ;
  - Membres du conseil d'administration ;
  - Participants / clients.
- **En quatre sections**
  - Le cycle de vie d'un renseignement personnel (collecte / utilisation / communication / conservation / destruction) ;
  - La liste des comptes / systèmes d'exploitation ;
  - L'inventaire des renseignements personnels ;
  - La liste des rôles et des accès.

2.Objectif

Le but de cette procédure est de garantir la protection de la vie privée des individus et de se conformer aux obligations légales en matière de protection des renseignements personnels.

3.Portée

La portée couvre l'ensemble du cycle de vie des renseignements personnels, depuis leur collecte jusqu'à leur destruction, conformément aux exigences légales et aux bonnes pratiques en matière de protection de la vie privée.

4.Définition

Renseignements personnels : *Toute information permettant d'identifier, directement ou indirectement, une personne physique.*
Conservation : *Stockage sécurisé des renseignements personnels pendant la durée requise.*
Destruction : *Suppression, élimination ou effacement définitif des renseignements personnels.*
Anonymisation : *Processus de modification des renseignements personnels de manière à ne plus permettre en tout temps et de façon irréversible l'identification, directe ou indirecte, des individus concernés*.

La durée de conservation pour chacune des catégories mentionnées plus haut a été établie à :

- 7 ans après la fin d'emploi pour les membres du personnel ;
- 7 ans pour les membres du CA, après la fin de leur mandat ;
- 7 ans pour les clients, après la fin de leur participation.

Pour plus de détails, se référer à l'inventaire complet des renseignements personnels détenus, tel que pour les méthodes et endroits de stockage sécurisés.

La destruction des renseignements personnels sur papier est faite par déchiquetage, au fur et à mesure, si la nécessité de les conserver n'est pas requise. Pour les renseignements numériques, ils sont supprimés des appareils, des serveurs et des outils infonuagiques, selon le calendrier établi. Chaque année et selon le calendrier établi, un inventaire (par date) des boîtes (sous clé) à détruire est fait et la destruction est alors confiée au Groupe Coderr.

Une preuve de ramassage est remise au GIAT (date de collecte) et une confirmation de destruction par la suite est également envoyée au GIAT, de la part de l'organisation en charge de la destruction. Aucun renseignement personnel ne peut donc être récupéré ou reconstitué à la suite de cette minutieuse démarche.

L'anonymisation des renseignements personnels ne se fait que pour les documents conservés à titre d'exemple, pour référence future. L'utilisation des CV à des fins sérieuses et légitimes est essentielle, car elle permet d'économiser beaucoup de temps aux intervenant(e)s lors de la conception. De pouvoir se référer à un document similaire en guise de modèle pour des descriptions d'emploi ou des compétences en lien avec le poste est primordial, d'où l'importance d'anonymiser les CV de clients, une fois le délai de conservation expiré.

La formation et la sensibilisation du personnel est régulière. L'organisme procède constamment à des rappels et communique tout changement ou toute mise à jour en lien avec les procédures de la protection des renseignements personnels, ainsi que les risques liés à la violation de la vie privée.

Cela inclut également la sensibilisation du personnel aux bonnes pratiques de sécurité des données et à l'importance de respect des procédures établies.

PROCÉDURE DE DEMANDE D'ACCÈS AUX RENSEIGNEMENTS PERSONNELS ET DE TRAITEMENT DES PLAINTES

DÉMARCHES À EFFECTUER POUR UNE DEMANDE D'ACCÈS

1- Soumission de la demande : L'individu qui souhaite accéder à ses renseignements personnels doit soumettre une demande écrite au responsable de la protection des renseignements personnels de l'organisation (RPRP). La demande peut être envoyée par la poste ou par courriel.

La demande doit clairement indiquer qu'il s'agit d'une demande d'accès aux renseignements personnels et fournir des informations suffisantes pour identifier l'individu et les renseignements recherchés.

2- Réception de la demande : La personne responsable accuse réception de la demande en guise de confirmation. La demande devra être traitée dans les trente (30) jours suivant sa réception.

3- Vérification de l'identité : Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable. Cela peut être fait en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.

Si l'identité ne peut pas être vérifiée de manière satisfaisante, le GIAT peut refuser de divulguer les renseignements personnels demandés.

4- Réponse aux demandes incomplètes ou excessives : Si une demande est incomplète ou excessive, le RPRP communique avec l'individu pour demander des informations supplémentaires ou clarifications. L'organisation se réserve le droit de refuser une demande si elle est manifestement abusive, excessive ou non justifiée.

5- Traitement de la demande : Une fois l'identité vérifiée, le RPRP procède à la collecte des renseignements demandés, afin de traiter les demandes. Le RPRP consulte les dossiers pertinents pour recueillir les renseignements personnels demandés en veillant à respecter les restrictions légales éventuelles.

6- Examen des renseignements : Avant de communiquer les renseignements à l'individu, le RPRP examine attentivement les informations pour s'assurer qu'elles ne contiennent pas de renseignements tiers confidentiels ou susceptibles de porter atteinte à d'autres droits. Si c'est le cas, il se pourrait que de tels renseignements peuvent être dissociés ou exclus de la divulgation.

7- Communication des renseignements : Une fois les vérifications terminées, les renseignements personnels sont communiqués à l'individu dans un délai raisonnable, conformément aux exigences légales en vigueur. Les renseignements doivent être communiqués par voie électronique chiffrée, par courrier postal sécurisé ou en personne, selon les préférences de l'individu et les mesures de sécurité appropriées.

8- Suivi et documentation : Toutes les étapes du processus de traitement de la demande d'accès aux renseignements personnels doivent être consignées de manière précise et complète. Les détails de la demande, les actions entreprises, les décisions prises et les dates correspondantes doivent être enregistrées dans un registre de suivi de demandes d'accès.

- Date de réception de la demande ;
- Date de l'accusé de réception ;
- Date de vérification de l'identité ;
- Méthode de vérification de l'identité ;
- Décision : demande acceptée ou refusée ;
- Date de la communication des renseignements (si applicable).

9- Protection de la confidentialité : Tout le personnel impliqué dans le traitement des demandes d'accès aux renseignements personnels doit respecter la confidentialité et la protection des données.

10- Gestion **des plaintes et recours** : Si un individu est insatisfait de la réponse à sa demande d'accès aux renseignements personnels, il doit être informé des procédures de réclamation et des recours disponibles devant la Commission d'accès à l'information (CAI). Les plaintes doivent être traitées conformément aux politiques et procédures internes en matière de gestion des plaintes (section suivante).

DÉMARCHES À EFFECTUER POUR LE TRAITEMENT DES PLAINTES

1- Réception des plaintes : Les plaintes peuvent être déposées par écrit, par téléphone, par courrier électronique ou tout autre moyen de communication officiel. Elles doivent être enregistrées dans un registre centralisé, accessible uniquement au personnel désigné. Les employés doivent informer immédiatement le RPRP dès la réception de la plainte.

2- Évaluation préliminaire : Le RPRP examine chaque plainte pour évaluer sa pertinence et sa gravité. Les plaintes frivoles, diffamatoires ou sans fondement évident peuvent être rejetées. Toutefois, une justification doit être fournie au plaignant.

3- Enquête et analyse : Le RPRP mène une enquête approfondie en collectant des preuves, en interrogeant les parties concernées et en recueillant tous les documents pertinents. Le responsable doit être impartial et avoir l'autorité nécessaire pour résoudre la plainte. Il doit maintenir la confidentialité des informations liées à la plainte et veiller à ce que toutes les parties impliquées soient traitées équitablement.

4- Résolution de la plainte : Le responsable et la direction proposent des solutions appropriées pour résoudre la plainte dans les meilleurs délais. Les solutions peuvent inclure des mesures correctives, des compensations financières ou toute autre action nécessaire pour résoudre la plainte de manière satisfaisante.

5- Communication avec le plaignant : Le RPRP communique régulièrement avec le plaignant pour le tenir informé de l'avancement de l'enquête et de la résolution de la plainte. Toutes les communications doivent être professionnelles, empathiques et respectueuses.

6- Clôture de la plainte : Une fois la plainte résolue, le RPRP doit fournir une réponse écrite au plaignant, résumant les mesures prises et les solutions proposées. Toutes les informations et documents relatifs à la plainte doivent être conservés dans un dossier confidentiel et être inscrites au registre des plaintes.

Annexe G : PROCÉDURE DE DEMANDE DE SUPPRESSION

PROCÉDURE DE DEMANDE DE DÉSINDEXATION ET DE SUPPRESSION DES RENSEIGNEMENTS PERSONNELS

1- Réception des demandes : Les demandes de désindexation et de suppression des renseignements personnels doivent être reçues par le RPRP.

Les clients peuvent soumettre leurs demandes par courriel, par téléphone ou par la poste.

2- Vérification de l'identité : Avant de traiter la demande, l'identité de l'individu doit être vérifiée de manière raisonnable. Cela peut être fait en demandant des informations supplémentaires ou en vérifiant l'identité de l'individu en personne.

Si l'identité ne peut pas être vérifiée de manière concluante, le GIAT peut refuser de donner suite à la demande.

3- Évaluation des demandes : Le RPRP doit examiner attentivement les demandes et les renseignements personnels concernés pour déterminer leur admissibilité à la désindexation ou à la suppression. Les demandes doivent être traitées de manière confidentielle et dans le respect des délais prévus.

4- Raisons d'un refus : Il existe aussi des raisons parfaitement valables pour lesquelles nous pourrions refuser de supprimer ou de désindexer des renseignements personnels :

- Pour continuer à fournir des services au client ;
- Pour des raisons d'exigence du droit au travail / gouvernementales / légales ;
- Pour des raisons juridiques en cas de litige.

5- Désindexation ou suppression des renseignements personnels : Le RPRP doit prendre les mesures nécessaires pour désindexer ou supprimer les renseignements personnels conformément aux demandes admissibles.

6- Communication du suivi : Le RPRP est chargé de communiquer avec les demandeurs tout au long du processus, en fournissant des confirmations d'accusé de réception et des mises à jour régulières sur l'état d'avancement de leur demande.

Tout retard ou problème rencontré lors du traitement des demandes doit être communiqué aux demandeurs avec des explications claires.

7- Suivi et documentation : Toutes les demandes de désindexation et de suppression des renseignements personnels ainsi que les actions entreprises pour y répondre, doivent être consignées dans registre et un système de suivi dédié à ces demandes.

Les renseignements doivent inclure les détails des demandes, les mesures prises, les dates et les résultats des actions effectuées.

Annexe H : **PROCÉDURE DE GESTION DU ROULEMENT DU PERSONNEL**

1- **Entrevue de départ ou mise à pied** : Récupérer les clés et désactiver l'accès de l'employé à tous les systèmes, y compris le système d'alarme. Suivre la procédure inscrite sur la liste (style checklist) « Information à traiter lors de l'accueil et du départ » lors de l'arrivée d'un nouvel employé ou au moment du départ d'un membre du personnel, afin de ne rien oublier. Cette liste est disponible dans le dossier administration du SharePoint :

ADMINISTRATION/DOSSIERS/GÉNÉRAUX/NOUVEAUX EMPLOYÉS/Liste pour accueil et départ .docx

Supprimer les données professionnelles des appareils appartenant aux employés, ainsi que les comptes de messagerie de son téléphone.

S'assurer que l'employé ne détienne aucune information ne lui appartenant pas en sa possession et qu'il retourne tout équipement appartenant à l'organisation, tels que l'ordinateur, le téléphone, la papeterie, les outils de travail, etc.

Compiler une liste de tous les emplacements où l'employé a stocké des données professionnelles, y compris les plateformes de stockage infonuagiques.

2- Téléphone : S'assurer que le numéro de téléphone de l'employé n'est pas transféré à un numéro externe et que la boîte vocale de bureau n'est pas transférée sur son téléphone cellulaire, s'il lui appartient.

Changer le mot de passe de la messagerie vocale, si le téléphone appartient au GIAT.

Modifier le message vocal sortant conformément aux directives de communication de GIAT.

Désigner une personne pour surveiller la messagerie vocale jusqu'à ce que ce numéro de téléphone puisse être supprimé ou réaffecté.

3- Accès aux courriels : Idéalement, ne jamais supprimer le courriel d'un employé. La bonne pratique serait de créer une boîte de courriel partagée et de bloquer les accès tel que mentionné plus bas.

Modifier le mot de passe du compte dans le système de courriel de GIAT. Si l'employé a utilisé un téléphone cellulaire pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie si ce n'est déjà fait.

Créer un message d'absence pour le compte de messagerie conformément aux directives de communication de GIAT.

Supprimer l'employé des listes de diffusion de courriels internes et des listes de courriels spécialisés. S'assurer que quelqu'un d'autre est membre pour ne pas manquer ces communications.

Contacter les partenaires, fournisseurs, collaborateurs avec lesquels l'employé a travaillé pour les informer du départ et leur fournir les coordonnées d'un nouveau contact.

Désigner quelqu'un et lui donner accès pour surveiller le courrier électronique de l'employé. Déterminer combien de temps la boîte restera disponible (entre un et douze mois), selon le poste, après quoi le compte sera supprimé. S'assurer de faire le suivi après la période établie.

4- Accès au réseau et/ou au Cloud : Supprimer l'employé de tous les groupes de contrôle d'accès pour la connexion au domaine de l'organisation, VPN, bureau à distance, système d'organisation et autres en lien avec le GIAT et ses partenaires (SIP, LGEstat, etc.).

Déplacer tous les fichiers de travail qui ont pu être stockés en dehors des dossiers de sauvegarde principaux et de l'organisation vers un emplacement central.

Révoquer l'accès de l'employé au compte de stockage infonuagique de GIAT. Supprimer les fichiers de travail de tout compte de stockage personnel.

Passer en revue les règles d'accès au pare-feu pour confirmer que l'utilisateur ne dispose d'aucun autre accès, tel qu'un VPN direct depuis son pare-feu personnel à la maison.

Confirmer qu'aucun logiciel d'accès à distance n'est installé sur les appareils (LogMein ou TeamViewer), que l'employé pourrait utiliser pour accéder à l'ordinateur ou au réseau.

Ces procédures ont été rédigées à l'aide de la trousse « MESPROCÉDURES ». Cette trousse est disponible gratuitement sur sos@mesprocedures.ca et est proposée par un regroupement de trois personnes afin de fournir des modèles accessibles aux entreprises et OBNL dans le cadre de l'application de la Loi 25.
Liste des personnes ayant initié ce projet :

- *Madame Emeline Manson, CY-clic.*
- *Madame Audrey Shink, Blue Eden.*
- *Madame Stéphanie David, Dubé Latreille Avocats.*

Le GIAT tient à les remercier sincèrement!