



POLITIQUE ENCADRANT LA GOUVERNANCE DES RENSEIGNEMENTS PERSONNELS

Version 3

12 septembre 2024
Résolution # TDS-24-68

N.B. Afin de faciliter la lecture de cette présente politique, nous avons employé le masculin comme genre neutre pour désigner aussi bien les femmes que les hommes.

PRÉAMBULE

Dans l'exercice de gestion, la *Table de développement social des Collines* (TDSCO) doit recueillir, traiter et communiquer des renseignements jugés personnels. Dans ce cadre, la TDSCO désire mettre en place, en respect de la *Loi sur la protection des renseignements personnels dans le secteur privé, chapitre P-39.1*, les processus, les méthodes, les règlements, les politiques pour assurer que le recueil, le traitement, la communication, la protection et la destruction des renseignements personnels soient conformes à la législation en vigueur dans ce domaine, et ultimement, assurer l'absence de tout incident de confidentialité et dans le cas contraire avoir en place les processus nécessaires pour minimiser ou éliminer les préjudices sérieux.

OBJECTIFS DE LA POLITIQUE

La présente politique a pour objectifs :

- de respecter la *Loi sur la protection des renseignements personnels dans le secteur privé*, c. P-39.1;
- de comprendre ce qu'est un renseignement personnel;
- de protéger les renseignements personnels détenus, acquis, traités, transmis et détruits dans le cadre de notre mission en mettant en place une politique et des pratiques adéquates;
- de réagir avec efficacité et démontrer notre diligence;
- de définir clairement les responsabilités et les obligations de toutes les personnes ayant accès à ce type d'informations dans l'organisme;
- d'établir les actions à entreprendre dans le cas d'un risque d'incident de confidentialité avec ou sans préjudice sérieux;
- d'établir les règles de conservation des renseignements personnels;
- d'établir les modes de destructions sécuritaires de renseignements personnels.

PORTÉE

La présente politique s'applique à l'ensemble du personnel de la TDSCO, ainsi qu'aux administrateurs du conseil d'administration, notamment dans :

- les lieux de travail;
- tout autre endroit où les personnes doivent se trouver dans le cadre de leur emploi (p. ex., réunion, formation, déplacement, activité sociale organisée par l'employeur);
- les communications par tout moyen technologique ou autres.

CADRE JURIDIQUE

La présente politique repose sur les lois suivantes :

- la *Loi sur la protection des renseignements personnels dans le secteur privé*, c. P-39.1;
- *Loi concernant le cadre juridique des technologies de l'information*, art. 44 et 45;
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, art. 122, 123, 134.2;
- ainsi qu'aux autres lois, règlements et normes qui y sont associés.

DÉFINITIONS

Anonymiser : Processus irréversible par lequel les renseignements personnels sont traités de manière à rendre impossible l'identification directe ou indirecte de la personne concernée.

Dépersonnalisation : Processus qui consiste à rendre un renseignement incapable d'identifier directement la personne concernée.

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

Liste nominative : Noms, numéros de téléphone, adresses géographiques de personnes physiques ou d'adresses technologiques où une personne physique peut recevoir de la communication d'un document ou d'un renseignement technologique.

Personne concernée : Personne physique qui est concernée par des renseignements personnels qui permettent, directement ou indirectement, de l'identifier.

Préjudice sérieux : Un préjudice du fait de la sensibilité des renseignements personnels, des conséquences de leur utilisation et de la probabilité qu'ils soient utilisés, lequel peut être préjudiciable envers la personne concernée.

Renseignement personnel : Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier, p. ex., motif d'absence, feuille de temps, diplôme, CV, dossier disciplinaire, situation sociale ou familiale, information nominale (y compris l'adresse courriel), etc. Les coordonnées d'affaires ne sont pas considérées comme un renseignement personnel au sens de la *Loi*.

Renseignement personnel sensible : Lorsqu'il suscite un haut degré d'attentes raisonnables en matière de vie privée, en raison de sa nature ou du contexte de son utilisation, p. ex., médical, biométrique (caractéristiques morphologiques, comportementales, biologiques), intime (santé, orientation sexuelle, groupe ethnique, état des finances, croyances philosophiques ou religieuses).

PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Ce responsable est la personne physique de qui relèvent les responsabilités de l'application et du respect de la *Loi*. La direction générale est désignée responsable par défaut à moins que le conseil d'administration ne délègue, par résolution, cette responsabilité à une autre personne.

Le formulaire de Désignation et engagement de la personne responsable de la protection des renseignements personnels est disponible dans l'Annexe 1.

RÔLE ET RESPONSABILITÉS DE LA PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS TOUT AU LONG DU CYCLE DE VIE DES RENSEIGNEMENTS PERSONNELS

La personne responsable de la protection des renseignements personnels est la direction générale de la *TDSCO*. Elle doit :

- produire et mettre en place une politique et des pratiques qui encadrent la gouvernance des renseignements personnels;
- faire l'inventaire des renseignements personnels détenus afin d'en connaître la nature et évaluer leur sensibilité;
- réaliser les évaluations des facteurs relatifs à la vie privée (ÉFVP) lequel est un processus servant à déterminer l'incidence que pourrait avoir un programme ou un service sur la vie privée d'une personne;
- savoir qui peut avoir accès à ces renseignements personnels, s'assurer que les accès sont exigés dans le cadre de leurs fonctions;
- sensibiliser et former le personnel et les administrateurs;
- appliquer ou faire appliquer les politiques et pratiques en matière de renseignements personnels;
- détenir, traiter et communiquer les renseignements personnels selon les règles édictées par la *Loi*;
- mettre en place des mesures pour prévenir ou limiter les conséquences d'un incident de confidentialité impliquant un renseignement personnel;
- assurer la gestion des incidents de confidentialité et tenir un registre de ces derniers.

RÔLE ET RESPONSABILITÉS DES PERSONNES AYANT ACCÈS À CE TYPE D'INFORMATION

Toutes les personnes ayant accès à ce type d'information, peu importe leur statut, ont la responsabilité de protéger et d'utiliser à bon escient les renseignements personnels accessibles dans le cadre du travail tout au long du cycle de vie des renseignements personnels. Les administrateurs ont la même responsabilité dans le cadre de l'accès aux documents relatifs à la personne morale.

En aucun temps, l'employé ou l'administrateur ne recueillera, ne consultera, ne transmettra ou ne détruira des renseignements personnels sans avoir au préalable reçu la permission du responsable de la protection des renseignements personnels ou en cas d'absence, de son remplaçant (Annexe 1).

La collecte de renseignements personnels doit se faire en respectant les 3 éléments suivants:

- obtenir le consentement de la personne concernée;
- être en mesure de démontrer la nécessité de la cueillette de renseignements
- procéder uniquement par cueillette directe auprès de la personne concernée.

Le non-respect de ces obligations pourrait engager un processus disciplinaire pouvant se traduire par un congédiement pour un employé et une destitution pour un administrateur.

SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS RECUEILLIS PAR LA TECHNOLOGIE DE L'INFORMATION

Technologie de l'information

La *TDSCO* utilise les technologies de l'information pour supporter ses opérations. Les renseignements personnels recueillis servent à offrir des services conformes aux attentes des personnes concernées et à la déclaration des services de la *TDSCO*. Tous les renseignements personnels qui sont collectés sont conservés dans un environnement sécurisé en respectant les obligations imposées par la *Loi*.

Personnes concernées

Toutes les personnes concernées ont l'obligation de suivre les indications prévues dans la présente politique et d'agir en tout temps pour préserver la sécurité des renseignements personnels recueillis par la technologie de l'information, détenus et traités par la *TDSCO*. Comme prévu à la politique, la *TDSCO* met en place des mesures de sécurité et de gestion adéquate, utiles et nécessaires, selon le niveau de sensibilité des renseignements personnels recueillis et traités par la technologie de l'information.

Accès aux renseignements personnels recueillis par la technologie de l'information

L'accès aux renseignements personnels obtenus par la technologie de l'information sera limité aux seules personnes ayant la qualité pour les recevoir au sein de la *TDSCO* lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

Identification, localisation et profilage

Dans le cas où la *TDSCO* aurait eu recours à une technologie comprenant des fonctions permettant d'identifier, de localiser ou de profiler, il est entendu que la personne concernée sera informée au préalable :

- du recours à une telle technologie;
- des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.

UTILISATION DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels ne peuvent être utilisés que pour la raison pour laquelle ils ont été collectés. Dans le cas où les renseignements personnels seraient utilisés à une autre fin, l'autorisation de la personne concernée devra être donnée avant l'utilisation des renseignements personnels.

Comme il est prévu à la *Loi*, la collecte des renseignements personnels donne l'autorisation à la personne concernée d'utiliser les renseignements collectés. Spécifiquement, les limites de l'utilisation des renseignements personnels sont les suivantes :

- limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de l'organisation lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions;
- limiter l'utilisation des renseignements personnels. À moins d'une exception prévue par la *Loi*, le consentement doit être obtenu de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli (annexe 2).

Sécurité lors de l'utilisation

Pendant l'utilisation des renseignements personnels, la personne qui en fait usage doit obligatoirement en assurer la protection. La personne doit, sans s'y restreindre :

- ne pas donner accès aux renseignements personnels à une personne qui n'y est pas autorisée;
- dans le cas où la personne qui utilise les renseignements personnels quitte temporairement son espace de travail, les renseignements personnels doivent être disposés de manière à ne pas être à la vue des passants :
 - les renseignements personnels doivent être rangés dans un endroit barré;
 - l'écran de l'ordinateur doit être verrouillé;
- lors de discussions traitant de renseignements personnels, celles-ci doivent se faire dans un lieu privé où la discussion ne peut être entendue par les personnes qui n'ont pas l'autorisation d'y avoir accès.

COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

Avant toute communication, qu'elle soit verbale ou écrite et par tous les moyens (téléphone, courriel, texto, lettre, rapport, site Internet, etc.), le consentement de la personne concernée est nécessaire sauf dans les cas prévus à la *Loi*.

Spécifiquement, les obligations suivantes doivent être respectées :

- obtenir le consentement des personnes concernées pour communiquer leurs renseignements à un tiers (p. ex., assureur ou prestataire de services), à moins d'une exception prévue par la *Loi*;
- respecter la règle du consentement à la communication;
- respecter les obligations prévues par la *Loi* lorsque la personne communique des renseignements personnels sans le consentement de la personne concernée;
- respecter les obligations particulières applicables à la communication de renseignements personnels à l'extérieur du Québec.

L'autorisation de collecter et d'utiliser les renseignements personnels ne permet pas la communication à un tiers des renseignements en question.

La personne concernée devra remplir et signer le *Formulaire pour le consentement à la communication de renseignements personnels* (Annexe 3).

DANS QUELS CAS FAIRE UNE ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (ÉFVP)?

Vous devez faire une ÉFVP dans les cas suivants :

- un projet d'acquisition, de développement et de refonte de système d'information;

- de prestation électronique de services impliquant des renseignements personnels soit la collecte, l'utilisation, la communication, la conservation ou la destruction de ces renseignements;
- avant de communiquer un renseignement personnel à l'extérieur du Québec.

La procédure détaillée peut être consultée en cliquant sur ce lien :

https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf

TRAITEMENT DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Traitement des plaintes

Le traitement adéquat, uniforme et diligent des plaintes est une priorité à la *TDSCO*. Toute personne insatisfaite du processus de collecte, d'utilisation, de communication ou de destruction de renseignements personnels peut déposer une plainte à la personne responsable de la protection des renseignements personnels.

Processus de traitement d'une plainte

Dans le cas où une plainte est déposée, la personne responsable de la protection des renseignements personnels doit suivre les étapes prévues à la *Procédure de traitement d'une plainte* (Annexe 4). Elle bénéficie de 30 jours pour le faire. Les étapes suivantes devront être suivies :

- a) Réception de la plainte;
- b) Analyse de la recevabilité;
- c) Si la plainte est non recevable : lettre à la personne plaignante et arrêt du processus;
- d) Si la plainte est recevable : lettre à la personne plaignante et enquête;
- e) Enquête;
- f) Résultat de l'enquête;
- g) Avis écrit à la personne plaignante sur le résultat de l'enquête;
- h) Mise en place des solutions.

La personne responsable prendra toutes les actions pour protéger au maximum les renseignements personnels détenus, traités et communiqués.

Mesures de sécurité

La personne responsable de la protection des renseignements personnels devra mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits pendant le processus de traitement des plaintes.

Ces mesures sont raisonnables compte tenu notamment de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

CONSERVATION DES RENSEIGNEMENTS PERSONNELS

La responsable de la protection des renseignements personnels verra à la conservation des renseignements personnels. La conservation consiste en la période pendant laquelle sont conservés les renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

Règles de conservation

Il s'agit spécifiquement :

- d'assurer la mise à jour et l'exactitude des renseignements personnels détenus au moment où ils sont utilisés pour une décision relative à la personne concernée;
- de mettre en place et respecter les mesures nécessaires pour assurer la sécurité des renseignements personnels;
- de conserver les renseignements personnels jusqu'à l'atteinte de la finalité pour laquelle ils ont été collectés ou selon les modalités déterminées par une loi;
- de conserver les renseignements personnels dans un endroit sécuritaire et prévu à cette fin;
- de permettre l'utilisation des renseignements personnels lorsque la finalité pour laquelle ils ont été collectés est accomplie, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la *Loi* ou par un calendrier de conservation établi par règlement du gouvernement.

Fin de la durée de conservation

À la fin de la durée de conservation des renseignements personnels, soit à l'arrivée de la finalité pour laquelle ils ont été collectés, la TDSCO s'assurera de :

- les détruire de manière sécuritaire et comme prévu à la présente politique;

ou

- les anonymiser (c'est-à-dire qu'ils ne permettent plus d'identifier la personne concernée ni d'établir un lien entre la personne concernée et les renseignements personnels), et ce de manière irréversible dans le but de les utiliser à des fins sérieuses et légitimes.

Temps de conservation

Le temps de conservation est la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé ou celui prévu dans le document *Temps de conservation des renseignements personnels* (annexe 5).

RÈGLES DE DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Moment de la destruction

La personne responsable de la protection des renseignements personnels doit s'assurer que la destruction des renseignements personnels se fasse de manière sécuritaire. De plus, si la TDSCO désire garder les renseignements personnels, la personne responsable de la protection des renseignements personnels devra en assurer l'anonymisation et l'utilisation à des fins sérieuses et légitimes.

Méthodes de destruction

Une méthode de destruction est un processus qui permet de détruire de manière permanente et irréversible des renseignements personnels. Il peut s'agir de déchiqueter, formater, réécrire, destruction physique, broyage, démagnétisation, écrasement d'information. Les pratiques sont prévues au document *Méthode de destruction de renseignements personnels* (Annexe 6).

Méthodes d'anonymisation

Une méthode d'anonymisation est un processus irréversible par lequel les renseignements personnels sont traités de manière à rendre impossible l'identification directe ou indirecte de la personne concernée.

ADOPTION ET MISE EN APPLICATION DE LA POLITIQUE

La présente politique encadrant la gouvernance des renseignements personnels a été adoptée par voie de résolution par le conseil d'administration de la TDSCO à sa séance régulière du 12 septembre 2024. Elle entre en vigueur à cette date.

La personne responsable de la protection des renseignements personnels a la responsabilité d'interpréter et d'appliquer la politique. Pour le bon fonctionnement administratif de la TDSCO et dans la mesure du maintien et du respect des politiques fixées par le conseil d'administration, la présente politique pourra être révisée ou modifiée dans le cadre de l'intégration de nouvelles mesures fixées par le conseil d'administration de la TDSCO ou par toute instance gouvernementale, afin d'y apporter les changements et précisions qui paraîtront nécessaires après sa mise en application.

Toutes les personnes ont l'obligation de signaler à la direction générale, personne responsable de la protection des renseignements personnels, ou au conseil d'administration, selon le cas, tout manquement à la politique de la TDSCO.

Signé par :

Logan Vaillant

1DD1DA4017E5480...

Monsieur Logan Vaillant
Président

DocuSigned by:

Gabrielle Simard


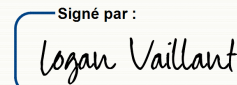
BFBFABDCECC0440...

Madame Gabrielle Simard
Secrétaire

ANNEXE 1 — DÉSIGNATION ET ENGAGEMENT DE LA PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

<p>En vertu de l'article 3.1 de la <i>Loi sur la protection des renseignements personnels dans le secteur privé</i>, toute personne qui exploite une entreprise est responsable de la protection des renseignements personnels qu'elle détient. Au sein de la <i>Table de développement social des Collines</i> (TDSCO), la direction générale veille à assurer le respect et la mise en œuvre de la présente <i>Loi</i>.</p> <p>Elle exerce la fonction de responsable de la protection des renseignements personnels; elle peut déléguer cette fonction par écrit, en tout ou en partie, à toute personne. Ses coordonnées sont publiées sur notre site Internet : www.tdsco.org</p>	
Nom de la personne responsable :	Julie Phaneuf
Titre de la personne responsable :	Directrice générale
Coordonnées :	dg@tdsco.org 873-655-8372
<p>En cas d'absence de la personne responsable de la protection des renseignements personnels, veuillez communiquer avec :</p>	
Nom de la personne remplaçante :	Logan Vaillant
Titre de la personne remplaçante :	Président
Coordonnées :	dg@laisondescollines.org

Par la présente, je déclare mon engagement à respecter et à faire respecter la présente politique et d'en assumer les responsabilités afférentes.

<p>DocuSigned by:</p>  <p>EE730FD8D714436...</p> <p>Julie Phaneuf</p> <p>Direction générale</p>	<p>18/09/2024</p> <hr/> <p>Date</p>
<p>Signé par :</p>  <p>1DD1DA4017E5486...</p> <p>Monsieur Logan Vaillant</p> <p>Président du conseil d'administration</p>	<p>18/09/2024</p> <hr/> <p>Date</p>

ANNEXE 2 — CONSENTEMENT À LA COLLECTE DES RENSEIGNEMENTS PERSONNELS

En conformité avec l'article 14 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, le présent formulaire vise à ce que le consentement de la personne concernée soit libre, éclairé et être donné à de fins spécifiques et à confirmer que le consentement qui ressort du présent formulaire ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Section 1. Identité de la personne concernée par les renseignements personnels

Prénom et nom :

Adresse :

Téléphone :

Courriel :

Section 2. Identité de la personne responsable de la protection des renseignements personnels qui demande la collecte des renseignements personnels (à compléter par la personne responsable de la protection des renseignements personnels qui demande la collecte des renseignements personnels)

Prénom et nom :

Nom de l'organisation :

Adresse de l'organisation :

Téléphone :

Courriel :

Section 3. Les renseignements personnels visés par la demande de consentement

Les renseignements personnels suivants sont visés par la demande :

3.1. Existe-t-il des renseignements personnels dans la liste précédente que vous désirez ne pas inclure dans votre consentement?

Non Oui, les suivants :

Section 4. La collecte de renseignements personnels

(à compléter par la personne responsable de la protection des renseignements personnels qui demande la collecte les renseignements personnels)

La collecte des renseignements personnels est nécessaire aux fins de (indiquer les besoins qui motivent la collecte) :

Les moyens de la collecte des renseignements personnels utilisés sont (indiquer les besoins et les moyens utilisés pour la collecte) :

Section 5. Les droits d'accès et de rectification

Pendant le processus de collecte, d'utilisation et de communication, la personne concernée a un droit d'accès et de rectification des renseignements personnels que détient (nom de l'organisation) sur son sujet. Les stipulations de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Section 6. Le droit des personnes concernées de retirer leur consentement

Pendant le processus de collecte, d'utilisation et de communication, la personne concernée a le droit de retirer son consentement en suivant les stipulations de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Section 7. Informations sur les tiers à qui pourraient être communiqués les renseignements personnels de la personne concernée selon le cas (à compléter par la personne responsable de la protection des renseignements personnels qui demande la collecte les renseignements personnels)

Il est important de mentionner qu'aucune communication des renseignements personnels de la personne concernée ne sera transmise sans l'autorisation écrite de la personne concernée en respectant les obligations prévues à la *Loi sur la protection des renseignements personnels dans le secteur privé*.

- Les renseignements personnels seront utilisés uniquement par (nom de l'organisation sous le contrôle de (nom du responsable de la protection des renseignements personnels) :

- Nom du tiers ou des catégories de tiers pour qui la collecte est faite :

- Nom des tiers à qui il est nécessaire de communiquer les renseignements :

- Il est possible que les renseignements soient communiqués à l'extérieur du Québec.

- Nom des tiers à qui pourraient être communiqués les renseignements personnels à l'extérieur du Québec :

Section 8. Durée du consentement

Ce consentement est valide, après ma signature de ce document, pour une durée de :

- Le temps nécessaire aux fins pour lesquelles il a été demandé
- Pour la durée suivante :

Une nouvelle entente devra être signée passé un délai d'un an.

Section 9. Protection des renseignements personnels

Les renseignements personnels qui seront collectés sont nécessaires aux fins de la réalisation mentionnée dans le présent formulaire. Tous les renseignements seront traités avec la plus grande discrétion et confidentialité possible. La personne responsable de la protection des renseignements personnels s'assurera à ce qu'ils soient utilisés que pour les fins pour lesquelles ils sont nécessaires.

Signature de la personne responsable de la protection des renseignements personnels

Signature

Section 10. Consentement à la collecte de renseignements personnels de la personne concernée

Par la présente signature, je confirme mon consentement manifeste, libre, éclairé et je suis informé des fins spécifiques pour lesquelles il est donné.

J'ai lu et je comprends la portée de ce document

Date

Signature de la personne concernée

ANNEXE 3 — FORMULAIRE POUR LE CONSENTEMENT À LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

(Ville et date)

(Nom du responsable)

(Coordonnées)

Objet : Consentement à la communication de renseignements personnels

Madame _____, (responsable de la protection des renseignements personnels),

Je soussigné.e , _____, consens à ce que vous , _____, (nom du responsable) au nom de la *Table de développement social des Collines-de-l’Outaouais* (TDSCO), divulguiez, communiquiez et échangeiez mes renseignements personnels pertinents contenus dans mon dossier détenu par la TDSCO aux intervenants œuvrant pour, _____, (nom de l’organisation) qui recevra les renseignements personnels).

En tout temps, je pourrai retirer mon consentement à la divulgation et à l’échange d’informations.

Signature de la personne concernée

Date

Signature de la personne faisant signer le formulaire

Date

ANNEXE 4 — PROCÉDURE DE TRAITEMENT D'UNE PLAINTE

Étapes	Délai	Interventions
[1] Réception de la plainte	Tout le processus d'enquête doit être terminé dans les 30 jours du dépôt de la plainte	Envoi d'un accusé de réception de la plainte
[2] Analyse de recevabilité L'analyse de recevabilité consiste à déterminer si, dans la mesure où toutes ou une partie des allégations de la plainte s'avéraient exactes, c'est-à-dire démontrées par preuve prépondérante, que cela pourrait constituer un manque en rapport à la gouvernance des renseignements personnels.		L'objet de la plainte est en rapport avec les renseignements personnels. La plainte vise une pratique prévue dans la politique de gouvernance. L'analyse démontre que les faits reprochés pourraient constituer un manque en rapport avec la politique de gouvernance.
[2.1] Si la plainte est non recevable		Envoi d'une lettre indiquant que la plainte n'est pas recevable
[2.2] Si la plainte est recevable, enquête		Envoi d'une lettre indiquant le début de l'enquête
[3] Enquête		Rédaction du rapport d'enquête
[4] Résultat de l'enquête		Rédaction du rapport d'enquête
[5] Avis écrit à la personne plaignante sur le résultat de l'enquête		Lettre indiquant le résultat de l'enquête et les modifications, selon le cas, qui seront mises en place
[6] Mise en place des solutions		Mise en place de modifications

ANNEXE 5 — TEMPS DE CONSERVATION DES RENSEIGNEMENTS PERSONNELS

Documents	Durée de conservation
Documents en rapport à l'équité et le maintien de l'équité salariale	6 ans à compter de l'affichage des résultats
Documents fiscaux	7 ans ou demander la permission
Documents relatifs aux formations complétées	6 ans
Documents rattachés à un litige en RH	3 ans
Dossiers de congédiement	3 ans
Registres de paie et documents relatifs	6 ans
Relevés d'emploi	6 ans *
Documents d'un processus d'embauche (questionnaire de préembauche, notes d'entrevues, tests de connaissance, etc.)	Le temps requis pour permettre au candidat non retenu d'épuiser l'ensemble des recours prévus dans la <i>Loi sur les normes du travail</i> (incluant le recours en révision et d'appel), à compter de la date de la fin du processus d'embauche
Procès-verbaux des réunions du Comité de santé et sécurité du travail	5 ans
Dossier médical du travailleur dans le cadre d'un programme de santé	Le Directeur de la santé publique doit s'assurer de la conservation du dossier médical d'un travailleur : 20 ans après la fin de son emploi ou 40 ans après le début de son emploi, selon la plus longue durée
Documents des séances du CA	Conservé indéfiniment en version papier ou électronique
Documents qui font l'objet d'une demande d'accès ou de rectification	Aucun délai, cependant, lorsqu'un renseignement personnel fait l'objet d'une demande d'accès qui est refusée par l'entreprise, il faut le conserver le temps requis pour permettre à la personne concernée d'épuiser les recours prévus à la <i>Loi</i>

* Il est fréquent que d'anciens employés demandent une confirmation d'emploi pour la reconnaissance des heures d'expérience dans le cadre d'un nouvel emploi. Afin de conserver ces données, une bonne pratique est de créer un fichier rassemblant la date d'embauche, la date de départ et le total d'heures travaillées.

ANNEXE 6 — MÉTHODE DE DESTRUCTION DE RENSEIGNEMENTS PERSONNELS

Support utilisé	Exemples de méthodes de destruction
Papier (original et toutes les copies)	Déchiqueteuse, de préférence à découpe transversale. Si le document est très confidentiel : déchiqueteuse + incinération.
Média numérique que l'on souhaite réutiliser ou recycler, p. ex., carte de mémoire flash (carte SD, XD, etc.), clé USB, disque dur d'ordinateur.	Formatage, réécriture, déchiquetage numérique (logiciel effectuant une suppression sécuritaire et qui écrira de l'information aléatoire à l'endroit où se trouvait le fichier supprimé)
Médias numériques non réutilisables, p. ex., certains CD, DVD, carte de mémoire flash, clé USB et disque dur.	Destruction physique (déchiquetage, broyage, meulage de surface, désintégration, trouage, incinération, etc.). La plupart des déchiqueteuses pourront détruire les CD et les DVD. Démagnétiseur pour les disques durs.
Machine contenant un disque dur, p. ex., photocopieur, télécopieur, numériseur, imprimante, etc.	Écrasement des informations sur le disque dur ou disque dur enlevé et détruit lorsque la machine est remplacée.