



POLITIQUE SUR LA GESTION ET LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS

Construction CYBCO

Mise à jour : 2024-02-29

TABLE DES MATIERES

1. OBJECTIFS	3
2. CHAMP D'APPLICATION	3
3. RÔLE ET RESPONSABILITÉS	3
4. DÉFINITIONS	4
5. MODALITÉS OPÉRATIONNELLES	5
6. PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	8
7. RÉVISION	9
ANNEXE 1 – CALENDRIER DE CONSERVATION	10

1. OBJECTIFS

« CONSTRUCTION CYBCO » (ci-après appelée l'entreprise) est une organisation qui recueille, utilise et divulgue des renseignements pour mener à bien sa mission. La confidentialité et le respect de votre vie privée sont importants pour nous.

La présente politique vise à démontrer les pratiques de l'organisation en matière de cueillette, d'utilisation, de divulgation et de conservation des renseignements personnels, lesquelles assurent une gestion efficace et sécuritaire de tous les renseignements personnels détenus au sein de l'entreprise, et ce, quel que soit le support utilisé.

Elle reflète la volonté de l'entreprise de se doter d'un système de gestion documentaire sécuritaire et uniforme.

Elle a également pour but d'assurer le respect des obligations législatives, tout particulièrement la *Loi sur la protection des renseignements personnels dans le secteur privé*¹ (ci-après la Loi), ainsi que la durée de conservation des différents renseignements utilisés. Elle vise également à établir un mécanisme de traitement des plaintes.

2. CHAMP D'APPLICATION

La présente politique s'applique à tous les employés de l'entreprise. Elle concerne tous les renseignements personnels, papier ou numérique, ayant une valeur administrative, financière, légale ou historique, détenus par un membre du personnel dans le cadre de ses fonctions.

La présente politique ne s'applique pas aux sites Web de tiers accessibles par des liens sur le présent site Web et l'entreprise n'est nullement responsable à l'égard des pratiques de protection des renseignements personnels de ces tiers.

3. RÔLE ET RESPONSABILITÉS

3.1. Direction générale

- 3.1.1. Déployer les ressources nécessaires à l'application de la présente politique.
- 3.1.2. Désigner et supporter le responsable de la protection des renseignements personnels.

3.2. Patrick Bellemare

- 3.2.1. Agir à titre de personne responsable de la protection des renseignements personnels.
- 3.2.2. Assurer la gestion, l'application et le respect de la présente politique.
- 3.2.3. Autoriser le transfert, le tri, la destruction ou l'archivage des renseignements personnels selon les règles du calendrier de conservation.
- 3.2.4. Gérer les demandes d'accès aux renseignements personnels.
- 3.2.5. Tenir un registre des incidents de confidentialité.

¹ Publication Québec. (2023). La Loi sur la protection des renseignements personnels dans le secteur privé. Repéré à : P-39.1 - Loi sur la protection des renseignements personnels dans le secteur privé (gouv.qc.ca)

- 3.2.6. Aviser la Commission et la personne concernée lorsqu'un incident lié à la confidentialité présente un risque de préjudice sérieux.
 - 3.2.7. Procéder à une évaluation des facteurs relatifs à la vie privée (ÉFVP) lorsque requis.
 - 3.2.8. Recevoir et traiter les plaintes relatives à la protection des renseignements personnels.
 - 3.2.9. Informer tout le personnel de la présente politique.
 - 3.2.10. Réviser, au besoin, la présente politique.
- 3.3. Firme externe – Grav-iti**
- 3.3.1. Collaborer au choix des outils informatiques nécessaires afin d'assurer le respect de la présente politique.
 - 3.3.2. Établir les mesures de sécurité requises à l'application de la présente politique.
- 3.4. Employés**
- 3.4.1. Aviser le responsable des renseignements personnels lorsqu'un incident de confidentialité survient.
 - 3.4.2. Classer et enregistrer les documents selon les bonnes pratiques en vigueur.
 - 3.4.3. Respecter la présente politique.

4. DÉFINITIONS

4.1. Calendrier de conservation

Calendrier qui détermine les périodes de conservation des renseignements personnels.

4.2. Cycle de vie

L'ensemble des étapes franchies par un renseignement personnel depuis sa cueillette, son transfert, sa consultation, sa transmission, son archivage et sa destruction.

4.3. Document

Information portée par un support papier ou numérique. Il peut s'agir ou non de renseignements personnels.

4.4. Document actif

Document consulté et utilisé à des fins administratives, financières ou légales.

4.5. Document inactif

Document qui n'a plus d'utilité administrative, financière ou légale et qui est archivé selon le calendrier de conservation.

4.6. Incident de confidentialité (*)

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.

4.7. Préjudice sérieux (*)

Gravité du risque de préjudice pour les personnes concernées par un incident de confidentialité. Pour l'évaluation, il faut considérer, notamment :

- la sensibilité des renseignements concernés ;
- les conséquences appréhendées de leur utilisation ;
- la probabilité qu'ils soient utilisés à des fins préjudiciables.

4.8. Renseignements personnels (*)

Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

4.9. Renseignements personnels sensibles (*)

Un renseignement personnel est considéré comme sensible lorsque, par sa nature notamment médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de respect de la vie privée.

4.10. Renseignements personnels dépersonnalisés (*)

Un renseignement personnel est dépersonnalisé quand il ne permet plus d'identifier directement la personne concernée. Par exemple, ces données devront être utilisées en ayant pris soin de supprimer préalablement le nom des personnes, l'adresse civique ou courriel, les numéros d'assurance sociale ou d'assurance-maladie.

Contrairement à l'anonymisation, la dépersonnalisation des renseignements personnels n'est pas une alternative à leur destruction. Elle constitue une mesure de protection de ces renseignements, notamment quand ils sont utilisés ou communiqués sans le consentement des personnes concernées, notamment à des fins d'études, de recherche ou de production de statistiques.

4.11. Renseignements personnels anonymisés (*)

Un renseignement personnel est anonymisé quand il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.

() Les définitions proviennent de la Commission d'accès à l'information du Québec*

5. MODALITÉS OPÉRATIONNELLES

5.1. Cueillette des renseignements personnels

Les articles 4 et 5 de la Loi permettent à l'entreprise de constituer un dossier sur une personne si elle a un intérêt sérieux et légitime.

Les renseignements personnels ne peuvent être utilisés que pour les fins pour lesquelles ils ont été recueillis, c'est-à-dire que leur utilisation doit avoir un lien direct et pertinent avec les fins pour lesquelles le renseignement a été recueilli au préalable. Par exemple, le NAS a été recueilli afin de traiter la paie d'un employé et ne peut être utilisé à d'autres fins.

Il est à noter que l'utilisation des renseignements personnels à d'autres fins est toutefois permise si la personne concernée y consent. À cet effet, veuillez consulter la section 5.3.

5.1.1. Photos

L'entreprise doit détenir un consentement de la personne concernée si elle détient des photos ou des vidéos permettant de l'identifier en utilisant le formulaire prescrit.

5.1.2. Vidéosurveillance

Notre entreprise utilise un système de vidéosurveillance pour **les chantiers** dont l'objectif est « d'assurer la sécurité des chantiers et de suivre l'avancement ou l'exécution des travaux à partir de la roulotte de chantier ». Les images sont consultées par les membres de l'équipe de chantier qui doivent suivre les travaux ou M. Bellemare. Cette télésurveillance se fait pour la plupart du temps en direct. Toutefois, les images sont utilisées en cas d'exception uniquement ou de possible litige.

Pour les chantiers, des images sont conservées dans la plateforme de gestion de projet Procore. L'accès à cette plateforme est sécurisé par usager et mot de passe. Les images sont entre autres utilisés pour les rapports journaliers et les inspections par l'équipe de construction CYBCO. Ceci dans le but de documenter les travaux en cours.

Notre entreprise utilise un système de vidéosurveillance pour **le bureau** dont l'objectif est « de surveiller les intrusions ». Les images sont consultées par M. Bellemare seulement en cas de vandalisme ou de vol. Les images sont conservées sur une plateforme sécurisée spécialisée. Accessible avec un code d'utilisateur et mot de passe.

La personne responsable de la gestion de la vidéosurveillance est Patrick Bellemare.

5.2. Conservation

5.2.1. Accès aux renseignements personnels

La liste des employés ayant accès aux renseignements personnels est incluse dans le document « *Inventaire des renseignements personnels* ». Certaines informations peuvent être transmises à un employé lorsqu'il a la qualité pour le connaître et à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions, conformément à l'article 20 de la Loi.

5.2.2. Classement des renseignements personnels

Les renseignements personnels détenus sous forme papier sont classés dans un bureau ou un classeur verrouillé.

Les renseignements personnels détenus sous forme numérique sont classés dans le répertoire protégé « Sharepoint / RH – Documents (1) ». Les documents incluant des données sensibles sont protégés avec des mots de passe.

5.2.3. Incident de confidentialité

Tous les incidents de confidentialité doivent être déclarés au responsable des renseignements personnels.

L'évaluation de l'incident doit être réalisée avec le formulaire « *Évaluation d'un incident de confidentialité* ».

Les incidents de confidentialité constituant un préjudice sérieux pour les personnes concernées doivent être déclarés à la Commission en utilisant le formulaire « *Avis incident de confidentialité* » prescrit par la Commission.

Les personnes visées par incident de confidentialité doivent être avisées avec la lettre « *Avis aux personnes concernées* ».

Le responsable des renseignements personnels doit consigner les incidents de confidentialité dans le *Registre des incidents de confidentialité*.

5.3. Transmission

5.3.1. Consentement

Par défaut, il faut obtenir l'autorisation requise de la personne concernée avant de transmettre un renseignement personnel à un tiers.

Le consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Donc, un renseignement personnel ne peut être utilisé à une autre fin par l'entreprise, à moins que la personne concernée n'y consente.

Ce consentement n'est pas requis si les renseignements personnels sont utilisés par les personnes citées au paragraphe 5.2.1., dans le cadre d'une transaction commerciale et lors de l'exercice d'un mandat ou l'exécution d'un contrat de service ou d'entreprise.

5.3.2. Accès aux renseignements personnels

Les employés peuvent accéder à leur renseignement personnel sur demande écrite au responsable de la protection des renseignements personnels.

5.3.3. Transmission électronique

Les renseignements personnels sensibles transmis électroniquement doivent être protégés par un mot de passe.

5.3.4. Références d'emploi

Seules les informations prévues à l'article 84 de la Loi sur les normes du travail peuvent être divulguées à l'expiration du contrat de travail. Il s'agit de la nature et de la durée de son emploi, du début et de la fin de l'exercice de ses fonctions ainsi que du nom et de l'adresse de l'employeur.

Aucune information ne doit être fournie concernant la qualité du travail ou de la conduite du salarié.

5.3.5. Processus de deuil

Il est permis de communiquer un renseignement personnel concernant une personne décédée à son conjoint ou à l'un de ses proches parents si ce renseignement est susceptible d'aider cette personne dans son processus de deuil, à moins que la personne décédée n'ait consigné par écrit son refus d'accorder ce droit d'accès.

5.3.6. Évaluation des facteurs relatifs à la vie privée (ÉFVP)

Une évaluation des risques liés à la vie privée (ÉFVP) est requise lors d'un projet impliquant des renseignements personnels et un projet risquant d'avoir une incidence sur le respect de la vie privée des personnes. L'ÉFVP consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées².

Vous trouverez ci-dessous des exemples de projets pouvant impliquer la collecte, l'utilisation ou la communication des renseignements personnels :

- Acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels;
- Communication d'un renseignement personnel à l'extérieur du Québec;
- Installer un système de vidéosurveillance
- Acquérir ou fusionner des organisations;
- Utiliser la géolocalisation, un système de reconnaissance faciale, des objets connectés, etc.
- Communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques.

5.4. Destruction

5.4.1. Généralités

Il faut détruire les renseignements personnels dès que la finalité pour laquelle ils ont été collectés est accomplie sous réserve du calendrier de conservation établi à l'annexe 1.

Dans le cas contraire, ils doivent être conservés à des fins sérieuses et légitimes, ils doivent être anonymisés.

5.4.2. Méthode de destruction

Il faut utiliser la méthode de destruction appropriée selon le support utilisé (déchiqueteuse, démagnétiseur de disque dur, formatage, destruction physique, etc.).

6. PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

- 6.1. Une plainte peut être adressée à l'entreprise par une personne concernée si elle est d'avis que la Loi sur la protection des renseignements personnels dans le secteur privé n'a pas été respectée à son égard.

La plainte doit être adressée à la personne responsable de la protection des renseignements personnels.

La personne responsable de la protection des renseignements personnels peut mandater une ressource externe pour exercer les fonctions qui lui sont dévolues au sens de la présente politique.

- 6.2. La plainte peut porter sur la cueillette, la conservation, l'utilisation, la communication ou la destruction des renseignements personnels;

² Commission d'accès à l'information. (2023). Réaliser une évaluation des facteurs relatifs à la vie privée. Repéré à : [CAI Guide EFVP](#)

- 6.3. D'abord, la personne responsable de la protection des renseignements personnels déterminera si la plainte est recevable. Elle informe la personne concernée de sa décision.
- 6.4. Si la plainte est recevable, la personne responsable de la protection des renseignements personnels fera enquête et déterminera s'il y a eu manquement aux dispositions contenues dans la Loi sur la protection des renseignements personnels dans le secteur privé. La personne responsable de la protection des renseignements personnels peut faire toutes les recommandations qu'elle estime appropriées pour régler la situation et améliorer la gestion et la protection des renseignements personnels au sein de l'entreprise. Elle communique la conclusion de son enquête à la personne concernée.
- 6.5. En cas d'insatisfaction, la personne concernée peut s'adresser à la Commission d'accès à l'information : cai.gouv.qc.ca

7. RÉVISION

La présente politique sera mise à jour annuellement par le responsable des renseignements personnels.

ANNEXE 1 – CALENDRIER DE CONSERVATION

Nature des documents	Période obligatoire	Période en vigueur
<p>Assurance collective</p>	<p>Loi sur les assurances, LRQ c A-32</p> <p>Aucune, sauf en présence de dispositions spécifiques au contrat</p>	<p>3 ans suivant la terminaison d'emploi (délai général de prescription – Code civil, article 2925)</p> <p>ou</p> <p>Plus de 3 ans dans la mesure où un litige est pendant</p>
<p>Assurance-emploi</p> <p>Relevés d'emploi, etc.</p>	<p>Loi sur l'assurance-emploi - articles 87(3) et 87(4)</p> <p>6 ans suivant la fin de l'année à l'égard de laquelle les documents en cause ont été tenus, sauf autorisation écrite du ministre de s'en départir</p> <p>ou</p> <p>jusqu'à ce qu'une décision soit rendue (y compris l'expiration de l'appel) lors d'un litige</p>	<p>7 ans</p>
<p>Comité santé et sécurité</p>	<p>Règlement sur les comités de santé et sécurité du travail, article 31</p> <p>5 ans</p>	<p>5 ans</p>
<p>Dossier employé</p> <p>Contrats d'emploi, lettres de congédiement, preuves de sanctions disciplinaires, etc.</p>	<p>Aucune période obligatoire</p>	<p>3 ans suivant la terminaison d'emploi (délai général de prescription – Code civil, article 2925)</p> <p>ou</p> <p>Plus de 3 ans dans la mesure où un litige est pendant</p>
<p>Équité salariale</p>	<p>Loi sur l'équité salariale, article 14.1</p> <p>6 ans</p>	<p>6 ans</p>

Nature des documents	Période obligatoire	Période en vigueur
<p align="center">Formation</p> <p>Programmes, contrats, inscriptions, factures, etc.</p>	<p>Règlement sur les dépenses de formation admissibles, RRQ, 1981, c D-8.3, r 3, art 4.</p> <p align="center">6 ans</p>	<p align="center">6 ans</p>
<p align="center">Paie</p> <p>Registres de paies, feuilles de temps, vacances, etc.</p>	<p>Règlement sur la tenue d'un système d'enregistrement, article 2</p> <p align="center">3 ans</p>	<p align="center">3 ans</p>
<p align="center">Registres des mesures d'échantillonnage en santé et sécurité au travail</p> <p>Qualité de l'air, air d'alimentation, contraintes thermiques, mesure du bruit, espaces clos, etc.</p>	<p>Règlement sur la santé et la sécurité au travail, articles 43, 48, 121, 141 et 307</p> <p align="center">5 ans</p>	<p align="center">5 ans</p>
<p align="center">Relevés fiscaux</p>	<p>Loi sur l'administration fiscale, article 35.1</p> <p align="center">et</p> <p>Loi de l'impôt sur le revenu, article 230 (4)</p> <p>6 ans suivant la fin du dernier exercice financier auquel les documents se rapportent</p>	<p align="center">7 ans</p>
<p align="center">Recrutement</p> <p>Curriculum vitae, vérification des antécédents criminels, évaluations médicales ou de compétence, etc.</p>	<p align="center">Aucune période obligatoire</p>	<p>Destruction des candidatures lorsque processus de recrutement complété</p>
<p align="center">Régime de retraite</p>	<p>Loi sur les régimes complémentaires de retraite, LRQ c R-15.1.</p> <p align="center">Aucune période obligatoire</p>	<p>Minimalement 3 ans à compter de l'exigibilité du régime de retraite, soit le décès de l'employé retraité (délai général de prescription – Code civil, article 2925)</p>

Nature des documents	Période obligatoire	Période en vigueur
		Permanent si l'employé est admissible
<p align="center">Rentes du Québec</p> Registres des informations relatives aux cotisants	Loi sur le régime des rentes du Québec, LRQ c R-9, art 66 Aucune période obligatoire	Minimalement quatre ans après la fin de l'exercice de l'année de terminaison d'emploi. Cela correspond à la prescription de quatre ans pour toute imposition par le ministre (prévue à l'article 66 de la Loi)
Réclamations en vertu de la Loi sur les accidents du travail et les maladies professionnelles	Loi sur les accidents de travail et les maladies professionnelles, LRQ c A-3.001. Aucune période obligatoire	3 ans suivant la terminaison d'emploi délai général de prescription – Code civil, article 2925) ou Plus de 3 ans dans la mesure où un litige est pendant
Vidéosurveillance		Bureau : 3 mois Chantier : 3 mois