POLITIQUE SUR LA GESTION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

EROS ET COMPAGNIE

Mise à jour : 2023-11-08

TABLE DES MATIÈRES

1. OBJECTIFS

« EROS ET COMPAGNIE » (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 efficiente et sécuritaire de tous les renseignements personnels détenus au sein d'Éros et Compagnie, 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 vise la protection des renseignements personnels de tous les employés, des collaborateurs de l'entreprise et de sa clientèle. 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.

Aux fins de l'application de cette présente politique, les personnes du programme d'ambassadrices ainsi que les autres types de collaborateurs sont considérés comme des tiers, et les renseignements personnels qui pourraient leur être octroyés par de la clientèle ne sont pas sous la responsabilité de l'entreprise.

3. RÔLE ET RESPONSABILITÉS

3.1. Présidence, 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.

3.1.3. Collaborer au choix des outils informatiques nécessaires afin d'assurer le respect de la présente politique.

3.1.4. Établir les mesures de sécurité requises à l'application de la présente politique.

[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. Direction des ressources humaines

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.

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. Employés et collaborateurs

3.3.1. Aviser le responsable des renseignements personnels lorsqu'un incident de confidentialité survient.

3.3.2. Classer et enregistrer les documents selon les bonnes pratiques en vigueur.

3.3.3. 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 et vidéos

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. L'entreprise s'engage à utiliser les photos et vidéos seulement aux fins consentis.

5.1.2. Vidéosurveillance

L'entreprise utilise un système de vidéosurveillance dont l'objectif est d'assurer la santé et la sécurité des équipes de travail ainsi que de la clientèle, de protéger l'intégrité physique des lieux, en plus de protéger l'entreprise contre le vol de ses produits.

Certaines installations de l'entreprise, notamment les boutiques et l'entrepôt, bénéficient de la vidéosurveillance à des endroits ciblés pour atteindre ces objectifs. Les endroits sous vidéosurveillance sont identifiés par affichage afin d'informer la clientèle et les membres de l'équipe. Aucune autre utilisation de la vidéosurveillance, notamment la surveillance de la prestation de travail de ses équipes, n'est permise par l'entreprise. Une utilisation inadéquate de la vidéosurveillance pourrait entraîner le retrait du privilège d'accès aux renseignements captés en plus de sanctions disciplinaires, si nécessaire.

Seulement les membres de l'organisation qui ont un intérêt sérieux et légitime, soit les directeurs de l'organisation ainsi que les gestionnaires et gérants de boutiques, sont autorisés à consulter les images enregistrées par la vidéosurveillance, selon le cadre régi par la présente.

Si une personne autre que celles autorisées par la présente désire obtenir ces images, elle devra en faire la demande écrite au responsable des renseignements personnels de l'entreprise, en décrivant les raisons et justifications. Une décision sera ensuite rendue après l'évaluation de la légitimité des intérêts de cette dernière ainsi que l'analyse à savoir s'il s'agit de la meilleure façon de remplir ses objectifs.

Les renseignements recueillis par vidéosurveillance se retrouvent sur des serveurs sécurisés, à même l'organisation, dont les accès informatiques sont octroyés uniquement aux personnes ciblées par la présente politique. Les renseignements captés sont conservés pour une période de 2 semaines, après quoi ils sont automatiquement supprimés. L'entreprise se réserve le droit de conserver certains renseignements particuliers dans le cadre d'une situation précise, incluant, mais sans s'y limiter, un recours légal, une enquête pour vol ou un accident en matière de santé et sécurité.

5.2. Conservation

5.2.1. Accès aux renseignements personnels

La liste des employés ayant accès aux renseignements personnels est incluse dans l'« *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 classeur verrouillé à clé, donc l'accès est limité au responsable des renseignements personnels. L'accès au bureau qui contient ces classeurs est également contrôlé. Ces renseignements font l'objet des mêmes procédures que les renseignements personnels numériques, notamment pour les engagements de l'entreprise quant aux délais de conservation.

Les renseignements personnels détenus sous forme numérique sont répertoriés dans des systèmes et plateformes informatiques sécurisés et dédiés, opérés par des tiers. Ces derniers ont fait l'objet de contrats d'affaires pour circonscrire les modalités de protection de renseignements personnels, en cohérence avec la présente politique. L'entreprise exige de ses fournisseurs de respecter les standards de la présente en matière de sécurité et de protection des renseignements personnels.

Seulement les types de renseignements nécessaires à la finalité de chacun des systèmes s'y retrouvent. Chaque système est hébergé sur des serveurs dédiés et sécurisés, dont les accès sont contrôlés afin qu'uniquement les renseignements nécessaires aux fonctions de chaque personne lui soient accessibles.

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

Seule une personne autorisée de l'équipe de gestion des ressources humaines peut fournir des références d'emploi, sous preuve d'un consentement éclairé et spécifique de la part de la personne concernée. L'entreprise va exiger une preuve de consentement signée avant de partager tout renseignement personnel.

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 concernées[2].

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 ;

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

- 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.

- Avant de communiquer un renseignement personnel à l'extérieur du Québec.

Veuillez consulter le guide d'accompagnement émis par la Commission : CAI Guide EFVP

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 ;

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
Assurance collective	Loi sur les assurances, LRQ c A-32 Aucune, sauf en présence de dispositions spécifiques au contrat	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
Assurance-emploi Relevés d'emploi, etc.	Loi sur l'assurance-emploi - articles 87(3) et 87(4) 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 ou jusqu'à ce qu'une décision soit rendue (y compris l'expiration de l'appel) lors d'un litige	8 ans
Comité santé et sécurité	Règlement sur les comités de santé et sécurité du travail, article 31 5 ans	5 ans
Coordonnées et historique de la clientèle	s.o.	Conservation illimitée ou Destruction à la demande du client
Dossier employé Contrats d'emploi, lettres de congédiement, preuves de sanctions disciplinaires, etc.	Aucune période obligatoire	5 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

Nature des documents	Période obligatoire	Période en vigueur
Équité salariale	Loi sur l'équité salariale, article 14.1 6 ans	8 ans
Formation Programmes, contrats, inscriptions, factures, etc.	Règlement sur les dépenses de formation admissibles, RRQ, 1981, c D-8.3, r 3, art 4. 6 ans	6 ans
Paie Registres de paies, feuilles de temps, vacances, etc.	Règlement sur la tenue d'un système d'enregistrement, article 2 3 ans et Loi sur l'équité salariale, article 14.1 6 ans	8 ans
Registres des mesures d'échantillonnage en santé et sécurité au travail Qualité de l'air, air d'alimentation, contraintes thermiques, mesure du bruit, espaces clos, etc.	Règlement sur la santé et la sécurité au travail, articles 43, 48, 121, 141 et 307 5 ans	5 ans
Relevés fiscaux	Loi sur l'administration fiscale, article 35.1 et Loi de l'impôt sur le revenu, article 230 (4) 6 ans suivant la fin du dernier exercice financier auquel les documents se rapportent	8 ans
Recrutement Curriculum vitae, vérification des antécédents criminels,	Aucune période obligatoire	3 ans suivant la fin d'un processus d'embauche

Nature des documents	Période obligatoire	Période en vigueur
évaluations médicales ou de compétence, etc.		
Régime de retraite	Loi sur les régimes complémentaires de retraite, LRQ c R-15.1. Aucune période obligatoire	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) Permanent si l'employé est admissible
Rentes du Québec 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	s.o.	2 semaines ou Plus de 2 semaines si un litige est pendant