

Fiche-conseil : Comment recueillir et gérer des renseignements délicats



Cette fiche-conseil aide les organisations à comprendre comment satisfaire aux exigences en matière de collecte et de gestion de renseignements délicats décrites dans l'indicateur 1 concernant le leadership et la stratégie du Protocole TSM pour un milieu de travail équitable, diversifié et inclusif (critères à l'échelle de l'entreprise), et l'indicateur 3 concernant la surveillance, le rendement et la production de rapports.

Les organisations recueillent et gèrent souvent des renseignements délicats tout en élaborant et en mettant en œuvre des stratégies et des plans d'action à l'appui de l'équité, de la diversité et de l'inclusion en milieu de travail. Les renseignements délicats comprennent les données qui doivent être protégées en raison des risques pour une organisation, des groupes, ou des personnes qui pourraient être associés à leur perte, leur utilisation abusive ou leur modification. Les renseignements délicats peuvent être en lien au bassin de talents et aux données sur les finances, la santé ou le statut socioéconomique, y compris les données liées à l'EDI. Cela comprend des renseignements personnels liés à l'identité, comme l'origine ethnique, l'orientation sexuelle, l'identité de genre, l'âge, le statut d'invalidité, le statut de citoyenneté ou d'immigration; des renseignements organisationnels liés à la rémunération ou à l'équité en matière d'emploi, le signalement et la résolution d'incidents; ou même des renseignements très délicats liés à la planification de la sécurité personnelle.

Les sociétés minières qui exercent leurs activités au Canada et qui recueillent et gèrent des renseignements délicats sont tenues de préserver la confidentialité et l'anonymat des données. Les entreprises sont liées par des lois et des règlements fédéraux et provinciaux sur la protection des renseignements personnels. À l'échelle fédérale, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) régit « la façon dont les organisations du secteur privé recueillent, utilisent et communiquent des [renseignements personnels](#) ». ¹ Certaines provinces ont des lois sur la protection des renseignements personnels semblables à la LPRPDE, particulièrement pour les données sur la santé, l'éducation et l'emploi.

¹ Commissariat à la protection de la vie privée, Aperçu des lois sur la protection des renseignements personnels. Les entreprises qui mènent des activités commerciales à but lucratif sont assujetties à la LPRPDE, tout comme les organisations sous réglementation fédérale en ce qui concerne les renseignements sur les employées et employés. La LPRPDE ne s'applique pas aux organisations qui exercent leurs activités entièrement en Alberta, en Colombie-Britannique ou au Québec.





Cueillette de renseignements délicats



1. Créer une politique de gestion des données

Avant de recueillir des renseignements délicats, assurez-vous que des politiques de collecte et d'utilisation des données de l'entreprise sont en place, qu'elles sont conformes aux cadres réglementaires appropriés et qu'elles sont communiquées à l'interne ainsi qu'aux fournisseurs d'information. Ces politiques traitent des protocoles de communication, ainsi que des pratiques de collecte et de transmission des renseignements, et de stockage et de destruction des données. Elles précisent les différentes méthodes de collecte de données qui peuvent être utilisées (p. ex. sondage, entrevue, groupe de discussion, etc.) et les mesures appropriées pour s'assurer que les renseignements délicats sont recueillis, gérés, stockés et détruits de façon appropriée. La communication de la politique aux groupes de parties prenantes, y compris le personnel, démontre une transparence et une conformité à l'environnement réglementaire dans lequel l'entreprise exerce ses activités. Les outils de collecte et de stockage des données utilisés pour les renseignements personnels ou délicats doivent être conformes à la politique de gestion des données de l'entreprise.

2. Obtenir le consentement

Avant de fournir des données, les personnes sont informées des risques associés à la divulgation de leurs renseignements pour favoriser la compréhension et assurer la prise de décisions éclairées au sujet de toute information transmise, c'est-à-dire le consentement éclairé. De même, une personne doit être capable de comprendre les risques connexes pour donner son consentement ou être en présence d'une tutrice légale ou d'un tuteur légal qui pourra le faire pour elle. Lorsque les renseignements recueillis sont délicats, le consentement peut être donné au moyen d'une indication verbale ou écrite claire, c'est-à-dire en autorisant ou en refusant le consentement au moyen d'un simple « oui ou non », réponse qui peut être retirée à tout moment. Pour favoriser la sensibilisation aux risques, informez les personnes des éléments suivants :

a) À quelles fins les renseignements personnels sont-ils recueillis, utilisés ou divulgués?

Donnez aux personnes des renseignements sur le but de la collecte des données, les objectifs de cette dernière, et s'il y a lieu, pourquoi et dans quelles circonstances elles seront communiquées ou divulguées. Il est important d'indiquer si l'utilisation des renseignements sera faite de manière à protéger la confidentialité ou l'anonymat des personnes.





b) Quels renseignements personnels sont recueillis?

Informez les personnes des renseignements précis qui sont recueillis, de la portée ou des restrictions de leur utilisation prévue et indiquez si la participation au processus de collecte des données est obligatoire ou volontaire. Offrir aux répondantes et répondants plusieurs options de réponses à des questions délicates, telles que « Je préfère ne pas répondre », peut également être une pratique efficace.

c) À qui les renseignements personnels seront-ils communiqués

Fournissez aux personnes de l'information sur l'utilisation des renseignements divulgués : qui aura accès aux données, seront-elles communiquées avec un tiers, et si oui, à quelle fin, comment seront-elles gérées, et par qui?

d) Y a-t-il des risques de préjudice et d'autres conséquences?

Assurez-vous que les personnes savent que même si des politiques et des outils sont mis en place pour atténuer les risques de préjudice, ceux-ci existent toujours. Dans la mesure du possible, cernez et communiquez les risques prévisibles ainsi que l'approche de l'organisation pour atténuer ou gérer ces risques.

3. Collecte de données

La collecte de données délicates est facilitée dans le cadre d'une culture respectueuse en milieu de travail, particulièrement dans une culture où la diversité est valorisée et où le partage des préoccupations ou le signalement des incidents au travail est soutenu.² De plus, la transparence de l'entreprise et la fiabilité éprouvée dans la gestion des données délicates favorisent la confiance et la volonté de consentir. Cela commence par limiter la collecte de données à l'information nécessaire. Dans le cadre de la collecte de données délicates, les personnes peuvent contrôler la quantité et la nature des renseignements qu'elles souhaitent transmettre. Les exceptions sont limitées et comprennent les données nécessaires à des fins d'emploi, comme pour la paie, alors que la date de naissance d'une personne, par exemple, est souvent demandée.

2 La collecte peut être faite au moyen de politiques et de procédures pertinentes, d'approches tenant compte des traumatismes ou d'une culture de signalement positive.





Gestion de l'accès aux données délicates

Si des données délicates sont recueillies, des plans de gestion, de stockage et de destruction sont également nécessaires. Chacun des facteurs suivants doit être pris en compte pour assurer l'harmonisation avec les politiques de l'entreprise et les exigences réglementaires en matière de protection de la vie privée.

1. Accès aux données

Tous les renseignements délicats, y compris les données en matière d'EDI, sont généralement chiffrés et consultés au moyen d'une authentification multifactorielle. Divers types de données délicates sont classifiés et accessibles uniquement par les utilisateurs autorisés selon un [principe clair et distinct d'accès sélectif](#). La classification des données peut être publique, interne, confidentielle ou à diffusion restreinte. L'accès aux données délicates doit se faire selon le principe d'« accès sélectif » et faire l'objet d'un examen régulier, car les personnes, les rôles et les méthodes et technologies de gestion des données changent souvent.

2. Stockage des données

Pour assurer leur protection, les renseignements délicats doivent être chiffrés et stockés uniquement en utilisant les méthodes actuelles et approuvées. Le stockage infonuagique sécurisé avec authentification multifactorielle est actuellement l'approche privilégiée. La création de copies papier ou de copies en double doit être limitée ou évitée. Si elle est permise temporairement, les copies doivent être protégées avec la même rigueur que la version originale.

L'examen régulier de l'information stockée pour en déterminer la pertinence conformément aux politiques de conservation des données de l'entreprise contribue à réduire les coûts et les risques liés au stockage inutile de renseignements délicats. Conformément aux règlements sur la conservation des documents et à la politique organisationnelle, détruisez les données lorsqu'elles ne sont plus utiles aux fins de collecte d'origine et qu'elles ne sont plus nécessaires à des fins d'archivage ou de conservation.

3. Destruction des données

Les données qui ne sont plus pertinentes sont généralement examinées par un ou une spécialiste de la conservation des données, puis détruites conformément aux procédures de conservation et de destruction des données de l'entreprise.





Risques associés à la communication de renseignements délicats

À des fins de conformité, les sociétés minières qui exercent leurs activités au Canada peuvent consulter les lois fédérales canadiennes (LPRPDE³), les exigences provinciales et territoriales ainsi que les lois sur les droits de la personne et l'équité en matière d'emploi pour établir des processus de gestion et de collecte de renseignements délicats, particulièrement en ce qui concerne les objectifs liés à l'emploi. Les entreprises qui exercent leurs activités dans d'autres pays peuvent également examiner les lois sur la protection de la vie privée dans ces régions et évaluer leur applicabilité.

Pour établir un plan complet de gestion de l'information, les entreprises cernent les risques liés à la communication de renseignements délicats, y compris la divulgation involontaire, par exemple par erreur humaine ou par transmission d'informations liées à un petit ensemble de données, et la façon dont les demandes de renseignements délicats seront traitées. Une atteinte à la protection des renseignements peut entraîner un risque personnel et professionnel important pour les personnes ainsi que des risques financiers, juridiques et d'atteinte à la réputation pour une organisation.



Amélioration continue

Pour créer un système de gestion de l'information sécuritaire, transparent et dynamique, offrez aux personnes l'occasion de poser des questions ou de formuler des commentaires sur le processus de collecte des données. Envisagez également de consulter un ou une spécialiste en protection de la vie privée au sujet du processus afin de solliciter de la rétroaction et d'explorer des façons d'optimiser le processus de collecte.

Références

GDPR.eu. (2023). *Complete Guide to GDPR Compliance*. (en anglais seulement) <https://gdpr.eu/>

Commissariat à la protection de la vie privée du Canada. (2018). *La LPRPDE et son règlement d'application*. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/

Commissariat à la protection de la vie privée du Canada. (2018). *Aperçu des lois sur la protection des renseignements personnels au Canada*. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/

3 Voir https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/ pour en savoir plus.

