BONNE SEMAINE DE LA PROTECTION DES DONNÉES, CANADA! NUMÉRO 3

Publié le 24 janvier, 2024

Catégories: Perspectives, Publications

Presque toutes les organisations recueilleront, utiliseront, partageront et stockeront les renseignements personnels de leurs employés. Une grande partie de ces renseignements, notamment les renseignements financiers, sur la santé et même l'information biométrique, sont considérés comme sensibles et doivent être traités avec grand soin.

En fonction de la ou des provinces où se trouvent ses salariés, de leur appartenance à un syndicat et du fait qu'elle soit sous réglementation fédérale ou provinciale, une organisation peut être assujettie à diverses lois concernant le traitement des renseignements personnels de ses salariés.

La Semaine de la protection des données offre une excellente occasion de veiller à ce que le programme de conformité de votre organisation en matière de protection des renseignements personnels tienne adéquatement compte des risques pour les données de vos salariés.

Les cinq meilleurs conseils de McMillan pour prendre le contrôle des données de vos salariés

1. **Évaluez la surveillance de vos salariés.** Les nouvelles technologies, combinées à des arrangements de travail hybrides permanents ou entièrement à distance, ont contribué à l'augmentation de l'utilisation d'outils de surveillance des salariés, notamment les dispositifs de localisation GPS, les solutions biométriques de consignation du temps, l'enregistrement vidéo et audio, la surveillance des courriels et du réseau, et plus encore. Ces outils peuvent être utiles pour vérifier la localisation des salariés, gérer l'assiduité, suivre la productivité des salariés et surveiller l'utilisation des technologies ou de l'équipement appartenant à l'entreprise, entre autres. Toutefois, ce n'est pas parce que ces technologies sont disponibles que leur utilisation sera conforme aux lois canadiennes applicables en matière de protection des renseignements personnels dans tous les cas. Les initiatives de surveillance des salariés doivent être conçues et déployées de manière à assurer le respect de toutes les exigences juridiques applicables, y compris (sans s'y limiter) de manière à réduire la collecte et l'utilisation des renseignements personnels des salariés à ce qui est nécessaire à des fins raisonnables et appropriées dans les circonstances, et à s'assurer que tous les avis et/ou politiques requis ont été fournis et conservés. Les organisations qui

utilisent, ou ont l'intention d'utiliser, des outils de surveillance des salariés peuvent envisager de procéder à une évaluation des facteurs relatifs à la protection de la vie privée avant leur conception et leur déploiement afin d'identifier les risques liés à la protection de la vie privée et de mettre en œuvre des mesures d'atténuation appropriées.

2. **Choisissez les fournisseurs de services avec soin.** De nombreuses organisations retiennent les services de fournisseurs ou de fournisseurs de services qui traitent les renseignements personnels des salariés en leur nom, notamment les fournisseurs de services de paie, les administrateurs d'avantages sociaux, les consultants en ressources humaines, et plus encore. Dans de nombreux cas, les employeurs demeurent responsables des renseignements personnels des salariés lorsqu'ils sont traités par des tiers, ce qui signifie que l'utilisation abusive ou la mauvaise gestion des données des salariés par un fournisseur de services peut entraîner des risques juridiques importants, en plus de nuire au moral des salariés. Une vérification soigneuse des fournisseurs qui traitent des renseignements personnels doit être faite pour s'assurer que des pratiques appropriées en matière de protection des renseignements personnels et de cybersécurité ont été mises en place afin de se conformer aux lois applicables en la matière et de protéger les renseignements personnels traités. Ces fournisseurs doivent également faire l'objet de mesures contractuelles appropriées afin d'offrir un niveau de protection comparable aux données sur les salariés. Enfin, la surveillance et la vérification continues de la conformité du fournisseur aux lois sur la protection des renseignements personnels et à ses engagements contractuels pourraient être nécessaires.
3. **Limitez l'accès interne aux données sur les salariés.** Les organisations devraient limiter l'accès aux renseignements personnels des salariés aux personnes qui doivent les utiliser pour s'acquitter de leurs fonctions particulières. Par exemple, les renseignements sensibles concernant la demande de mesures d'adaptation et d'invalidité d'un salarié ne devraient généralement être accessibles qu'à un sous-ensemble précis de membres du personnel de l'organisation qui ont besoin d'y avoir accès pour donner suite à la demande de mesures d'adaptation. Le fait d'inclure ces renseignements dans le dossier d'un membre du personnel plus largement accessible peut, entre autres, faire augmenter le risque que les salariés les trouvent en furetant et les utilisent à mauvais escient. Les organisations devraient également veiller à ce que l'accès aux renseignements personnels des salariés qui quittent leur emploi soit limité aux membres du personnel qui auront besoin d'y avoir accès à l'avenir, par exemple pour répondre à toute réclamation ou plainte judiciaire éventuelle ou pour démontrer qu'ils se conforment aux exigences de tenue de dossiers prévues par la loi.
4. **Concevez des initiatives de DEI avec soin.** Un certain nombre d'organisations recueillent et utilisent les renseignements personnels des salariés dans le but d'évaluer le besoin et d'élaborer, de mettre en œuvre et de suivre l'efficacité d'initiatives en matière de diversité, d'équité et d'inclusion dans leur milieu de

travail. Bien que ces initiatives soient généralement bien intentionnées, elles peuvent soulever une foule de préoccupations et de considérations en matière de protection de la vie privée et de sécurité, notamment quant à la collecte, à l'utilisation et à la protection de renseignements personnels sensibles sur les salariés, comme les données sur la race, l'origine ethnique, la religion, le handicap, l'orientation sexuelle, l'identité ou l'expression de genre des salariés, et plus encore. Les lois sur la protection des renseignements personnels et/ou les droits de la personne peuvent limiter les circonstances dans lesquelles ces renseignements peuvent être recueillis et la façon dont ils peuvent être utilisés et divulgués. Ces limites doivent être évaluées et intégrées dans la conception et la mise en œuvre de toutes les initiatives de DEI, et un plan doit être mis en place pour garantir la protection de cette information d'une manière adaptée à sa sensibilité.

5. **Mettez en œuvre la minimisation des données.** Les données sur les salariés ne devraient pas être conservées indéfiniment. L'accumulation d'une grande quantité de données, particulièrement sur les anciens salariés, entraîne un certain nombre de risques, y compris le risque d'utilisation abusive et d'atteintes coûteuses à la protection des données. Il est important que les organisations élaborent des calendriers détaillés de conservation des données qui tiennent compte de toute période de conservation prévue par la loi (comme l'obligation de conserver des données pour démontrer la conformité aux lois fiscales et aux normes d'emploi) tout en prévoyant la suppression sécuritaire (ou l'anonymisation, lorsque la loi applicable le permet) de ces renseignements, le cas échéant.

L'équipe Protection de la vie privée et des données de McMillan fournit des conseils pratiques aux organisations en ce qui concerne le traitement et la protection des renseignements personnels des salariés. Célébrez la Semaine de la protection des données en communiquant avec votre conseiller/conseillère chez McMillan pour discuter de stratégies visant à concilier les droits des salariés et les besoins opérationnels de votre organisation!