LES CINQ PRINCIPALES MESURES QUE VOUS N'APPLIQUEZ PROBABLEMENT PAS (MAIS QUE VOUS DEVRIEZ) POUR VOUS CONFORMER AUX LOIS CANADIENNES SUR LA PROTECTION DE LA VIE PRIVÉE – *MESURE Nº 5 : FORMATION DES EMPLOYÉS*

Publié le 25 septembre, 2024

Catégories: Perspectives, Publications

Vous avez sans doute remarqué un thème commun dans les quatre bulletins précédents de cette série : la formation des employés constitue une mesure à prendre essentielle pour assurer l'efficacité d'un programme canadien de conformité en matière de protection de la vie privée.

Les employés sont souvent le « maillon faible » du programme de protection de la vie privée et des données d'une organisation. Même s'il est impossible d'éviter complètement l'envoi de courriels aux mauvais destinataires, le cliquage sur des liens d'hameçonnage, l'élimination inappropriée de documents, la perte de dispositifs portables non chiffrés et d'autres erreurs humaines, on peut en réduire considérablement la probabilité si le personnel reçoit une formation appropriée. Lorsque des erreurs se produisent ou que des anomalies sont relevées, les employés doivent signaler ces incidents de façon adéquate et en temps opportun afin que les dommages potentiels soient limités.

Les employés font également office de première barrière de sécurité dans l'administration du programme de conformité en matière de protection de la vie privée de votre organisation. Ils sont responsables de diverses fonctions importantes en la matière, notamment la conception de produits, de services et d'initiatives qui respectent la vie privée; la détermination du moment où effectuer une évaluation des facteurs relatifs à la protection de la vie privée et de sa pertinence; la sélection, la mobilisation et la surveillance des fournisseurs qui traitent des renseignements personnels; l'obtention du consentement aux fins de collecte, d'utilisation et de communication de tels renseignements; et la réception des demandes, des questions et des plaintes des personnes concernées, leur transmission aux supérieurs hiérarchiques et la réponse à donner. Pour qu'ils puissent mettre en œuvre de manière cohérente et conforme à la loi les politiques et procédures de votre organisation en matière de protection de la vie privée, vos employés doivent recevoir une formation adéquate.

Une telle formation fait aussi partie des obligations énoncées dans les lois applicables sur la protection de la vie

privée. Par exemple, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDE** »), une organisation est tenue d'informer le personnel sur les politiques et les pratiques de l'organisation en matière de protection de la vie privée et de le former à ce sujet.

Par contre, ce ne sont pas tous les types de formation qui permettront l'atteinte de ces objectifs importants. Pour qu'un programme de formation sur la protection de la vie privée et des données soit efficace, il doit inclure ce qui suit :

- Une séance obligatoire que tous les employés doivent suivre au début de leur emploi avant d'avoir accès à des renseignements personnels.
- Des séances périodiques et continues pour rafraîchir les connaissances des employés sur les concepts clés ainsi que tenir compte des nouvelles pratiques, des modifications apportées aux politiques et aux procédures, de l'évolution du portrait global des risques et de l'actualité dans le secteur du droit.
- Du contenu adapté à chaque rôle, y compris des exemples pratiques de problèmes de protection de la vie privée et des données qui peuvent se poser dans le cadre des fonctions et des responsabilités quotidiennes des employés.
- Des activités interactives, comme des simulations d'attaques par hameçonnage, des études de cas ou des exercices (résoudre des problèmes simulés de violation des données, par exemple).
- Des renseignements sur la façon dont les membres du personnel doivent faire part de leurs questions, de leurs préoccupations ou d'autres circonstances nécessitant un soutien supplémentaire, et à qui s'adresser le cas échéant.

Un aspect clé souvent négligé de la formation est l'importance de l'adapter au rôle de l'employé. Dans bien des cas, les informations générales à propos des exigences des lois sur la protection de la vie privée ne sont pas très utiles lorsque les employés doivent prendre des décisions sur la façon de traiter les renseignements personnels dans l'exercice de leurs fonctions. De plus, le type de renseignements personnels auxquels ils ont accès et la façon de les traiter peuvent varier considérablement d'un service à l'autre. Par exemple, le personnel des ressources humaines n'exerce pas les mêmes activités de traitement des données que celui du service aux clients. Chaque groupe devra connaître les éléments relatifs à la protection de la vie privée qui concernent ses activités.

Enfin, il est important de comprendre qu'une telle formation ne se limite pas à la sécurité de l'information. Bien entendu, les employés doivent être formés de manière à ce qu'ils puissent protéger les renseignements personnels et prévenir les violations des données par des tiers malveillants. Toutefois, il est tout aussi indispensable pour eux de comprendre d'autres aspects de la conformité en matière de protection de la vie privée, comme les limites qui s'appliquent à l'utilisation de renseignements personnels sous le contrôle de

l'organisation à une fin différente sans qu'un nouveau consentement ait été recueilli ou qu'une exception pertinente au consentement ait été autorisée. Par ailleurs, le « furetage » demeure un enjeu considérable. Les employés doivent comprendre que même s'ils ont accès à certains renseignements personnels, ils n'ont pas pour autant la permission de les examiner ou de les utiliser à une fin autre que l'exercice de leurs fonctions.

Mesures à adopter

Concevez et instaurez un programme efficace de formation sur la protection de la vie privée et des données à l'intention du personnel de votre organisation 1) en élaborant une formation et en la donnant à tous les nouveaux employés avant de leur autoriser l'accès à des renseignements personnels; 2) en élaborant et en planifiant une formation d'appoint ainsi qu'en la donnant périodiquement aux employés actuels, notamment pour rafraîchir leurs connaissances sur les notions de base importantes et tenir compte des modifications apportées aux lois applicables, aux indications réglementaires et aux politiques, procédures et pratiques de votre organisation; 3) en veillant à ce que le matériel de formation existant traite des exigences particulières prévues par les indications réglementaires et les lois canadiennes sur la protection de la vie privée; 4) en mettant au point et en appliquant des politiques et des procédures internes quant à la formation du personnel; 5) en concevant et en mettant à la disposition du personnel des ressources, comme des listes de vérification ou des aide-mémoire, qui renforcent les acquis sur les concepts explorés pendant la formation; 6) en tenant à jour des dossiers de formation appropriés; et 7) en veillant à ce que les contrats conclus avec les fournisseurs qui traitent des renseignements personnels pour le compte de votre organisation comprennent des modalités appropriées sur la formation de leurs employés.

L'équipe du groupe Protection de la vie privée et des données de McMillan peut aider votre organisation à adopter les mesures ci-dessus. Nous vous invitons à communiquer avec votre représentant.e chez McMillan pour obtenir le soutien dont votre organisation a besoin en vue de respecter ces questions essentielles de conformité en matière de protection de la vie privée.

Par Lyndsay Wasser et Kristen Pennington

Mise en garde