大成 DENTONS

Dentons Data COVID-19

Trousse d'outils relative à la protection des renseignements personnels et des données dans le cadre du redémarrage de vos activités

NOTE : Dentons a élaboré le présent guide pour aider ses clients canadiens à faire face aux enjeux en matière de protection des renseignements personnels auxquels ils pourraient être confrontés lors de la réouverture de leur entreprise et du retour au travail de leurs employés, et ce, dans le contexte de la COVID-19 et de la reprise graduelle des activités économiques. Veuillez noter que les informations fournies dans cette trousse d'outils ne sont pas destinées à constituer un avis d'ordre juridique. Chaque entreprise devra élaborer ses propres plans en tenant compte de la nature de ses activités, du ou des territoires de compétence où elle mène ses activités ainsi que des renseignements, des arrêtés et des recommandations fournis par les gouvernements et les autorités de santé publique. Nous espérons que les employeurs trouveront dans notre trousse d'outils l'information de base dont ils ont besoin afin de bien planifier et gérer la reprise de leurs activités. Si vous avez des questions, veuillez communiquer avec l'un des membres du groupe Technologies transformatrices et stratégies de gestion des données de Dentons.

Table des matières

05 ...Introduction

06 ... Contrôle de l'accès aux lieux de travail – Dépistage des signes et symptômes de la COVID-19

07 ... A. Considérations générales

09 ... B. Dépistage actif (questionnaire)

09 ... C. Mesure de la température corporelle et imagerie thermique

10 ... D. Identifiants biométriques

11 ... E. Applications de traçage des contacts

13 ... Fournisseurs et autres

14 ... Divulgation de l'information relative aux employés déclarés positifs aux tests de dépistage de la COVID-19

16 ... Mobilité des employés

17 ... Systèmes de vidéoconférence en ligne

24 ... Surveillance des employés

26 ... Personnes-ressources

Introduction

La crise de la COVID-19 est sans précédent et des changements sont apportés aux cadres juridiques canadiens, y compris aux lois sur la protection des renseignements personnels, à mesure que la situation évolue. Le Commissariat à la protection de la vie privée (CPVP) du Canada a reconnu que la pandémie exige une application souple et contextuelle des lois sur la protection des renseignements personnels. Ainsi, des mesures qui ne seraient pas raisonnables dans des circonstances ordinaires peuvent être justifiées dans les circonstances actuelles.

Les entreprises et autres organisations (ci-après les entreprises) auront plusieurs nouveaux facteurs à considérer à mesure que nous franchirons les différentes étapes du retour au travail, qui s'étaleront sur une période de temps encore indéterminée. Le présent guide traite d'un grand nombre de questions liées à la protection des renseignements personnels et de la vie privée auxquelles les entreprises seront confrontées au cours de l'année à venir, alors que les mesures de confinement seront allégées ou resserrées selon ce qu'il sera nécessaire de faire pour prévenir la propagation du virus.

Nous avons préparé cette trousse d'outils en complément aux trousses d'outils pour le retour au travail qu'a créées notre groupe de droit du travail afin d'aider les entreprises à bien comprendre les exigences « souples et contextuelles » en matière de protection des renseignements personnels dans le cadre de la reprise de leurs activités.

Voici les principaux sujets dont il est question dans les pages qui suivent :

Contrôle de l'accès aux lieux de travail – Dépistage des signes et symptômes de la COVID-19

a. Considérations générales

b. Dépistage actif (questionnaire)

c. Mesure de la température corporelle et imagerie thermique

d. Identifiants biométriques

e. Applications de traçage des contacts

f. Fournisseurs et autres

Divulgation de l'information relative aux employés déclarés positifs aux tests de dépistage de la COVID-19

Mobilité des employés

Systèmes de vidéoconférence en ligne

Surveillance des employés

Contrôle de l’accès aux lieux de travail – Dépistage des signes et symptômes de la COVID-19

Les entreprises pourraient envisager l'adoption de mesures de dépistage des signes et symptômes de la COVID-19, qu'il s'agisse de demander aux employés ou aux clients de répondre à certaines questions, de mesurer la température corporelle des employés ou des clients ou de recueillir certaines données biométriques, afin d'identifier les personnes potentiellement infectées et de leur interdire l'accès aux lieux de travail. L'objectif poursuivi est généralement d'éviter la propagation de la COVID-19 ou d'aider à retracer les personnes ayant été en contact avec la COVID-19 à des fins épidémiologiques ou préventives (ou les deux).

Le dépistage des signes et symptômes de la COVID-19 entraîne nécessairement la collecte, l'utilisation et la communication de certains renseignements personnels et par conséquent, touche aux droits des personnes en vertu des lois canadiennes sur la protection des renseignements personnels. Quelle que soit la forme des mesures de dépistage, certaines obligations en matière de protection des renseignements personnels s'appliquent.

Les entreprises sont tenues par la loi de s'assurer que leurs lieux de travail sont sécuritaires. Toutefois, les considérations relatives à la sécurité ne leur permettent pas de déroger aux dispositions des lois canadiennes sur la protection des renseignements personnels. Elles doivent trouver un équilibre entre la sécurité et la protection de la vie privée. Toutes les mesures de sécurité qui entraînent la collecte, l'utilisation ou la communication de renseignements personnels doivent être raisonnablement justifiables dans les circonstances et doivent faire l'objet d'un consentement (à moins que l'une des très rares exceptions en matière de consentement s'applique).

La majorité des exigences en matière de sécurité sur les lieux de travail qui sont directement liées à la COVID-19 découlent des lignes directrices et des recommandations fournies par les organismes de santé publique des provinces et territoires canadiens. À elles seules, ces lignes directrices et ces recommandations n'ont pas force de loi, mais elles constituent néanmoins des « précautions raisonnables » et servent de points de référence. En fait, toute entreprise qui ne met pas de telles lignes directrices ou recommandations en œuvre s'expose et expose ses employés et ses clients à des risques inutiles.

Lorsqu'elles élaborent des politiques, des procédures, des formations et des communications concernant les processus de contrôle de l'accès, les entreprises doivent se baser sur des informations à jour provenant de sources fiables. Rester à jour peut s'avérer difficile : les informations peuvent changer chaque semaine, voire chaque jour, et les entreprises doivent faire preuve de diligence et ajuster leurs pratiques en conséquence. Il est préférable de suivre les conseils des agences gouvernementales fédérales, provinciales et locales en matière de protection des renseignements personnels, de santé publique et de santé et sécurité au travail. Tout programme de dépistage des signes et symptômes de la COVID-19 devrait être annoncé à l'aide d'affiches (sur lesquelles l'information est présentée de préférence en une combinaison d'images et de texte) placées dans des endroits stratégiques sur les lieux de travail, lorsque cela est possible.

Outre les questions relatives à la protection des renseignements personnels et des données, il convient de noter que certains aspects touchant les droits de la personne ou les lois du travail, notamment en matière de santé et sécurité au travail, doivent être pris en compte lorsque l'entreprise met en place des mesures de dépistage ou de collecte d'information sur l'état de santé d'une personne. Pour obtenir de plus amples renseignements sur ces questions, veuillez consulter nos trousses d'outils sur le retour au travail ou communiquer avec un membre du groupe de droit du travail de Dentons.

A. Considérations générales

Les deux éléments essentiels pour satisfaire aux obligations en matière de protection des renseignements personnels lors de la mise en œuvre d'un programme de dépistage des signes et symptômes de la COVID-19 sont les évaluations des facteurs relatifs à la vie privée (EFVP) et les pratiques de gouvernance de l'information. Les EFVP aident les entreprises à mettre en œuvre des initiatives efficaces dans le cadre desquelles la collecte d'information sera faite en toute conformité aux lois applicables, alors que les pratiques de gouvernance de l'information aident les organisations à se conformer aux obligations en matière de protection des renseignements personnels une fois que les renseignements sont entre leurs mains.

(i) Évaluation des facteurs relatifs à la vie privée (EFVP)

Avant de mettre en place des mesures de dépistage des signes et symptômes de la COVID-19 exigeant la collecte, l'utilisation ou la communication de renseignements personnels, il est prudent (et obligatoire dans le cas de certaines organisations du secteur public) de mener une EFVP. Une EFVP est une évaluation systématique d'une initiative, d'une technologie ou d'une pratique de traitement de l'information proposée. Elle sert à repérer et à analyser les risques d'atteinte à la vie privée ainsi qu'à établir les bases sur lesquelles les risques devront être gérés, y compris à identifier les mesures à mettre en œuvre pour ramener les risques à un niveau acceptable.

La portée et le contenu d'une EFVP varieront en fonction de la nature des activités de l'entreprise, mais une EFVP devrait porter sur l'intention, la justification et l'efficacité de l'initiative proposée, identifier les risques et évaluer la tolérance aux risques, déterminer l'objectif poursuivi afin d'éviter que renseignements personnels soient utilisés à d'autres fins que celle qui est prévue, créer (ou confirmer) des politiques, identifier les personnes au sein de l'entreprise qui sont responsables du traitement des renseignements personnels et établir un calendrier et un processus de conservation des renseignements recueillis.

(ii) Gouvernance de l'information

La première étape d'une bonne gouvernance de l'information consiste à circonscrire les renseignements à recueillir. Au cours des activités de dépistage des signes et symptômes de la COVID-19, l'entreprise doit seulement recueillir les renseignements personnels qui sont raisonnablement nécessaires pour atteindre les objectifs visés. Lorsqu'elle recueille plus de renseignements que ce qui est raisonnablement nécessaire, elle ne fait pas que contrevenir aux lois canadiennes sur la protection des renseignements personnels : elle augmente aussi de façon significative les risques d'atteinte à la protection des données, les risques de litiges et le montant des dommages-intérêts dans l'éventualité où une telle atteinte se produirait.

L'entreprise doit conserver les renseignements qu'elle recueille uniquement pour la période nécessaire aux fins visées ou pour la période requise par la loi, après quoi les renseignements doivent être détruits de façon sécuritaire. Afin de consigner ses pratiques et les mesures qu'elle prend pour assurer sa conformité, une entreprise peut créer des méta-dossiers, dans lesquels elle inscrit par exemple que des personnes ont été soumises à des activités de dépistage, mais qu'aucune ne présentait des signes ou symptômes de la COVID-19.

Les entreprises sont tenues, en vertu des lois canadiennes sur la protection des renseignements personnels, de prendre les mesures appropriées pour protéger les renseignements personnels qu'elles ont en leur possession, et ce, qu'il s'agisse de mesures physiques (p. ex. conservation des données dans un lieu d'entreposage fermé à clé), techniques (p. ex. bases de données protégées par un mot de passe) ou administratives (p. ex. pratiques en matière de protection des renseignements personnels ou ententes de confidentialité). Ce qui est approprié dépend de la nature et de la forme des renseignements personnels visés. Plus une entreprise détient de renseignements personnels et plus elle les conserve longtemps, plus les risques de violation (et les dommages éventuels en cas de violation) sont élevés.

Les entreprises devraient adopter des politiques de gouvernance de l'information, y compris des dispositions fixant la durée de conservation de certains types d'informations, et consigner celles-ci. Les politiques en matière de protection des renseignements personnels et de la vie privée dont les entreprises disposent déjà peuvent probablement servir de point de départ, car il s'agit de politiques avec lesquelles les employés sont déjà familiers. Les politiques de gouvernance de l'information doivent comprendre des dispositions relatives à la destruction de manière sécuritaire (ou à la dépersonnalisation rigoureuse, le cas échéant) des renseignements personnels et prévoir les cas d'exception (p. ex. la suspension des mesures de destruction en cas de litige).

B. Dépistage actif (questionnaire)

En vertu des lignes directrices actuelles en matière de santé publique, les entreprises devraient procéder à un dépistage actif des signes et des symptômes de la COVID-19 chez les personnes (y compris les employés, les entrepreneurs, les visiteurs, etc.) qui souhaitent entrer dans leurs locaux, et ce, au moyen d'un questionnaire. Ces lignes directrices en soi constitue un motif raisonnable pour procéder à la collecte de certains renseignements personnels, dans la mesure où l'entreprise recueille seulement les renseignements qui sont requis pour assurer la sécurité sur les lieux de travail et dans la mesure où les pratiques de dépistage sont conformes aux lois canadiennes sur la protection des renseignements personnels.

Les questionnaires doivent être basés sur les directives actuelles en matière de santé publique (en d'autres termes, portés sur les signes et les symptômes connus au moment où les mesures sont prises), et sur d'autres facteurs de dépistage non médicaux (comme le fait d'avoir été en contact ou non avec une personne infectée ou potentiellement infectée), et les questions doivent être mises à jour au besoin pour suivre l'évolution des directives.

Il reste à voir si les responsables de la santé publique ou les ministères provinciaux du travail recommanderont aux entreprises de poursuivre le dépistage actif même après que le gouvernement aura assoupli les restrictions actuellement en vigueur. En tout état de cause, les entreprises qui servent les populations vulnérables (p. ex. les hôpitaux et les établissements de soins de longue durée) devraient envisager sérieusement de maintenir le dépistage jusqu'à ce que la menace de la COVID-19 soit disparue.

Comme ce type de dépistage sert avant tout à contrôler l'accès aux lieux de travail, il n'est généralement pas nécessaire de recueillir des renseignements personnels (il n'est pas nécessaire d'identifier la personne ou de conserver de l'information à son sujet). Les entreprises qui sont tenues de vérifier l'identité des personnes (p. ex. les bars) doivent veiller à ce que l'étape de vérification de l'identité soit séparée de l'étape de dépistage des signes et symptômes de la COVID-19.

C. Mesure de la température corporelle et imagerie thermique

La mesure de la température corporelle peut être invasive et ne pas plaire à tout le monde. L'imagerie thermique est une technique moins invasive permettant d'obtenir une image avec différentes couleurs en fonction des températures présentes. Elle permet ainsi d'obtenir une idée de la température corporelle d'une personne. Toutefois, dans les deux cas, on procède à la collecte de renseignements sur la santé d'une personne, lesquels sont généralement considérés comme des renseignements personnels sensibles.

Les examens et les tests médicaux, y compris la mesure de la température corporelle, ne sont généralement acceptables que s'ils sont raisonnablement nécessaires pour atteindre un objectif raisonnable et légitime et s'ils sont réalisés avec le consentement de la personne. Dans des circonstances normales, il n'est généralement pas permis d'exiger des tests de santé, y compris la mesure de la température corporelle, car de tels tests sont dans l'ensemble inutilement invasifs. Ce qui serait plus acceptable, c'est de mesurer la température seulement dans les cas précis où l'entreprise a des motifs raisonnables de croire qu'une personne est symptomatique.

Toutefois, comme la pandémie de COVID-19 est exceptionnelle, il est probable que les obligations qui incombent aux entreprises, en vertu des lois applicables en matière de santé et de sécurité au travail, à savoir entre autres l'obligation de prendre toutes les précautions raisonnables pour protéger la santé et la sécurité de leurs employés ou des autres personnes sur les lieux de travail, peuvent justifier l'utilisation d'instruments de mesure de la température corporelle ou d'appareils d'imagerie thermique, en particulier si l'entreprise fournit des services à des personnes vulnérables. Dans le cas des entreprises essentielles qui, en vertu des arrêtés gouvernementaux, sont tenues de rester ouvertes, et ce, malgré les risques accrus, la prise de mesures de contrôle plus rigoureuses pourrait être justifiée.

Lorsque l'économie redémarrera et que les entreprises non essentielles commenceront à rouvrir leurs portes, ces dernières pourraient envisager de se servir d'instruments pour mesurer la température corporelle ou d'appareils d'imagerie thermique afin de contrôler l'accès des clients à leurs locaux. Si de telles mesures peuvent être raisonnables dans le contexte de la COVID-19, les entreprises qui choisiront cette approche devraient apposer des affiches (ou autres formes de signalisation) indiquant clairement que l'entreprise prend la température corporelle ou l'image thermique des personnes, afin que ces dernières puissent choisir en toute connaissance de cause d'entrer ou de ne pas entrer dans les locaux. Les entreprises devraient aussi envisager d'autres moyens de livrer leurs biens ou de fournir leurs services (p. ex. permettre aux personnes qui ne souhaitent pas qu'on prenne leur température corporelle ou leur image thermique et à qui l'entreprise interdit l'entrée d'obtenir les biens ou les services en ligne ou de ramasser les biens à l'extérieur de l'établissement).

Par conséquent, les entreprises qui, pendant la pandémie, utilisent des instruments pour mesurer la température corporelle ou des appareils d'imagerie thermique devraient le faire en conjonction avec d'autres mesures de contrôle actif (voir plus haut). Dans la mesure du possible, ces entreprises devraient également demander à un tiers ou à une personne ayant reçu une formation adéquate et portant un équipement de protection individuelle de prendre la température ou l'image thermique des personnes. Idéalement, l'endroit où le dépistage se passe doit être isolé (que ce soit derrière un rideau ou dans une salle réservée à cette fin) afin qu'il soit impossible pour les personnes qui attendent de voir la température corporelle des autres.

N'oubliez pas que la température corporelle d'une personne peut être élevée en raison d'un problème médical qui ne pose pas de risque déraisonnable pour la santé et la sécurité des personnes qui se trouvent sur les lieux de travail. En d'autres termes, vous ne pouvez pas dire à une personne dont la température corporelle est élevée qu'elle a peut-être contracté la COVID-19, mais seulement qu'en vertu des directives qui ont été mises en place, vous interdisez l'accès à vos locaux à toutes personnes dont la température corporelle est supérieure à X degrés.

Encore une fois, étant donné que l'utilisation d'instruments pour mesurer la température corporelle et d'appareils d'imagerie thermique ne sert qu'au contrôle de l'accès aux lieux de travail, il n'est probablement pas nécessaire de consigner des renseignements permettant d'identifier une personne. L'entreprise peut par contre conserver des données dépersonnalisées ou agrégées (p. ex. le nombre de personnes dont l'entreprise a pris la température ou l'image thermique, le nombre de personne à qui elle a refusé l'accès à ses locaux, etc.).

Lorsque la pandémie de COVID-19 aura pris fin et que les activités commerciales auront repris, il sera probablement difficile de justifier l'utilisation par les entreprises d'instruments pour mesurer la température corporelle d'une personne, à l'exception, des établissements de soins de longue durée et des autres organisations qui fournissent des services à des personnes vulnérables.

D. Identifiants biométriques

Les éléments d'identification biométriques (empreintes digitales, balayage de la rétine ou reconnaissance faciale) peuvent être des outils efficaces pour identifier les personnes présentes sur les lieux de travail d'une entreprise, mais comme pour les renseignements tirés de l'utilisation d'un instrument de mesure de la température corporelle, les données biométriques sont des renseignements personnels sensibles et les entreprises auront presque toujours besoin d'obtenir le consentement exprès de la personne avant de collecter de telles données.

Avant d'envisager l'utilisation de la biométrie (empreinte digitale, reconnaissance faciale, balayage de la rétine ou des mains, etc.), les entreprises devraient se demander si l'utilisation d'outils d'analyse des caractéristiques biométriques d'une personne est nécessaire et efficace. Elles devraient également évaluer les risques en matière de protection des renseignements personnels que soulève l'utilisation de ces outils et voir s'il existe des moyens moins invasifs pour identifier une personne ou vérifier son identité.

Du fait que les données biométriques sont en pratique immuables, la collecte de telles données devrait reposer sur de solides motifs. Les entreprises qui se servent de la biométrie pour identifier une personne devraient prendre des mesures robustes pour protéger les données et assurer une gouvernance rigoureuse en ce qui a trait au stockage, à la conservation et à la destruction des renseignements recueillis.

Les entreprises qui se sont rapidement tournées vers le paiement en ligne en réponse à la COVID-19 devraient revoir leurs processus de traitement des données, en particulier si le processus de paiement nécessite la collecte de données biométriques aux fins de l'authentification de la personne.

E. Applications de traçage des contacts

Le traçage des contacts est le processus qui consiste à identifier les personnes qui ont été en contact avec la COVID-19, à informer ces personnes qu'elles sont peut-être à risque et à identifier les personnes avec lesquelles elles ont elles-mêmes été en contact, afin de contenir la propagation du virus.

« L'éthique des informations de santé publique, de la protection des données et de la confidentialité des données doit être prise en compte à tous les niveaux des activités de recherche des contacts, dans toutes les activités de formation y afférentes et lors de la mise en œuvre des outils correspondants. »

Organisation mondiale de la santé,
Recherche des contacts dans le cadre
de la COVID-19

En général, les applications de traçage des contacts (ci-après les « applications de traçage ») utilisent la fonction Bluetooth des appareils mobiles sur lesquels elles ont été installées pour enregistrer les numéros d'identification des appareils Bluetooth détectés à proximité (à l'intérieur d'un rayon donné). Les numéros sont stockés dans l'appareil et lorsque la personne reçoit un diagnostic de COVID-19, elle est invitée à téléverser la liste de tous les numéros d'identification que son appareil contient dans les systèmes de l'autorité de santé publique afin qu'ils soient utilisés pour retracer les personnes qui auraient été en contact avec la COVID-19 et de leur envoyer des notifications automatiques (en temps normal, les numéros des appareils que la fonction Bluetooth détecte à proximité ne sont conservés nulle part).

Les gouvernements du monde entier, y compris du Canada, travaillent sur des programmes nationaux dans le cadre desquels leurs citoyens seront invités à télécharger et à utiliser des applications de traçage, mais déjà plusieurs applications de ce type ont été conçues et peuvent être utilisées par les entreprises du secteur privé. Le commissaire à la protection de la vie privée (CPVP) du Canada et ses homologues provinciaux et territoriaux ont conjointement publié des principes que les gouvernements qui prévoient utiliser les applications de traçage devraient respecter. Bien que ces principes ne soient pas contraignants pour les entreprises du secteur privé, ils fournissent à celles-ci un cadre utile pour la mise en œuvre ou la sélection d'applications :

- Consentement : L'utilisation des applications doit être volontaire. Le programme de traçage doit poursuivre des objectifs raisonnables et bien définis et le consentement doit être valable (c'est-à-dire éclairé) à toutes les fins.
- Nécessité et proportionnalité : L'utilisation des applications de traçage doit être fondée sur la science, nécessaire pour une fin particulière, adaptée à cette fin et susceptible d'être efficace.
- Finalité : Les renseignements personnels doivent être utilisés uniquement pour les fins prévues (c'est-à-dire la prévention de la transmission de la maladie) et pour aucune autre fin.
- Dépersonnalisation : Les entreprises devraient utiliser des données dépersonnalisées ou agrégées dans la mesure du possible, à moins que de ce type de données ne permette pas d'atteindre le ou les objectifs visés.
- Durée limitée dans le temps : Tout renseignement personnel recueilli pendant la pandémie doit être détruit à la fin de la crise.
- Transparence : Les personnes doivent être pleinement informées des renseignements qui seront recueillis, des utilisations prévues, des personnes ou organisations qui y auront accès, de l'emplacement où ils seront stockés, des mesures prévues pour les protéger pendant la période de conservation ainsi que du moment où ils seront détruits.

- Responsabilité : Les organisations devraient élaborer un plan de suivi et d'évaluation de l'efficacité de la recherche des contacts.
- Garanties : Des mesures de protection juridiques et techniques appropriées, y compris des dispositions contractuelles robustes conclues avec les développeurs d'application, doivent être mises en place pour assurer la sécurité des données.

Les entreprises ne doivent pas promouvoir ou recommander une application de traçage en particulier sans avoir examiné et compris comment l'application se positionne par rapport aux principes ci-dessus. Les entreprises qui demandent aux personnes de télécharger et d'utiliser une application de traçage avant d'entrer dans leurs locaux doivent informer ces personnes de la manière dont leurs renseignements peuvent être utilisés et des risques en matière de protection des renseignements personnels que l'utilisation de telles applications soulève. Si un programme d'utilisation d'une application de traçage est mis en œuvre, l'entreprise doit consigner les mesures qu'elle prend (communications, formations, etc.) pour assurer sa conformité aux exigences visées.

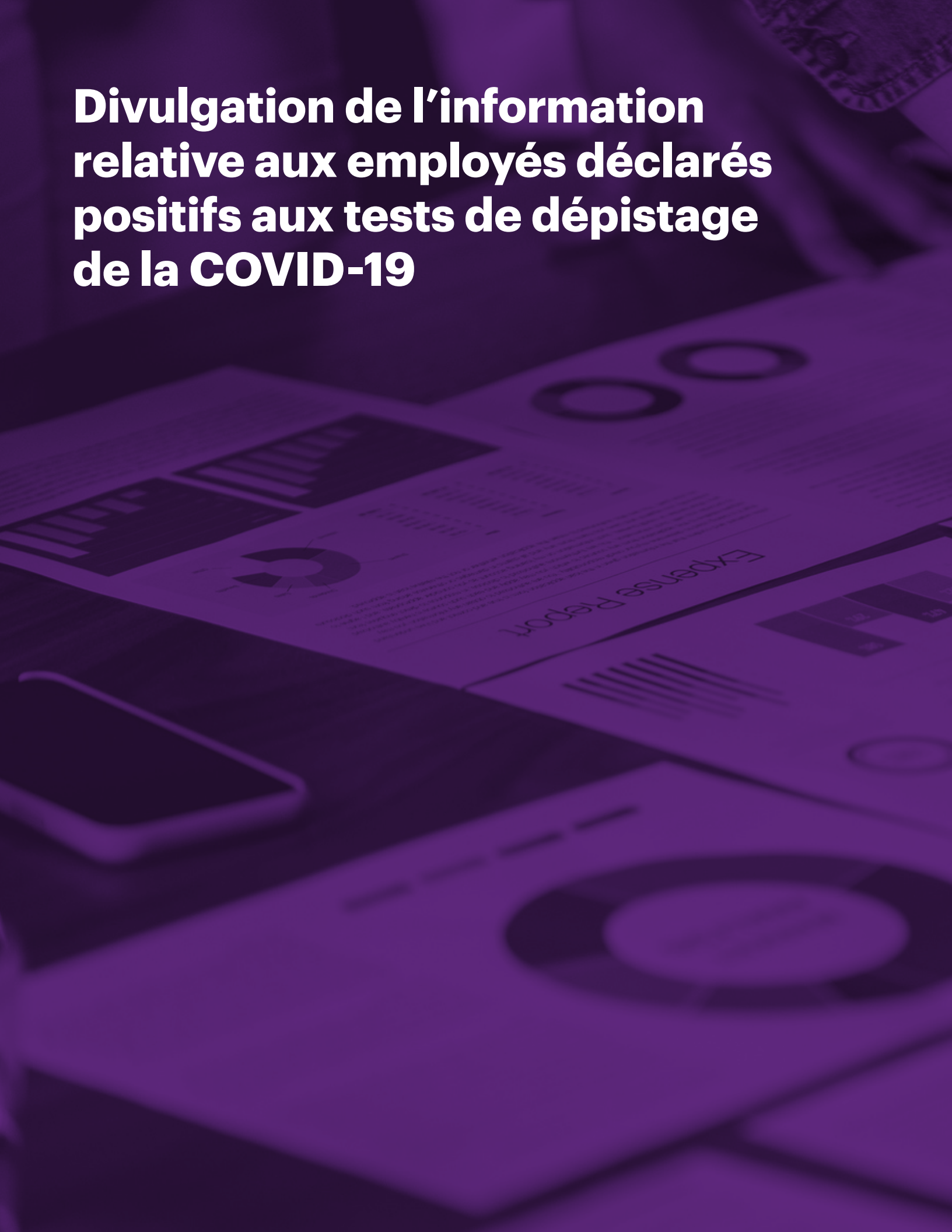
Les entreprises qui se servent d'une application de traçage créée par un tiers doivent avoir conclu des ententes détaillées et précises comprenant des dispositions relatives au partage, à l'utilisation et à la sécurité des données.

Comme pour les entreprises qui choisissent d'utiliser des instruments de mesure de la température corporelle ou des appareils d'imagerie thermique, les entreprises qui choisissent de se servir d'une application de traçage pour contrôler l'accès à leurs lieux de travail doivent s'assurer que les personnes qui ne souhaitent pas télécharger ou utiliser l'application ont un autre moyen d'accéder aux biens ou aux services qu'elles fournissent (p. ex. service de commande en ligne ou service de ramassage à l'extérieur du magasin).

F. Fournisseurs et autres

Les sections précédentes se concentraient surtout sur les employés et les clients, mais la réouverture des entreprises nécessite la réouverture de toute la chaîne d'approvisionnement, ce qui signifie que des fournisseurs de produits et de services auront probablement à pénétrer dans les locaux des entreprises, voir même plusieurs entreprises les unes à la suite des autres. De par la multiplicité des lieux de travail qu'ils visiteront, les fournisseurs sont des vecteurs potentiels d'infection. Les entreprises doivent réfléchir à la manière dont elles vont gérer la situation de ces personnes « itinérantes ». Bon nombre des points dont nous avons parlé dans les pages qui précèdent s'appliquent également aux relations que les entreprises entretiennent avec leurs fournisseurs et les entreprises devraient élaborer un plan de contrôle de l'accès des fournisseurs et d'autres personnes à leurs locaux.

Divulgation de l’information relative aux employés déclarés positifs aux tests de dépistage de la COVID-19



Les entreprises sont tenues par la loi d'assurer la sécurité de leurs milieux de travail. Par conséquent, elles doivent demander à leurs employés de ne pas se présenter au travail s'ils sont malades et ne pas laisser entrer les personnes qu'elles savent malades sur les lieux de travail. Toutefois, le fait d'exiger de leurs employés qu'ils leur divulguent les résultats de leurs tests de dépistage ou des renseignements sur leur état de santé en général soulève quelques questions en matière de protection des renseignements personnels.

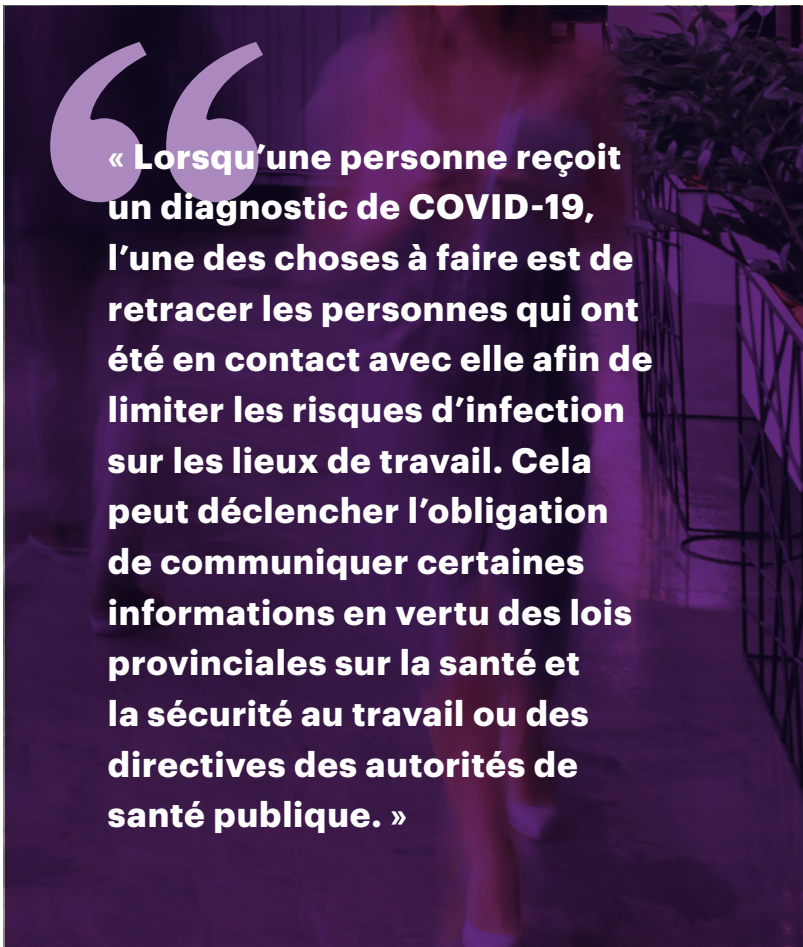
Lorsqu'une personne reçoit un diagnostic de COVID-19, l'une des choses à faire est de retracer les personnes qui ont été en contact avec elle afin de limiter les risques d'infection sur les lieux de travail, ce qui peut déclencher l'obligation de communiquer certaines informations en vertu des lois provinciales sur la santé et la sécurité au travail ou des directives des autorités de santé publique. Les entreprises sont également tenues de consulter tout comité de santé et de sécurité au travail sur les questions de sécurité au travail.

Les lois canadiennes sur la protection des renseignements personnels prévoient des exceptions qui permettent aux entreprises de divulguer des renseignements personnels lorsque cela est nécessaire en raison d'une situation d'urgence, mais la communication du nom d'un employé infecté ou potentiellement infecté n'est pas nécessaire pour atteindre les objectifs de santé et de sécurité en cas de diagnostic positif à la COVID-19. Les entreprises doivent désigner une personne ne faisant pas partie de la chaîne hiérarchique directe de gestion du personnel à qui les rapports relatifs à des employés déclarés positifs à des tests de dépistage seront envoyés et doivent prendre des mesures pour protéger l'identité des personnes infectées. L'information relative au fait qu'un employé a reçu un diagnostic de COVID-19 (ou qu'il est présumé avoir contracté la maladie) doit être communiquée aux autres employés ou clients sans qu'il soit possible d'identifier la personne visée (p. ex. « un employé de notre magasin de Hamilton a été déclaré positif le X »). Tout renseignement qui permettrait aux personnes à qui l'information est communiquée (qu'il s'agisse de collègues de travail ou autres) d'identifier la personne par déduction (p. ex. le fait de dire aux employés qu'un de leurs collègues de l'atelier de production a été déclaré positif à la COVID-19 et que cette personne n'a pas travaillé depuis le X pourrait permettre aux employés de savoir de qui il s'agit) sera considéré comme une information permettant l'identification de la personne infectée, ce qui va à l'encontre des principes de la loi.

Il convient de noter que dans des circonstances ordinaires, il n'est pas conseillé aux employeurs de chercher à obtenir des renseignements relatifs au diagnostic de leurs employés, car ils n'ont pas besoin de cette information pour évaluer leur aptitude au travail. De même, il sera difficile de faire valoir la nécessité d'exiger la divulgation d'information sur un diagnostic médical après la pandémie.

Comme toujours, l'état de santé d'un employé, d'un fournisseur ou d'une autre personne avec laquelle une entreprise est entrée en contact doit être traité comme une information personnelle sensible et ne doit pas être divulgué sans reposer sur des dispositions légales claires. Ces informations devront également être protégées avec le plus grand soin (p. ex. en les cryptant) pour éviter toute perte ou divulgation accidentelle et pour empêcher les employés qui « fouinent » dans les systèmes de tomber dessus.

Les entreprises doivent également établir pendant combien de temps elles conserveront les renseignements visés.



« Lorsqu'une personne reçoit un diagnostic de COVID-19, l'une des choses à faire est de retracer les personnes qui ont été en contact avec elle afin de limiter les risques d'infection sur les lieux de travail. Cela peut déclencher l'obligation de communiquer certaines informations en vertu des lois provinciales sur la santé et la sécurité au travail ou des directives des autorités de santé publique. »

Mobilité des employés

Les gouvernements ont commencé à lever certaines restrictions et les employés ont commencé à retourner sur leurs lieux de travail, ce qui fait que des employés auront peut-être à sortir des dossiers du bureau et à les apporter chez eux. Les modalités de travail flexibles, que ce soit au bureau ou à la maison, ouvrent la porte aux atteintes à la vie privée. Cette section décrit ce que les employés devraient faire pour protéger la confidentialité des renseignements de leur employeur lorsqu'ils travaillent à l'extérieur du bureau.

Sortir des dossiers papier du bureau

Les employés ne devraient sortir des dossiers contenant des renseignements personnels que lorsque cela est absolument nécessaire à l'accomplissement de leurs tâches. Lorsqu'ils doivent apporter des dossiers chez eux, ils devraient faire des copies et laisser les originaux au bureau. Dans la mesure du possible, les employés devraient essayer de travailler uniquement sur des versions électroniques des dossiers et laisser les copies papier au bureau.

Les dossiers papier contenant des renseignements personnels devraient être rangés dans des chemises et transportés dans un porte-documents verrouillé ou une boîte scellée et l'employé devrait les garder près de lui en tout temps durant ses déplacements. Lorsqu'il se déplace en voiture, l'employé devrait toujours mettre les documents papier dans le coffre de la voiture verrouillé et ne jamais laisser la voiture sans surveillance pour aller faire par exemple des emplettes. De même, un employé ne devrait jamais ouvrir ou examiner des documents papier ou électroniques pendant son trajet en transport en commun.

Si un employé doit laisser des documents contenant des renseignements personnels ou confidentiels au bureau, il devrait les placer dans un tiroir, un classeur ou une pièce verrouillé(e) à clé et prendre d'autres mesures de sécurité. Comme il y a moins d'employés dans les lieux de travail, les bureaux sont la cible de voleurs, certains cherchant des objets de valeur et d'autres des renseignements personnels.

Protection des renseignements confidentiels à la maison

Les documents papier peuvent avoir beaucoup de valeur et certaines personnes malhonnêtes fouillent dans les poubelles pour recueillir des renseignements qu'elles pourront utiliser pour créer par exemple des courriels frauduleux (le fraudeur se fait passer pour votre client ou pour un membre de votre équipe qui travaille sur le même dossier que vous afin de vous piéger).

Les règles concernant la destruction de données diffèrent d'un pays à l'autre, mais les deux pratiques suivantes doivent absolument être adoptées à la maison : 1) imprimer le moins de documents possible et 2) ne jeter AUCUN document contenant des renseignements confidentiels sur les clients ou des données à caractère personnel à la poubelle. Les employés peuvent utiliser une déchiqueteuse s'ils sont certains de pouvoir respecter les normes de sécurité s'appliquant au déchiquetage à la maison selon le type de données que contiennent les documents papier visés. Autrement, ils doivent trouver un lieu sécuritaire pour ranger les documents en question jusqu'à ce qu'ils puissent les rapporter au bureau de manière sécuritaire ou les jeter de manière sécuritaire.

Cela pourrait sembler superflu, mais le fait de garder son bureau en ordre et dégagé aidera l'employé à protéger la confidentialité des données clients et des renseignements personnels. Il convient de noter que les membres de la famille de l'employé sont pour les clients de votre organisation des tiers. En gardant son bureau dégagé, l'employé s'assurera qu'ils ne tomberont pas accidentellement sur des renseignements confidentiels.

Enfin, en désignant un coin dans sa maison (et/ou en utilisant un casque d'écoute) pour ses appels privés ou ses conférences téléphoniques avec ses collègues ou clients, l'employé empêchera les personnes non concernées d'entendre des choses qu'elles ne devraient pas entendre. Le fait de toujours travailler au même endroit aidera aussi à protéger les données clients et les renseignements de votre organisation.

Souvenez-vous que la mesure la plus facile qu'un employé peut prendre est de se débarrasser de son habitude d'imprimer tous les documents qu'il doit examiner ou réviser. Enfin, une note pour les

organisations qui détiennent des secrets commerciaux : en règle générale, les secrets commerciaux (qui sont un type de renseignements confidentiels) sont protégés seulement si des mesures raisonnables sont prises pour protéger leur confidentialité et c'est pourquoi il est important de prendre les mesures décrites dans cette section pour protéger les renseignements confidentiels à la maison.

Appareils électroniques

L'accès à l'ordinateur portatif ou à l'ordinateur de bureau à la maison devrait être contrôlé par un mot de passe et toutes les données qui se trouvent sur le disque dur devraient être cryptées. L'employé devrait aussi utiliser d'autres mesures de protection raisonnables, notamment installer un logiciel antivirus et des pare-feux sur l'ordinateur dont il se sert pour travailler. Les employés ne devraient utiliser que des logiciels approuvés par leur organisation.

L'employé doit surveiller son ordinateur portatif en tout temps durant ses déplacements. Si la personne doit absolument consulter des renseignements personnels sur un ordinateur portatif pendant qu'elle est à l'extérieur du bureau, elle doit s'assurer que personne d'autre ne peut voir ce qui s'affiche à l'écran. Un employé ne devrait jamais regarder des renseignements confidentiels sur un ordinateur portatif pendant un trajet en transport en commun.

Lorsque la personne qui travaille de la maison a fini de travailler, elle doit fermer sa session puis éteindre son ordinateur portatif ou ordinateur de bureau. Pour une protection accrue, l'ordinateur devrait être fixé à une table ou à un autre objet au moyen d'un câble de sécurité. L'ordinateur utilisé pour le travail ne doit pas être partagé avec d'autres personnes, même si ce sont des amis ou des membres de la famille.

Des principes similaires s'appliquent pour les appareils sans fil tels que les cellulaires. L'accès à de tels appareils devrait être protégé par un mot de passe et toutes les données qui s'y trouvent devraient être cryptées. Afin de prévenir la perte ou le vol de l'appareil, l'employé devrait le transporter dans un porte-documents verrouillé ou un sac fermé qu'il gardera près de lui durant ses trajets en transport en commun. Si la personne doit absolument consulter des renseignements confidentiels sur un appareil sans fil pendant qu'elle est en public ou dans les transports en commun, elle doit s'assurer que personne d'autre qu'elle ne peut voir ce qui est affiché à l'écran.

De nombreuses entreprises ont dû mettre en place rapidement des systèmes de paiement mobile ou de paiement en ligne. Afin de se protéger et de protéger leurs clients, les entreprises devraient en profiter pour réviser leur processus de gestion des paiements. À titre d'exemple, lorsqu'un client vient chercher les biens que vous lui avez vendus, doit-il vous montrer sa carte?

Quelles mesures de sécurité avez-vous mises en place pour prévenir les échanges de cartes et les autres utilisations malveillantes des renseignements bancaires? Les employés remettent-ils le terminal de point de vente aux clients? Si oui, gardez-vous l'œil ouvert afin d'éviter qu'un terminal soit remplacé par un appareil d'apparence identique par un criminel souhaitant voler des renseignements bancaires.

Obligations d'information

Les employés doivent immédiatement signaler à leur supérieur la perte ou le vol de renseignements personnels ou d'un appareil contenant des renseignements personnels d'employés. L'employeur et son conseiller juridique évalueront la situation afin de déterminer s'il est nécessaire d'aviser les parties concernées et/ou les autorités.

La perte ou le vol de renseignements personnels de clients ou un accès non autorisé à ceux-ci pourrait déclencher des obligations de divulgation et de notification. Il n'est pas souhaitable pour les organisations déjà confrontées à la crise de la COVID-19 de devoir en plus gérer une crise des données. C'est pourquoi nous vous recommandons de réviser vos pratiques en matière de protection des renseignements personnels et de rappeler ces règles à vos employés.

Les entreprises devraient également réviser leurs plans d'intervention en cas d'incident et les mettre à jour afin de tenir compte (a) du télétravail (votre plan était sûrement basé sur le fait que tous vos employés travaillaient au même endroit) et (b) de tous les changements qui sont survenus au niveau des employés : mises à pied, congés ou absences liées à la COVID-19.

« Les entreprises devraient également réviser leurs plans d'intervention en cas d'incident et les mettre à jour afin de tenir compte (a) du télétravail (votre plan était sûrement basé sur le fait que tous vos employés travaillaient au même endroit) et (b) de tous les changements qui sont survenus au niveau des employés : mises à pied, congés ou absences liées à la COVID-19. »

Systèmes de vidéoconférence en ligne

Dans le contexte où les entreprises s'adaptent au télétravail et transfèrent leurs opérations dans l'univers numérique, nombreuses sont celles qui se sont tournées vers les systèmes de vidéoconférence en ligne pour tenir des rencontres virtuelles entre collègues ou avec des clients. Zoom, Google Hangouts, Skype, Slack, Cisco Webex, BlueJeans et Microsoft Teams ne sont que quelques exemples des systèmes de vidéoconférence en ligne qui existent. Vous trouverez ci-après un résumé des questions importantes que soulève l'utilisation de ces systèmes en matière de protection des renseignements personnels ainsi que des pratiques exemplaires à adopter.

Renseignements personnels

Bien souvent, les systèmes de vidéoconférence en ligne recueillent une quantité considérable de renseignements personnels, p. ex. :

- Des renseignements couramment utilisés pour identifier une personne, comme son nom, son nom d'utilisateur, son adresse, son adresse courriel, ses numéros de téléphone ou autres.
- Le titre de la personne et le nom de son employeur.
- Des renseignements bancaires, comme le numéro de carte de crédit ou de débit.
- Des renseignements sur le profil de la personne dans les réseaux sociaux (lorsqu'une personne passe par les réseaux sociaux pour se brancher).
- Des renseignements sur l'appareil de la personne, son réseau et sa connexion internet, comme son ou ses adresses IP, son adresse MAC, d'autres authentifiants comme le numéro d'identification unique de l'appareil, le type d'appareil, le type de système d'exploitation et sa version, etc.
- Des renseignements sur l'utilisation que fait la personne du système de vidéoconférence.
- D'autres renseignements téléversés, présentés ou créés pendant que la personne utilise le système de vidéoconférence.

Vu la quantité de renseignements personnels pouvant être recueillis par un système de vidéoconférence en ligne, il est important que les entreprises et les particuliers lisent et s'assurent de comprendre les politiques en matière de protection des renseignements personnels des systèmes et les conditions d'utilisation de ces derniers. Plus particulièrement, ils doivent s'assurer de bien comprendre de quelles façons le système de vidéoconférence en ligne recueille, utilise, stocke et divulgue les renseignements personnels des personnes qui se créent un compte ou qui ne font qu'utiliser le système. Les entreprises doivent s'assurer que les politiques et conditions d'utilisation des systèmes qu'elles choisissent d'utiliser sont conformes à leurs politiques internes et à leurs obligations en matière de protection des renseignements personnels et de gestion des données. Dans certaines situations, les entreprises pourraient devoir modifier leurs politiques internes afin d'autoriser l'utilisation de tels systèmes.

Les organisations qui fournissent maintenant leurs services en ligne par l'entremise de systèmes de vidéoconférence en ligne devront peut-être mettre à jour leurs politiques en matière de protection des renseignements personnels afin de tenir compte de leur nouvelle réalité et d'y inclure les nouveaux types d'utilisations probables des renseignements personnels.

Enregistrements

De nombreux systèmes de vidéoconférence en ligne permettent à l'hôte d'une vidéoconférence d'enregistrer celle-ci et de sauvegarder l'enregistrement sur le serveur du système ou sur un appareil personnel. Les participants à une vidéoconférence reçoivent normalement une notification lorsque l'hôte décide d'enregistrer celle-ci (si un participant ne veut pas être enregistré, il peut demander à l'hôte de mettre fin à l'enregistrement ou quitter la conférence). Si l'hôte choisit de sauvegarder l'enregistrement sur le serveur du système de vidéoconférence, il devra d'abord s'assurer que les politiques en matière de protection des renseignements personnels du système et les conditions d'utilisation de celui-ci sont compatibles avec les politiques internes et les obligations en matière de protection des renseignements personnels et de gestion des données de son entreprise. La plupart des systèmes de vidéoconférence donnent aux enregistrements un nom par défaut qui dans certains cas peut être facile à deviner et à trouver en ligne pour des personnes malhonnêtes. Pour réduire les risques, il est fortement recommandé de toujours renommer les enregistrements. Si l'hôte choisit de sauvegarder

l'enregistrement localement, il devra s'assurer que l'endroit où il choisit de le sauvegarder répond aux normes de son entreprise en matière de protection des renseignements personnels.

Risque d'infiltration

Récemment, les médias ont rapporté plusieurs cas d'infiltration dans des vidéoconférences ou de détournement de session de vidéoconférence par des tiers, un phénomène appelé « Zoom-bombing ». De telles infiltrations sont possibles lorsque la conférence n'est pas protégée par un mot de passe ou qu'il n'y a pas de « salle d'attente » où les participants sont identifiés avant d'être admis à la vidéoconférence. Le risque augmente lorsque le lien vers la vidéoconférence est publié sur des forums publics ou des réseaux sociaux. Au-delà des risques évidents sur le plan de la confidentialité, de telles infiltrations peuvent causer des dommages à la réputation, réduire la crédibilité d'une personne ou d'une entreprise, vous faire perdre des clients et vous obliger à rétablir la sécurité de vos réseaux de communications. Afin de réduire le risque d'infiltration par un tiers, les hôtes doivent s'assurer que les conférences sont privées et accessibles uniquement aux personnes qui y ont été invitées. Nous vous recommandons aussi de protéger vos vidéoconférences avec un mot de passe, surtout si vous avez l'intention de discuter de sujets sensibles ou d'échanger de l'information confidentielle ou des renseignements personnels. De plus, si vous donnez de la formation à vos employés au sujet de l'utilisation adéquate de ces systèmes, vous contribuerez à prévenir ce type d'incidents.

Envoi de fichiers

L'utilisation des fonctions de partage de liens ou de fichiers dans les systèmes de vidéoconférence présente des risques similaires à ceux qui existent lorsque vous cliquez sur un lien ou ouvrez une pièce jointe dans un courriel. Si une personne malhonnête infiltre votre conférence, elle pourrait être en mesure de convaincre les participants de cliquer sur un lien ou d'ouvrir une pièce jointe qui seront infectés. Dans la mesure du possible, utilisez un système plus sûr qu'un système de vidéoconférence en ligne appartenant à un tiers pour échanger des fichiers avec des collègues ou des clients.

Pratiques exemplaires

Voici des conseils pour utiliser les systèmes de vidéoconférence en ligne tout en protégeant les renseignements personnels et les renseignements appartenant à vos clients et à votre entreprise :

- Choisissez un système de vidéoconférence en ligne qui est suffisamment sécurisé. Voici quelques facteurs à considérer : le niveau de cryptage, la possibilité d'exiger un mot de passe ou d'appliquer une autre méthode d'identification pour filtrer les participants, etc. Portez également attention à la façon dont les données sont gérées. Certains systèmes acheminent les données à l'extérieur du Canada ou stockent les données partagées sur des serveurs contrôlés par le propriétaire du système.
- Établissez des règles et vos attentes en ce qui concerne le type de discussions qui peuvent se dérouler dans un système en particulier (p. ex., vous pourriez interdire la diffusion de matériel confidentiel par l'entremise d'un système de vidéoconférence en ligne). Abstenez-vous de divulguer des renseignements confidentiels ou personnels durant votre vidéoconférence. Si les parties ont l'intention d'échanger de l'information personnelle ou privée, pensez à désactiver l'option permettant aux participants d'enregistrer la conférence. Nous vous recommandons également de concevoir des politiques relatives aux vidéoconférences et de veiller à ce que vos employés et toute autre personne concernée soient au courant des politiques en question.
- Assurez-vous que toutes les personnes qui utiliseront le système de vidéoconférence sont au courant du fait que le propriétaire du système pourrait recueillir des données et les vendre pour réaliser un profit (p. ex., il pourrait vendre une analyse des données recueillies pour des fins de marketing). Nous vous recommandons d'obtenir le consentement du client avant d'utiliser un système de vidéoconférence pour communiquer avec lui (veillez à obtenir son consentement par courriel afin de pouvoir le consigner dans un dossier). Avisez-le plus particulièrement du fait que le propriétaire du système est en mesure de recueillir des données et qu'il pourrait utiliser celles-ci.

- Tenez-vous au courant de tous les développements concernant le système de vidéoconférence que vous utilisez. Plusieurs sites Web et médias fiables publient des nouvelles au sujet des failles décelées dans les systèmes de vidéoconférence.
- Révisez la politique en matière de protection des renseignements personnels de votre entreprise afin de vous assurer qu'elle autorise l'utilisation de systèmes de vidéoconférence en ligne (si ce n'est pas le cas, veillez à y ajouter de telles dispositions).
- Lorsque vous vous créez un compte dans un système de vidéoconférence en ligne, ne vous inscrivez pas en utilisant vos comptes de réseaux sociaux. Nous vous recommandons d'utiliser une adresse courriel et un mot de passe unique pour accéder au système afin de limiter la quantité de renseignements personnels que le système peut recueillir.
- Afin de prévenir les intrusions par des tiers, assurez-vous que vos conférences sont privées et que seules les personnes qui ont été invitées peuvent y accéder. Dans la mesure du possible, protégez vos vidéoconférences avec un mot de passe, particulièrement si vous avez l'intention de mentionner des renseignements personnels pendant votre discussion. Vous empêcherez ainsi les personnes indésirables de se joindre à la conférence.
- Soyez conscients de votre environnement durant la conférence, c'est-à-dire de la pièce ou de l'endroit où vous êtes (les personnes et les objets qui sont visibles en arrière-plan peuvent révéler des choses sur vous que vous ne voulez pas nécessairement que les gens sachent), et de qui peut vous entendre (vous devrez peut-être porter un casque d'écoute ou vous isoler dans une pièce afin d'éviter que d'autres personnes entendent votre conversation).
- Si vous installez une application de vidéoconférence sur votre téléphone, tablette ou ordinateur, assurez-vous de passer en revue les autorisations que vous accordez à l'application et de garder celle-ci à jour. Les développeurs publient régulièrement des mises à jour pour améliorer les fonctionnalités de leur outil et pallier les vulnérabilités qui ont été décelées.
- Si vous utilisez un navigateur Web pour tenir votre vidéoconférence, nous vous recommandons d'ouvrir une nouvelle fenêtre et de ne laisser aucun autre onglet ouvert. Il est aussi préférable de fermer toutes les autres applications afin d'éviter que les autres participants voient par exemple les notifications de votre boîte de messagerie.
- Avant d'enregistrer une vidéoconférence, même localement, obtenez le consentement des participants. N'enregistrez pas les conférences sur le nuage du fournisseur à moins que cela soit conforme à la politique interne de votre entreprise en matière de protection des renseignements personnels.

Surveillance des employés

Comme bon nombre d'employés seront appelés à continuer à travailler de chez eux, les entreprises chercheront des moyens de surveiller les personnes qui ne sont plus au bureau sous la supervision directe de leur gestionnaire. Les employeurs disposent d'un certain nombre d'outils de surveillance des employés, mais ces derniers ne sont pas nécessairement adaptés aux activités particulières d'une entreprise. Il convient de déterminer si l'utilisation de ces outils est autorisée afin de choisir le bon. Les employeurs ont le droit de surveiller les activités de leurs employés et de protéger leurs systèmes informatiques et leurs informations confidentielles, mais les lois canadiennes sur la protection des renseignements personnels imposent des limites au regard de la portée de la surveillance technologique.

Les logiciels de sécurité informatique peuvent conduire à une collecte excessive d'informations personnelles sur les employés, en particulier lorsque ces derniers utilisent des appareils ou des ordinateurs personnels pour accéder aux systèmes de leur entreprise dans le cadre de leur travail. Par conséquent, les organisations devraient envisager la possibilité de réaliser une EFVP et demander à leur responsable de la protection des renseignements personnels de collaborer avec les équipes des TI et de l'approvisionnement afin d'élaborer un programme de surveillance et de choisir un outil adéquat.

En supposant qu'au terme d'une EFVP rigoureuse, l'entreprise détermine que l'utilisation des outils de surveillance des employés est raisonnablement justifiée, elle devrait envisager les meilleures pratiques suivantes pour la mise en œuvre des programmes et protocoles de sécurité :

- Les employés doivent être informés que des programmes ont été mis en place et que des renseignements sont recueillis lorsqu'ils accèdent aux systèmes de l'entreprise. L'avis (qui de façon générale peut être inclus dans les conditions d'utilisation de l'entreprise) doit préciser l'objectif de la collecte d'information, le fonctionnement du système, les fins auxquelles les renseignements seront utilisés et la ou les personnes avec qui communiquer pour obtenir de plus amples renseignements.
- Éviter la collecte continue et en temps réel de renseignements personnels, comme l'enregistrement des frappes au clavier ou la capture d'écran. Ces pratiques doivent être réservées à des enquêtes ciblées lorsqu'on peut raisonnablement soupçonner que la ou les personnes ont commis des actes répréhensibles.

- Éviter de collecter plus d'informations que nécessaire. Les programmes fourre-tout entraîneront la collecte de plus de renseignements personnels que nécessaire, ce qui contrevient aux lois canadiennes sur la protection des renseignements personnels.
- Établir des politiques et donner de la formation aux employés qui utiliseront les outils de surveillance. La formation devrait comprendre non seulement une formation technique sur l'utilisation du logiciel et une formation sur la sécurité, mais aussi une formation sur la protection des renseignements personnels. Dans la mesure où cela ne compromet pas la sécurité, mettez le matériel de formation et les politiques à la disposition des employés aux fins de transparence.
- Enregistrer l'accès aux systèmes et examiner périodiquement les registres pour s'assurer que le système est utilisé correctement.
- Évaluer périodiquement l'efficacité du programme, notamment en déterminant s'il existe un moyen moins intrusif de traiter les problèmes que le programme vise à résoudre.

Comme l'a indiqué le commissaire à la protection de la vie privée du Canada, l'adoption d'une approche souple et contextuelle dans l'application des lois sur la protection des renseignements personnels pendant cette pandémie pourrait permettre une utilisation plus large des outils de surveillance des employés. Par contre, cela doit être fondée sur une justification légitime. Les entreprises doivent également se demander si la raison de la surveillance proposée est raisonnable et si leurs objectifs peuvent être atteints d'une autre manière. Malgré les difficultés liées au travail à distance, les logiciels de surveillance ne remplacent pas la gestion personnelle.

En outre, la mise en œuvre de tels outils et programmes peut être raisonnable aujourd'hui, mais elle pourrait ne plus l'être à mesure que le pays et l'économie rouvriront. Les entreprises ne doivent pas supposer que ce qui est permis aujourd'hui le sera à l'avenir, et doivent suivre avec attention l'évolution de la situation.

Personnes-ressources

Kirsten Thompson
Chef du groupe national
Technologies transformatrices et stratégies de gestion des données
D +1 416 863 4362
kirsten.thompson@dentons.com

Kelly Osaka
Associée
D +1 403 268 3017
kelly.osaka@dentons.com

Chantal Bernier
Avocate-conseil
D +1 613 783 9684
chantal.bernier@dentons.com

Elizabeth Allum
Avocate
D +1 403 268 3003
elizabeth.allum@dentons.com

Taylor Buckley
Avocat principal
D +1 604 648 6522
taylor.buckley@dentons.com

Luca Lucarini
Avocat
D +1 416 863 4735
luca.lucarini@dentons.com

Karl Schober
Avocat principal
D +1 416 863 4483
karl.schober@dentons.com

Chloe Snider
Associée
D +1 416 863 4674
chloe.snider@dentons.com

Dentons, dont les membres œuvrent dans 184 bureaux répartis dans 76 pays, est à l'avant-plan de la réponse juridique à la COVID-19 depuis le début de la crise. Pour obtenir de plus amples renseignements sur les questions juridiques que la COVID-19 soulève partout dans le monde, veuillez consulter notre Centre de ressources COVID-19 à l'adresse https://www.dentons.com/en/issues-and-opportunities/covid-19-coronavirus-hub. Nos avocats, qui sont plus de 10 000 dans le monde, sont prêts à vous aider à relever tous les défis à l'échelle mondiale.

À PROPOS DE DENTONS

Dentons est le plus grand cabinet d'avocats au monde. Dans plus de 75 pays, ses professionnels de haut calibre, bien ancrés dans leurs collectivités et avec l'appui des innovations reconnues du cabinet en matière de service à la clientèle, dont Nextlaw, service de consultation stratégique d'avant-garde, offrent à ses clients des solutions qui allient acuité juridique et sens des affaires. Fort de sa démarche polycentrique axée sur les objectifs à atteindre, de son engagement à favoriser l'inclusion et la diversité et de ses effectifs de haut calibre, Dentons défie le statu quo et défend les intérêts de ses clients et des collectivités en cette ère de la Nouvelle dynamique.

dentons.com

© 2020 Dentons. Dentons est un cabinet d'avocats mondial qui sert ses clients partout dans le monde grâce à ses cabinets membres et aux membres de son groupe. La présente publication n'est pas destinée à constituer un avis d'ordre juridique ou autre et vous ne devriez pas agir ou vous abstenir d'agir sur la foi de son contenu. Veuillez consulter les avis juridiques à l'adresse dentons.com.

CSBrand-30922-Return-to-Work-Toolkit-Dentons-Data-FRE 02 — 30/07/2020