# Dix conseils pour empêcher les employés de fureter

Les organismes publics et les dépositaires détiennent de grandes quantités de renseignements personnels et de renseignements médicaux personnels sur les Manitobains et Manitobaines pour fournir divers services, programmes et prestations. Il est parfois difficile de faire en sorte que ces renseignements ne soient consultés que par les employés qui en ont besoin, et seulement lorsqu'ils sont nécessaires à des fins professionnelles légitimes – mais c'est un défi qui doit être relevé.

En l'absence de mesures de protection appropriées, la curiosité humaine et d'autres motivations (y compris la volonté de causer du tort à une personne ou l'appât du gain) peuvent mener certains employés à consulter des renseignements personnels sans autorisation et sans motif légitime lié à leur travail – c'est ce qu'on appelle le « furetage ».

Le fait, pour un employé, de consulter ou de visionner des renseignements personnels est considéré comme une forme d'« utilisation » de ces renseignements. Selon la Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP) et la Loi sur les renseignements médicaux personnels (LRMP), les renseignements personnels et les renseignements médicaux personnels ne doivent pas être utilisés (ni communiqués) sauf pour des motifs autorisés sous le régime de ces lois. Les deux lois exigent que ces renseignements soient protégés par des garanties satisfaisantes contre certains risques comme l'accès, l'utilisation, la communication et la destruction non autorisées. En outre, la LRMP exige que les garanties administratives, techniques et physiques tiennent compte du niveau de sensibilité des renseignements médicaux personnels.

Même si le furetage correspond aux actions non autorisées d'un employé à des fins qui lui sont propres, l'obligation de rendre compte revient néanmoins à l'organisme public ou au dépositaire qui a la responsabilité de protéger les renseignements personnels contre l'utilisation ou la communication non autorisée. Nous donnons ci-dessous des conseils sur ce que les organismes publics et les dépositaires (organisations) peuvent faire pour empêcher les employés de fureter et pour prévenir de telles situations.

Le présent document est une adaptation de la publication du Commissariat à la protection de la vie privée du Canada intitulée *Dix trucs pour empêcher les employés de fureter* et destinée aux organisations du secteur privé qui sont assujetties à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Cette publication a été modifiée avec la permission du Commissariat.

**Ombudsman du Manitoba**

**www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1 800 665-0531 | 204 982-9130**

# ÉDUQUER

## 1 Favorisez une culture de protection de la vie privée

Au sein d'une organisation, la culture de protection de la vie privée est ce qu'il y a de plus important pour prévenir le furetage, parce qu'elle appuie l'efficacité de toutes les autres mesures. L'engagement de l'organisation à l'égard du respect de la vie privée et des pratiques exemplaires dans ce domaine est d'autant plus efficace que la direction se montre elle-même engagée et appuie les efforts en ce sens.

La mise en place d'une telle culture commence par l'établissement d'attentes et d'exigences claires envers les employés. Élaborez un ensemble exhaustif de politiques et de procédures en matière de protection de la vie privée, et transposez-les et mettez-les en place dans des pratiques concrètes pour faire en sorte que les employés : i) comprennent que la protection de la vie privée est une valeur organisationnelle de base et ii) sachent ce que cela signifie dans le cadre de leurs activités de tous les jours. De plus, donnez à l'agent chargé de la protection de la vie privée de votre organisation (ou à un autre responsable) le mandat clair d'éduquer les employés, de surveiller le respect des obligations, de faire enquête et de traiter les cas d'infraction. Lorsque l'on met à l'avant-plan l'importance de la protection de la vie privée et des pratiques qui s'y rattachent, les employés sont moins enclins à fureter sans réfléchir, ce qui aide à éviter les incidents dus à l'impulsivité, aux malentendus ou à la curiosité.

## 2 Offrez une formation périodique ou « ponctuelle » et des rappels au sujet des politiques sur le furetage

Souvent, les renseignements sur les obligations en matière de protection de la vie privée font partie de la trousse d'orientation que l'employé reçoit lorsqu'il est embauché. Bien qu'il s'agisse là d'une bonne pratique, cela ne devrait pas être la seule fois où ces obligations devraient être présentées aux employés. Une formation et des rappels réguliers font en sorte que les connaissances restent à jour. Incorporez des exemples pratiques qui sont adaptés à votre milieu de travail. De plus, lorsque c'est possible, utilisez un rappel « ponctuel » sous la forme, par exemple, d'un simple autocollant sur un classeur ou d'un message apparaissant à l'ordinateur dans une fenêtre flash, pour présenter aux employés des renseignements clés sur leurs obligations en matière de protection de la vie privée au moment précis où ils risquent d'en avoir besoin.

## 3 Assurez-vous que les employés savent que les infractions entraîneront des conséquences

Que ce soit en raison de leur curiosité, d'une demande d'une autre personne ou de l'attrait d'un gain quelconque, notamment financier, certains employés peuvent être incités à fureter. Il revient aux organisations de s'assurer que leurs employés savent que le furetage peut avoir de graves répercussions. Les employés devraient comprendre que : i) le furetage peut avoir de lourdes conséquences et entraîner de graves dommages, ii) l'organisation prend des mesures pour repérer et dissuader les fureteurs, et iii) les fureteurs subiront les conséquences de leurs actes. L'absence de l'un ou l'autre de ces trois facteurs aura un impact négatif sur l'efficacité des mesures d'une organisation visant à prévenir le furetage.
Un bon moyen d'accroître la sensibilisation est de demander aux employés de signer (au moment de l'embauche et à intervalles réguliers par la suite) des ententes de confidentialité portant à la fois sur l'accès non autorisé aux renseignements personnels et sur la communication non autorisée de ces renseignements. Les organisations qui détiennent des renseignements personnels devraient savoir qu'aux termes de la LRMP, les employés et les mandataires d'un dépositaire doivent signer une promesse de confidentialité.

# PROTÉGER

## 4 Veillez à ce que l'accès soit limité aux renseignements quisont nécessaires pour remplir les fonctions du poste

L'accès d'un employé aux renseignements personnels et aux renseignements médicaux personnels devrait être accordé à celui-ci en fonction de son rôle de façon qu'il ne puisse consulter que les renseignements dont il a besoin pour exercer ses fonctions. Si c'est possible, cela signifie par exemple que l'employé ne peut avoir accès qu'aux renseignements les moins délicats d'une personne ou qu'à ceux qui concernent un nombre limité de personnes, que son accès est limité à certaines périodes ou à certains endroits, ou que d'autres restrictions s'appliquent. Les organisations devraient aussi avoir des processus documentés pour accorder ou révoquer l'accès aux renseignements, selon les besoins (p. ex. lorsqu'un employé change de rôle). Plus particulièrement, lorsque les renseignements sont de nature délicate, elles devraient utiliser des moyens matériels (p. ex. le verrouillage des classeurs) ou des mesures administratives (p. ex. politiques et conséquences appropriées) et techniques (p. ex. permissions d'accès restreint) pour prévenir l'accès inapproprié aux renseignements.

## 5 Prévoyez des mesures pour pouvoir bloquer l'accès de certains employés aux renseignements de certaines personnes

Il peut y avoir des situations où une personne a une raison légitime de souhaiter qu'un ou plusieurs employés d'une organisation (p. ex. des membres de la famille ou d'ex-conjoints avec lesquels la personne a une relation litigieuse) ne puissent avoir accès à ses renseignements personnels. Les organisations devraient donc prévoir des moyens leur permettant autant que possible de donner suite à de telles demandes, en appliquant les procédures destinées à prévenir ou à surveiller l'accès de l'employé ou des employés à ces renseignements. Il va sans dire que l'employé dont l'accès a été bloqué ne doit pas pouvoir contourner cette mesure.

## 6 Établissez des registres ou adoptez d'autres outils de surveillance

L'accès inapproprié peut ne pas être décelé immédiatement. Des incidents peuvent être mis au jour au bout d'un certain temps ou à la suite d'une plainte. L'établissement de registres d'accès, pour les renseignements électroniques, ou l'adoption d'autres outils de surveillance permettra à l'organisation de faire enquête sur les allégations de furetage et de confirmer ou rejeter ces allégations après l'examen de ces registres*. Le fait d'informer les employés de l'existence de ces mesures de surveillance joue également un rôle clé dans la dissuasion. Si les employés se rendent compte qu'il y a de fortes probabilités qu'ils se fassent prendre, ils risquent beaucoup moins d'être enclins à fureter.

# SURVEILLER

## 7 Surveillez et vérifiez de façon proactive vos registres d'accès et autres outils de surveillance

En plus d'utiliser des registres d'accès pour faire enquête sur les incidents allégués, il est important que les organisations aient en place des mesures proactives pour surveiller tout accès non autorisé ou pour procéder à une vérification en cas de furetage non détecté. De telles mesures sont essentielles pour détecter et empêcher l'accès non autorisé des employés aux renseignements, et elles sont particulièrement importantes pour les organisations qui, pour des raisons opérationnelles, doivent permettre à leurs employés d'accéder facilement aux renseignements des clients ou des patients. Ceci peut se faire sous forme de vérifications régulières des employés ou de vérifications au hasard dans le cas des organisations de grande taille*. De plus, afin de maximiser la dissuasion, il faut faire savoir aux employés que ces mesures proactives sont effectivement utilisées. En l'absence de mesures de détection proactives, les employés pourraient continuer indéfiniment de fureter sans que la personne visée, ni même l'organisation, ne soient au courant.

*Veuillez consulter les exigences précises de la LRMP sur les documents concernant l'activité des utilisateurs et leur examen.

## 8 Sachez ce qu'est un accès « normal » pour être mieux en mesure de détecter les cas d'accès inapproprié

Un employé a accédé aux renseignements personnels d'une certaine personne dix fois dans une même semaine, ou une fois par semaine pendant une année. Un autre employé a accédé une fois à 900 dossiers différents sur une période de deux ans. Ces comportements sont-ils révélateurs d'un problème? Les organisations devraient comprendre, en matière d'accès, les tendances de base qui se rattachent à différents rôles pour mieux relever les anomalies. Des alertes peuvent ensuite être programmées pour signaler à l'organisation les comportements potentiellement problématiques.

# INTERVENIR

## 9 Faites enquête sur toutes les allégations de furetage par des employés

En raison de leur gravité potentielle, les allégations de furetage par des employés doivent être prises au sérieux. Lorsque notre bureau apprend qu'un employé s'adonne à une telle activité, nous nous attendons à ce que l'organisation concernée puisse montrer qu'elle a entrepris une enquête rigoureuse et opportune et, lorsqu'il était approprié de le faire, qu'elle a pris les mesures nécessaires pour régler le problème d'accès non autorisé de l'employé aux renseignements personnels, pour atténuer les préjudices actuels ou futurs causés à la personne touchée et pour réduire la probabilité que l'incident se reproduise (cela pouvant inclure la révision des politiques, le renforcement des mesures de sécurité, l'accroissement de la surveillance ou d'autres mesures semblables).

## 10 Lorsque les mesures proactives échouent, intervenez de manière appropriée

Il y a des circonstances où aucune mesure proactive raisonnable n'aurait permis d'empêcher un employé de fureter ou de détecter ce genre d'incident. Dans ces cas, il est important que l'organisation intervienne de façon appropriée. Elle peut notamment imposer des sanctions au fureteur (y compris des mesures disciplinaires) et signaler l'incident à la personne touchée (en lui donnant suffisamment de renseignements, comme la durée et la portée de l'infraction, pour lui permettre de prendre des mesures afin d'atténuer les impacts potentiels de l'incident). Elle peut aussi aviser notre bureau de la situation.

Le furetage représente un risque grave pour la protection de la vie privée et, si ce risque n'est pas écarté, il peut causer de lourdes pertes financières et nuire pendant longtemps à la réputation des personnes concernées mais aussi de votre organisation. En veillant au respect de la LAIPVP et de la LRMP et en prenant les mesures nécessaires pour atténuer ce risque, notamment en adoptant les pratiques décrites ci-dessus, vous pouvez faire beaucoup pour renforcer votre réputation à titre d'organisation sensibilisée à la protection de la vie privée et surtout pour protéger les renseignements qui vous sont confiés sur la population du Manitoba.

**Ombudsman du Manitoba**
Maintient vos droits à l'information et à la protection de la vie privée
www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1 800 665-0531 | 204 982-9130