Commissariat
à la protection de la
vie privée du Canada

BUREAU EN GROS

Rapport de vérification de la commissaire à la protection de la vie privée du Canada

Article 18 de la *Loi sur la protection des renseignements personnels et les documents électroniques*

RAPPORT FINAL

2011

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

613-947-1698, 1-800-282-1376
Télécopieur : 613-947-6850
ATS : 613-992-9190
Suivez-nous sur Twitter : @privacyprivee

No de catalogue IP54-39/2011F-PDF
ISBN 978-1-100-97441-5

Cette publication se trouve également sur notre site Web au : **www.priv.gc.ca**.

Table des matières

Points saillants

PORTÉE DE L'EXAMEN

De 2004 à 2008, le Commissariat à la protection de la vie privée (le Commissariat) a enquêté sur deux plaintes selon lesquelles Bureau en gros n'avait pas protégé adéquatement les renseignements personnels qu'elle avait en sa possession. Les deux plaintes étaient liées à l'achat et au retour d'un dispositif de stockage de données. Dans les deux cas, les dispositifs retournés contenaient encore des renseignements personnels de l'acheteur. Bureau en gros a revendu les dispositifs sans effacer les données, ce qui a entraîné la communication inappropriée de renseignements personnels à d'autres clients. Dès que Bureau en gros a accepté de modifier certaines de ses méthodes, les plaintes ont été considérées comme résolues. En effet, à la suite de la plainte déposée en 2008, l'entreprise a accepté d'instaurer une procédure complète de nettoyage et de restauration de tous les dispositifs de stockage de données retournés. Plus tard, les médias ont toutefois affirmé qu'il s'était reproduit un incident semblable au sein de l'entreprise. Le contexte dans lequel les plaintes ont été déposées et la couverture médiatique qui en a découlé comptent parmi les facteurs qui ont incité la commissaire adjointe à la protection de la vie privée à conclure que Bureau en gros n'avait pas instauré de procédures de nettoyage et de restauration suffisamment efficaces pour protéger adéquatement les renseignements personnels des clients et qu'elle contrevenait peut-être à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE ou la Loi). La commissaire adjointe a donc jugé qu'il y avait des motifs raisonnables pour déclencher une vérification des pratiques de gestion des renseignements personnels de Bureau en gros.

Nous avons examiné les politiques, les pratiques et les processus de gestion des renseignements personnels de Bureau en gros en mettant l'accent sur la gestion des dispositifs de stockage de données retournés. Nous avons inspecté des points de vente au détail choisis afin d'évaluer les mécanismes de contrôle de nature physique et informatique mis en place pour assurer la sécurité des renseignements personnels. Nous avons également examiné les processus opérationnels, les formulaires ainsi que le programme de formation et de sensibilisation en matière de protection de la vie privée. Enfin, nous avons vérifié les dispositifs de stockage de données destinés à la revente pour déterminer s'ils avaient été correctement nettoyés et restaurés.

IMPORTANCE DE L'EXAMEN

Chaque année, les Canadiennes et les Canadiens achètent un nombre considérable d'ordinateurs de bureau, d'ordinateurs portatifs, de disques durs externes, de clés USB et d'appareils photo numériques. Ces appareils permettent de conserver d'énormes quantités de données, y compris des renseignements personnels. Les documents et les images qui se trouvaient auparavant dans des dossiers, des tiroirs ou des classeurs se trouvent de plus en plus souvent sur des ordinateurs personnels ou des appareils électroniques.

Un grand nombre d'entreprises de vente au détail ont adopté une politique de « satisfaction garantie ou argent remis » pour leurs activités commerciales. Les consommateurs peuvent acheter un article, l'utiliser un certain temps et, s'ils n'en sont pas satisfaits, le retourner pour obtenir un remboursement complet. Par ailleurs, les appareils informatiques et électroniques sont généralement assujettis à une garantie du

fabricant aux termes de laquelle le consommateur peut retourner un produit défectueux dans un délai prédéterminé et en obtenir le remplacement. Certains de ces articles sont remis en état, remballés et revendus.

Cette pratique comporte le risque intrinsèque que ces produits soient revendus sans que les renseignements personnels qui s'y trouvent soient entièrement supprimés, menaçant ainsi les renseignements personnels des acheteurs antérieurs. La communication non autorisée de tels renseignements peut avoir de graves conséquences pour ces derniers, par exemple des pertes financières attribuables à l'usurpation d'identité ou à la fraude, une humiliation ou une atteinte à la réputation.

La mise en œuvre de politiques, de procédures et de mécanismes de contrôle visant à ce que les renseignements personnels soient suffisamment protégés est un élément essentiel d'une bonne gestion de la protection de la vie privée. Étant assujettie à la LPRPDE, Bureau en gros est tenue de prendre des mesures de nature technologique, physique et organisationnelle pour préserver l'intégrité et la sécurité des renseignements personnels de ses clients — y compris des données qui se trouvent sur les produits retournés ou en réparation.

CONSTATATIONS

Bureau en gros a fondé sa politique sur les dix principes de protection de la vie privée énoncés à l'annexe 1 de la Loi. Ces principes ont été intégrés à une série de politiques et de procédures de l'entreprise. La responsabilité liée à l'observation de la Loi est bien établie et connue. Les employés sont conscients de l'importance de protéger les données des clients ainsi que de leurs rôles et responsabilités à ce chapitre.

Nous avons constaté que Bureau en gros ne recueille généralement que les renseignements personnels nécessaires pour offrir un service. Toutefois, les clients ne sont pas toujours informés de la façon dont leurs renseignements seront utilisés ou du fait que cette information pourrait être acheminée aux États-Unis pour y être traitée.

Bureau en gros offre un service de photocopie et d'impression en ligne pour les clients du secteur privé et le public en général. Un formulaire de demande avec les données à imprimer attachées sont envoyés électroniquement. Ces documents sont conservés pendant un an pour faciliter le traitement des commandes subséquentes portant sur les mêmes données. Cette pratique aide peut-être à répondre aux besoins des clients, mais conserver des renseignements personnels — y compris des curriculum vitæ et des documents juridiques comme des ententes de divorce ou de garde — sous prétexte qu'ils pourraient servir un jour contrevient à la bonne gestion de la protection de la vie privée et au principe de la limitation de la conservation.

Selon la politique de Bureau en gros, tous les renseignements personnels doivent être rangés dans un endroit sécurisé, comme un classeur ou une pièce verrouillés, lorsqu'ils ne servent pas. Nous avons relevé d'importantes lacunes à cet égard. Des formulaires de livraison, de transfert et de commande spéciale étaient rangés dans des classeurs non verrouillés et nous avons vu des dispositifs de stockage de données retournés placés sur des étagères ouvertes ou laissés sans surveillance à des comptoirs de services. Nous avons aussi remarqué des formulaires de commande renfermant des renseignements personnels jetés dans des poubelles ou des bacs de recyclage.

Avant la vérification, dans le but d'éviter une autre atteinte à la protection des données, Bureau en gros a révisé ses procédures de traitement des appareils informatiques et électroni-ques de stockage de données qui ont été retournés. Ces procédures, qui comprennent de solides mécanismes de contrôle, ne sont pas toujours appliquées. Dans 15 des 17 succursales inspectées, nous avons observé que des dispositifs étaient remballés et faisaient l'objet d'une certification attestant qu'ils avaient été nettoyés alors que ce n'était pas le cas, n'étaient pas vérifiés par un gérant avant d'être replacés dans les stocks ou étaient retournés directement au fournisseur sans avoir été nettoyés.

Nous avons testé 149 dispositifs de stockage de données qui avaient été emballés pour la revente, et qui avaient subi le processus de nettoyage et de restauration de Bureau en gros. L'échantillon comprenait des ordinateurs de bureau, des ordinateurs portatifs, des disques durs externes et des cartes mémoire. Nous avons constaté que 54 des 149 appareils testés contenaient des données (des données qui avaient été stockées dans le dispositif, intentionnellement ou non, par le client ou pour celui-ci). Un certain nombre d'entre eux comprenaient des renseignements personnels, y compris des numéros d'identification émis par le gouvernement, des états financiers, des antécédents professionnels, des renseignements médicaux, des courriels, des lettres personnelles et des photographies. La question de la gestion des dispositifs de stockages de données retournés n'est donc pas encore réglée.

Le contrôle de l'accès à un système de TI et aux données qui y sont stockées constitue une importante mesure de protection de la vie privée. En effet, la possibilité que des renseignements personnels soient menacés est réduite puisque l'accès est uniquement accordé à ceux qui ont un besoin légitime. Nous avons remarqué que les activités des utilisateurs ne sont pas enregistrées pour déterminer si le droit d'accès a été exercé correctement. Sans un moyen de surveiller l'accès au système, Bureau en gros ne peut affirmer, avec un degré de certitude raisonnable, que les données des clients sont toujours utilisées et communiquées à des fins légitimes.

La conformité aux procédures et aux contrôles de sécurité est évaluée dans le cadre du programme de vérification interne de Bureau en gros. Toutefois, l'organisation n'a pas été en mesure de produire des documents prouvant que la collecte, la conservation et l'élimination de renseignements personnels font l'objet d'examens officiels. Une stratégie de surveillance continue comprenant des vérifications permettrait d'atténuer les risques pour la vie privée et de donner une certaine assurance que les principes relatifs à l'équité dans le traitement de l'information sont respectés dans le contexte des opérations courantes de Bureau en gros.

Bureau en gros a réagi aux recommandations que nous avons formulées à la suite de notre vérification et s'est engagée à étudier des moyens pour la mise en application de chacune d'entre elles, sauf une. Les réponses formulées par l'organisation figurent en italique après chacune des recommandations du Commissariat. Les recommandations et les réponses ont été reproduites à l'annexe A de ce rapport.

Introduction

À PROPOS DE L'ORGANISATION FAISANT L'OBJET DE LA VÉRIFICATION

1. Bureau en gros ltée (Bureau en gros) est un grand détaillant de fournitures, de mobilier et de machines de bureau ainsi que de dispositifs électroniques de stockage de données comme des ordinateurs de bureau, des ordinateurs portatifs, des disques durs et des dispositifs de stockage portables. Bureau en gros nous a informés qu'elle accepte un certain nombre d'appareils électroniques retournés par des clients insatisfaits, conformément à sa politique sur les retours. L'entreprise exploite plus de 300 points de vente au détail partout au Canada; elle se spécialise dans les services offerts aux petites entreprises et aux clients qui travaillent à la maison. Toutes les activités commerciales sont coordonnées par le siège social de Bureau en gros à Richmond Hill (Ontario).

2. En plus des ventes au détail, Bureau en gros offre des services de photocopie et d'impression, parfois en libre-service. Les demandes de services de photocopie et d'impression peuvent être présentées en personne ou en ligne. Chaque succursale possède également un centre technique offrant des services de réparation et de mise à niveau d'ordinateurs et d'installation de logiciels. Des renseignements supplémentaires sur Bureau en gros se trouvent sur le site Web officiel de l'entreprise : http://www.staples.ca/FRA/Catalog/stap_home.asp.

MOTIFS RAISONNABLES POUR LA VÉRIFICATION

3. Entre 2004 et 2008, le Commissariat a enquêté au sujet de deux plaintes selon lesquelles Bureau en gros avait omis de protéger adéquatement les renseignements personnels qu'il avait en sa possession. Les deux plaintes étaient liées à l'achat et au retour de dispositifs électroniques de stockage de données. Dans les deux cas, les dispositifs retournés contenaient encore des renseignements personnels de l'acheteur. Bureau en gros a revendu les dispositifs sans effacer les données, ce qui a entraîné la communication inappropriée de renseignements personnels à d'autres clients.

4. Le Commissariat a conclu que Bureau en gros n'a pas suffisamment protégé les renseignements personnels des plaignants, ce qui a entraîné les communications non autorisées. Les plaintes ont été résolues quand Bureau en gros a accepté de prendre des mesures correctives. À la suite de la plainte déposée en 2008, l'entreprise a accepté d'instaurer une procédure complète de nettoyage et de restauration de tous les dispositifs de stockage de données retournés. Plus tard, les médias ont affirmé qu'il s'était reproduit un incident semblable au sein de l'entreprise. Le contexte dans lequel les plaintes ont été déposées et la couverture médiatique qui en a découlé comptent parmi les facteurs qui ont incité la commissaire adjointe à la protection de la vie privée à conclure que Bureau en gros n'avait pas instauré de procédures

de nettoyage et de restauration suffisamment efficaces pour protéger les renseignements personnels des clients et qu'elle contrevenait peut-être à la *Loi sur la protection des renseignements personnels et les documents électroniques*. La commissaire adjointe a donc jugé que les motifs étaient suffisants pour déclencher une vérification des pratiques de gestion des renseignements personnels de Bureau en gros.

OBJET DE LA VÉRIFICATION

5. La vérification était axée sur la gestion par Bureau en gros des renseignements personnels de ses clients. L'objectif était d'évaluer si l'organisation avait pris des mesures adéquates pour protéger les renseignements personnels — notamment ceux enregistrés sur des dispositifs de stockage de données ayant été retournés — et si les politiques, processus et pratiques en matière de gestion des renseignements personnels étaient conformes aux dix principes relatifs à la protection de la vie privée prévus à l'annexe 1 de la LPRPDE. Les responsables de la vérification n'ont pas évalué les pratiques de gestion des renseignements personnels de Bureau en gros ni comparé celles-ci avec les normes et les pratiques pouvant être en vigueur chez d'autres détaillants.

6. La vérification ne comprenait aucun examen de la manière dont Bureau en gros gère les renseignements personnels de ses employés ou de fournisseurs de services tiers. En outre, même si nous avons évalué les mesures de protection en matière de TI, la vérification ne visait pas à examiner l'ensemble des infrastructures de sécurité de Bureau en gros dans ce domaine. La section « **Au sujet de la vérification** » du présent rapport donne plus de renseignements sur la portée, les critères et l'approche de la vérification.

Observations et recommandations

LEADERSHIP ET RESPONSABILITÉ EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

7. Les organisations assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* sont responsables des renseignements personnels en leur possession. Pour s'assurer que cette responsabilité est bien comprise, les organisations doivent établir des modalités claires en ce qui concerne la responsabilité liée à la protection de la vie privée et le respect des obligations aux termes de la LPRPDE. Par conséquent, nous nous attendions à ce que Bureau en gros :

   - ait nommé une ou des personnes chargées de veiller au respect de la LPRPDE;
   - ait mis en œuvre des politiques, des procédures et des pratiques tenant compte des dix principes de protection de la vie privée prévus à l'annexe 1 de la Loi.

8. Nous avons examiné les politiques et les procédures de Bureau en gros relatives à la protection de la vie privée, les documents donnant un aperçu des responsabilités à ce chapitre et les documents de formation de l'entreprise. Nous avons aussi examiné le protocole de gestion des atteintes à la protection des renseignements personnels de Bureau en gros. Nous avons relevé des pratiques positives, mais aussi des améliorations à apporter.

Les rôles et les responsabilités sont clairement établis et bien compris

9. Pour que les obligations découlant de la LPRPDE soient respectées, il faut que les responsabilités liées au respect de la Loi soient clairement établies et expliquées. Les employés doivent être informés des politiques, des processus et des pratiques de protection de la vie privée et bien comprendre leurs rôles et leurs responsabilités pour que ces mécanismes de conformité donnent les résultats escomptés.

10. Selon la politique sur le droit à la vie privée de Bureau en gros, tous les employés sont chargés de protéger les renseignements personnels, mais le responsable de la protection de la vie privée de Bureau en gros est chargé d'établir l'orientation stratégique générale et d'assurer le respect de la vie privée au niveau de la direction. Voici les tâches confiées au responsable de la protection de la vie privée :

    - veiller à ce que le personnel soit bien formé et comprenne ses obligations en matière de protection de la vie privée;
    - cerner et atténuer les risques liés à la protection de la vie privée;
    - surveiller la conformité à la LPRPDE.

11. La conformité aux exigences de la LPRPDE dépend en grande partie du degré de compréhension des dispositions de la Loi par les personnes qui traitent les renseignements personnels. La sensibilisation et la formation sont essentielles pour atteindre les objectifs de la Loi.

12. Bureau en gros a mentionné que la sensibilisation des employés à l'importance de la protection de la vie privée est au cœur de sa gestion dans ce domaine. Divers mécanismes sont utilisés pour sensibiliser les employés, le principal étant la formation obligatoire sur la protection de la vie privée et la gestion de l'information. Cette formation est donnée par voie électronique. Le siège social de Bureau en gros surveille les taux de réussite, qui sont communiqués chaque mois aux gérants des succursales. Nous avons examiné le module de formation et les documents de référence connexes. Ceux-ci mettent l'accent sur l'importance de protéger les renseignements personnels, donnent un aperçu des dix principes de protection de la vie privée et fournissent une orientation sur la collecte, l'utilisation, la communication et l'élimination de renseignements personnels.

13. Le programme obligatoire de sensibilisation à la protection de la vie privée est complété par des réunions avec l'ensemble du personnel, ce qui donne l'occasion aux représentants du siège social de Bureau en gros de parler des enjeux liés à la protection de la vie privée avec les employés. Par exemple, une campagne nationale a récemment été lancée pour faire en sorte que tous les employés connaissent les personnes-ressources au sein de l'entreprise au sujet de la protection de la vie privée.

14. En plus d'examiner les documents relatifs aux programmes, nous avons parlé avec des employés de divers secteurs de Bureau en gros. Tous les employés du service à la clientèle, les techniciens et les gérants étaient conscients de l'importance que revêt la protection des renseignements personnels, ainsi que de leurs rôles et de leurs responsabilités à cet égard.

Les politiques et les procédures relatives à la protection de la vie privée fournissent un cadre de travail pour protéger les renseignements personnels

15. Les organisations assujetties à la LPRPDE sont tenues de mettre en œuvre des politiques et des procédures tenant compte des dix principes de protection de la vie privée énumérés à l'annexe 1 de la Loi. Nous nous attendions à ce que des politiques et procédures suffisamment détaillées pour aider à la compréhension de la gestion par Bureau en gros des renseignements personnels qui lui sont confiés soient en place.

16. Nous avons étudié les politiques en matière de protection de la vie privée, de gestion de l'information et de conservation ainsi que les documents d'orientation connexes. Nous avons également examiné les procédures relatives aux retours, aux réparations et aux copies de sauvegarde chez Bureau en gros. L'ensemble de ces documents forme un cadre exhaustif de protection des renseignements personnels.

17. Bureau en gros a adopté les dix principes de protection de la vie privée énoncés à l'annexe 1 de la Loi comme politique de gestion des renseignements personnels. La politique sur le droit à la vie privée, qui se trouve sur le site Web de l'entreprise, y renvoie. La politique ne mentionne pas quels types de renseignements personnels sont recueillis par Bureau en gros, comment ils sont utilisés, à qui et dans quelles circonstances ils sont communiqués à des tiers ou comment ils sont protégés. La politique ne traite pas de l'acheminement ni du stockage de renseignements personnels à l'extérieur du Canada. Pourtant, la politique américaine de Bureau en gros sur la protection de la vie privée aborde en détail la question de la collecte, de l'utilisation et de la communication des renseignements personnels.

18. La politique de protection de la vie privée d'une organisation est un outil essentiel pour protéger les renseignements personnels des clients. Apporter des modifications aux politiques en matière de protection de la vie privée de Bureau en gros pourrait rendre plus transparentes les pratiques de gestion des renseignements personnels. Les clients auraient ainsi une certaine assurance que leurs attentes en matière de protection de la vie privée sont respectées (voir les paragraphes 35 à 38).

Un processus de gestion des atteintes à la protection des renseignements personnels est en place

19. Une atteinte à la protection des renseignements personnels survient lorsque des renseignements personnels sont consultés, utilisés ou communiqués sans autorisation. Elle peut se produire quand des renseignements personnels sont volés, perdus ou transmis par mégarde. Elle peut également découler d'une procédure déficiente de l'entreprise ou de lacunes opérationnelles.

20. Même si la LPRPDE n'impose pas d'obligations précises aux organisations en ce qui concerne les atteintes à la protection des renseignements personnels, la capacité de découvrir ces incidents et de réagir en conséquence est un élément crucial de la gestion de la protection de la vie privée. Pour aider les organisations à ce chapitre, le Commissariat a publié un document d'orientation énumérant quatre étapes à suivre en cas d'atteinte réelle ou présumée à la protection des renseignements personnels : (1) limitation de l'atteinte et évaluation préliminaire; (2) évaluation des risques associés à l'atteinte; (3) signalement aux personnes concernées; (4) prévention de récidives.

21. Bureau en gros a établi une procédure à suivre en cas d'atteinte à la protection des données appartenant à des entreprises ou à des clients. Ce processus est énoncé dans la politique de protection de la vie privée et les documents d'orientation internes. Quand des employés apprennent que la sécurité des systèmes ou des renseignements de Bureau en gros a été — ou pourrait avoir été — menacée, ils doivent le signaler immédiatement au centre de soutien des systèmes d'information. S'il est impossible de communiquer avec le centre, l'employé doit s'adresser au responsable de la protection de la vie privée de Bureau en gros. Tous les gérants et les employés interviewés connaissaient le processus de gestion des atteintes.

22. Le siège social de Bureau en gros coordonne tous les efforts visant à atténuer et à limiter les atteintes. Selon la nature de l'incident, le responsable de la protection de la vie privée, le directeur national des opérations ou le centre de soutien des systèmes d'information est chargé de gérer les atteintes et de fournir des instructions au personnel. L'évaluation des atteintes, y compris de la question de savoir s'il faut informer les personnes touchées, se fait au cas par cas. Il n'y a aucune politique officielle en cas d'atteinte à la protection des renseignements personnels, mais le responsable de la protection de la vie privée nous a informés que tous les incidents sont analysés dans le but de découvrir la source du problème et de s'y attaquer. Il n'est pas toujours nécessaire de s'attaquer à la racine du problème, par exemple si l'incident est peu susceptible de se reproduire ou s'il n'y a pas assez de renseignements pour cerner les causes du problème au moyen d'efforts raisonnables. Dans certains cas, le problème est résolu à l'étape de la limitation de l'atteinte. Quand l'enquête révèle que l'atteinte découle d'une lacune des politiques ou des procédures, une note est envoyée à toutes les succursales pour les informer des mesures prises pour remédier à la situation.

Les activités de surveillance de la conformité doivent être intensifiées

23. Les organisations ont la responsabilité de se conformer aux principes énoncés à l'annexe 1 de la Loi. Pour respecter leurs obligations en matière de conformité, elles doivent disposer d'un outil pour mesurer leur degré de conformité. Nous avons vérifié si Bureau en gros évalue régulièrement ses propres pratiques de traitement des renseignements personnels. Nous avons également examiné des documents de vérifications internes et interviewé des gérants de succursales.

24. Nous avons appris que chaque point de vente au détail fait l'objet d'une vérification au moins une fois par année civile. Le document de vérification utilisé pour évaluer le rendement des succursales est axé sur la prévention des vols, le traitement des transactions, la réception et l'expédition de marchandises et les activités générales. Les vérifications évaluent également le respect des procédures et des contrôles de sécurité établis qui sont conçus pour protéger les données des clients, par exemple :

    - les renseignements personnels et les ordinateurs des clients sont rangés dans des zones sécurisées;
    - les dispositifs de stockage de données retournés sont traités par les membres des services techniques avant d'être revendus;
    - les données des clients ne sont sauvegardées sur aucun appareil ou disque dur de la succursale.

25. La politique de retour de Bureau en gros stipule qu'un gérant doit vérifier si les dispositifs de stockage de données ont été nettoyés avant de les revendre. Nous avons découvert que cette pratique n'est pas toujours respectée : la plupart des gérants, lorsqu'ils acceptent qu'un article soit revendu, tiennent pour acquis que le processus de nettoyage et de restauration a été efficace. Quatorze des dix-sept succursales examinées ont confirmé qu'il n'y a pas d'inspections aléatoires et que les dispositifs revendus ne sont pas testés dans le cadre du processus de vérification interne.

26. Pour protéger la vie privée, il faut aussi recueillir seulement les renseignements personnels nécessaires à des fins légitimes, faire en sorte que les renseignements ne soient pas utilisés ou communiqués à d'autres fins que celles auxquelles ils ont été recueillis (sauf si le client a donné son consentement ou si la loi l'exige) et détruire les renseignements qui ne sont plus requis. Bureau en gros n'était pas en mesure de produire des documents montrant que la collecte, la conservation et l'élimination de renseignements personnels faisaient l'objet d'examens officiels. En outre, bien qu'un processus de gestion des atteintes à la protection des renseignements personnels soit établi, aucun mécanisme de surveillance ne permet de s'assurer que les mesures correctives permettent de faire face à tous les aspects de l'atteinte.

27. Une stratégie de surveillance permanente comprenant des vérifications internes constituerait un moyen d'atténuer les risques pour la vie privée et garantirait que les principes énoncés à l'annexe 1 de la Loi sont respectés dans le cadre des activités quotidiennes de Bureau en gros.

28. RECOMMANDATION

- Bureau en gros devrait prévoir des examens de la conformité en matière de protection de la vie privée dans son programme de vérification interne.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a modifié sa liste de vérification visant à empêcher les pertes afin d'aborder plus en détail le stockage, la collecte, la conservation et l'élimination des renseignements personnels et d'autres aspects relatifs à la protection de la vie privée.

L'entreprise a mis sur pied un programme prévoyant l'inspection hebdomadaire des salles de technologie pour garantir le respect de la vie privée. En outre,

elle offre des formations dans toutes ses succursales sur la protection de la vie privée dans les salles de technologie afin de renforcer les pratiques exemplaires de protection de la vie privée en ce qui a trait aux produits retournés par les clients ou à réparer. L'entreprise a créé une formation sur le code d'éthique et sur la gestion des renseignements personnels qui est obligatoire pour tous les associés, ce qui permet de mettre l'accent sur les priorités en matière de protection de la vie privée.

L'entreprise a centralisé ses services de récupération de données pour éviter que les succursales conservent des renseignements sur les clients dans la zone des services techniques. Elle a poursuivi le développement et la diffusion d'une application automatique qui repère les fichiers (pouvant appartenir aux clients) enregistrés par erreur sur les ordinateurs de la salle de technologie. Tous les fichiers repérés par cette application sont supprimés, conformément à la politique de l'entreprise de ne jamais conserver des données appartenant aux clients dans ses magasins.

L'entreprise continuera d'établir de nouveaux examens de conformité pour soutenir ses politiques en matière de protection de la vie privée. Une équipe de gouvernance interfonctionnelle a été créée pour veiller au respect de la vie privée.

GESTION DU CYCLE DE VIE DES RENSEIGNEMENTS PERSONNELS

29. La Loi prévoit les règles de gestion des renseignements personnels détenus par une organisation. Elle établit un équilibre entre la nécessité pour les entreprises de recueillir, d'utiliser et de communiquer des renseignements personnels à des fins légitimes et le droit des personnes à la vie privée. En résumé, la LPRPDE impose aux organisations les obligations suivantes :

    - déterminer clairement les fins de la collecte avant la collecte ou au moment de celle-ci;
    - obtenir le consentement avant de recueillir, d'utiliser ou de communiquer des renseignements personnels;
    - recueillir seulement les renseignements nécessaires pour atteindre les objectifs fixés;
    - utiliser et communiquer les renseignements personnels uniquement aux fins auxquelles ils ont été recueillis;
    - conserver les renseignements personnels uniquement pendant la période pour laquelle ils sont nécessaires.

30. Nous avons examiné comment Bureau en gros gère les renseignements personnels pour évaluer dans quelle mesure l'entreprise se conforme aux obligations susmentionnées. Nous avons étudié les politiques et les procédures, mais aussi les processus de gestion des renseignements personnels dans les divers secteurs d'affaires de Bureau en gros, de la collecte jusqu'à l'élimination.

Les clients ne sont pas toujours informés de l'objectif de la collecte

31. Bureau en gros recueille des renseignements personnels sur ses clients aux points de vente et dans le contexte des processus de photocopie, d'impression et de réparation. Les données recueillies ne comprennent généralement que le nom, l'adresse, le numéro de téléphone et l'information sur les paiements (c.-à d. le numéro de carte de crédit ou de débit). Lorsqu'un dispositif pouvant contenir des données est retourné pour une réparation ou un remboursement, le mot de passe du client est recueilli pour faciliter l'accès au dispositif. De plus, Bureau en gros recueille des renseignements personnels de personnes qui demandent une carte de crédit Bureau en gros, tels que le nom, l'adresse, la date de naissance, le numéro d'assurance sociale (facultatif), l'emploi et les renseignements financiers.

32. La LPRPDE exige que les personnes soient au courant de la collecte, de l'utilisation et de la communication de leurs renseignements personnels et qu'elles fournissent leur consentement. Pour que celui-ci soit valable, la Loi exige que les objectifs de la collecte, de l'utilisation et de la communication soient énoncés clairement.

33. La politique sur le droit à la vie privée de Bureau en gros stipule que l'entreprise recueillera et utilisera des renseignements personnels sur ses clients uniquement pour pouvoir les identifier et communiquer avec eux, pour protéger la compagnie et ses clients contre les erreurs et la fraude et pour fournir à ces derniers des renseignements sur les produits et les services. Elle mentionne également que les renseignements personnels sur les clients ne seront utilisés à aucune autre fin et ne seront jamais communiqués à un tiers sans le consentement du client.

34. Les objectifs de la collecte sont mentionnés dans la politique, mais ils ne sont pas indiqués sur tous les formulaires servant à recueillir les données sur les clients. On peut raisonnablement croire que ces derniers comprennent pourquoi les coordonnées sont recueillies (c.-à-d. le nom, l'adresse et le numéro de téléphone) pour livrer des produits commandés ou en réparation, mais ils ignorent peut-être que les renseignements recueillis pour accorder un remboursement peuvent aussi servir à détecter les fraudes. Pour que les clients soient parfaitement informés, il faudrait que tous les documents employés pour recueillir des renseignements personnels indiquent clairement l'objectif de la collecte et la façon dont les renseignements seront utilisés.

Il y a un manque de transparence concernant la circulation transfrontalière des données

35. La circulation transfrontalière des données est chose courante dans l'économie mondialisée actuelle. Étant donné que de nombreuses organisations mènent des activités à l'échelle internationale, les renseignements personnels peuvent être recueillis sur un territoire et transférés dans un autre pour être traités et stockés. Ces transferts de données se produisent pour diverses raisons, notamment la disponibilité des fournisseurs de services, l'amélioration des services à la clientèle et l'efficience des opérations. La LPRPDE n'interdit pas la circulation transfrontalière à des fins commerciales légitimes, mais elle exige que les organisations fassent preuve de transparence à ce chapitre.

36. Nous avons examiné les processus opérationnels, les formulaires, la politique sur le droit à la vie privée et les avis affichés sur le site Web de Bureau en gros concernant les achats en ligne. Notre enquête a révélé que les commandes reçues par les centres d'appel de Bureau en gros et les documents saisis par le service de copie et d'impression en ligne sont acheminés et stockés aux États-Unis. Ces documents contiennent parfois des renseignements personnels, mais nous n'avons rien trouvé qui démontre que les clients sont au courant de ces transferts de données et Bureau en gros n'a fourni aucune preuve à cet égard.

37. Les principes de protection de la vie privée prévus à l'annexe 1 de la Loi visent à permettre aux personnes de contrôler la façon dont leurs renseignements personnels sont traités. Les gens ont le droit de savoir que leurs données personnelles seront possiblement traitées ou stockées dans un autre pays et que les autorités sur ce territoire y auront accès. Certaines personnes seraient prêtes à accepter un certain risque pour obtenir un produit ou un service particulier, mais elles devraient avoir suffisamment de renseignements à leur disposition pour prendre une décision éclairée.

38. S'il y a lieu, Bureau en gros a le devoir d'informer ses clients que leurs renseignements personnels pourraient être consultés par les organismes chargés de l'application de la loi et de la sécurité nationale d'un territoire étranger. Un tel avis devrait être clair et compréhensible et donné au moment où les renseignements personnels sont recueillis.

La collecte ne se limite pas aux renseignements nécessaires aux fins de l'évaluation du risque de crédit

39. La gestion du cycle de vie des renseignements personnels commence par la collecte. Les organisations assujetties à la LPRPDE doivent seulement recueillir les données sur les clients qui sont nécessaires à l'atteinte d'objectifs commerciaux légitimes.

40. Comme il est indiqué au paragraphe 31, Bureau en gros recueille des renseignements personnels sur ses clients dans le cadre des ventes, des retours, des réparations, des services de photocopie et des demandes de crédit. Nous nous attendions à ce que la collecte soit utile et non excessive.

41. Nous avons constaté que les pratiques de Bureau en gros respectent le principe de la limitation de la collecte, à une exception près. Certaines succursales photocopiaient des documents d'identité délivrés par le gouvernement dans le cadre du programme de crédit instantané (en magasin), même si la politique de l'entreprise interdit une telle collecte. Ces documents, qui comprennent des permis de conduire, des cartes d'assurance maladie et des passeports, étaient joints aux formulaires de demande de crédit.

42. Les documents d'identité délivrés par le gouvernement contiennent beaucoup de renseignements personnels. En plus du nom, ils peuvent fournir l'adresse du détenteur, sa nationalité, sa date de naissance, une photographie et une description de l'apparence physique (p. ex. la couleur des yeux et la taille).

43. Les émetteurs de cartes de crédit ont légitimement besoin de recueillir des renseignements personnels pour identifier et évaluer le demandeur. Il est nécessaire de connaître le passif financier ainsi que la source et l'importance des revenus pour évaluer le risque de crédit, mais pas la description physique du demandeur.

44. De plus, il faut faire la distinction entre examiner un document, consigner les renseignements qui s'y trouvent et conserver une photocopie du document entier. Même s'il est nécessaire d'enregistrer certains renseignements aux fins d'identification, la photocopie des documents constitue une collecte excessive de renseignements personnels.

45. Une autre pratique liée aux demandes de crédit instantané mérite qu'on s'y attarde. Quand une demande est remplie, l'information est fournie à l'émetteur de carte de crédit aux fins d'évaluation. Dans près des trois quarts des succursales visitées, ces renseignements étaient transmis par téléphone dans la zone des ventes. Cette pratique fait en sorte que les renseignements personnels du demandeur risquent d'être révélés aux personnes à proximité. Les employés des ventes et du service à la clientèle de Bureau en gros devraient être éclairés à ce sujet.

46. Par ailleurs, de nombreuses succursales conservaient indéfiniment des demandes de crédit faites en magasin, qu'elles aient été approuvées ou non. Cette pratique a cessé au cours de la vérification.

Le consentement explicite est obtenu aux fins de marketing

47. Les organisations assujetties à la LPRPDE peuvent seulement utiliser et communiquer les renseignements personnels aux fins auxquelles ils ont été recueillis, sauf si la personne a accordé son consentement ou si la loi l'exige. L'organisation peut demander le consentement en offrant une option d'adhésion (consentement explicite) ou de retrait (consentement implicite).

48. Si le formulaire offre une option d'adhésion, souvent appelée « consentement explicite », il faut que la personne autorise l'organisation à utiliser ses renseignements personnels à des fins secondaires, c'est-à-dire qui diffèrent des fins auxquelles les renseignements ont été recueillis au départ. Si le client ne donne pas son adhésion (qu'il n'a pas dit « oui »), l'organisation ne présume pas qu'il accorde son consentement. Inversement, selon l'option de retrait, la personne doit refuser explicitement les fins secondaires, faute de quoi (si la personne ne dit pas « non »), l'organisation présume que le consentement est accordé et utilise ou communique les renseignements personnels aux fins proposées.

49. Nous avons examiné les processus opérationnels de Bureau en gros et les formulaires utilisés pour recueillir les renseignements personnels. Nous avons constaté que les données personnelles des clients ne sont recueillies que pour offrir les services. La politique d'entreprise adoptée par Bureau en gros prévoit que le client doit donner son adhésion (le consentement explicite) à l'utilisation secondaire de ses renseignements personnels aux fins de marketing. Les formulaires, tant sur papier qu'en format électronique, contiennent une case que les clients doivent cocher s'ils désirent recevoir des produits de marketing (p. ex. des offres spéciales, des annonces de nouveaux produits, des dépliants électroniques, des catalogues, etc.). Si la personne n'a pas coché la case, Bureau en gros considère qu'elle n'a pas accordé son consentement aux fins secondaires. L'organisation a également mis en place un mécanisme permanent permettant de retirer son consentement en tout temps.

Les documents joints aux commandes d'impression et de photocopie sont conservés plus longtemps que nécessaire

50. La Loi précise qu'une organisation ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées. Nous nous attendions à ce que Bureau en gros ait mis des mécanismes en place pour satisfaire à cette obligation. Nous avons examiné la politique et le calendrier de conservation ainsi que les procédures connexes.

51. Nous avons vu des documents qui n'étaient pas couverts par le calendrier de conservation et d'élimination, d'autres qui étaient conservés au-delà de la date d'élimination prévue et d'autres encore dont la période de conservation était excessive (ils étaient conservés indéfiniment). Au cours de la vérification, Bureau en gros a révisé son calendrier de conservation et

d'élimination, ajouté au calendrier des documents oubliés et raccourci la période de conservation de certains documents. Malgré ces efforts, la période de conservation d'une catégorie de documents est encore trop longue.

52. Le centre de copie et d'impression de Bureau en gros offre un service en ligne. Une demande — avec le document à imprimer en pièce jointe — est envoyée électroniquement à l'aide d'un service de présentation des documents en ligne qui relie directement l'ordinateur du client au réseau du centre d'impression. Un courriel automatique est généré lorsque la commande est prête. Les documents joints aux commandes d'impression ou de photocopie envoyées en ligne sont conservés dans une base de données de Bureau en gros pendant un an.

53. Nous avons été informés que les documents sont conservés pour faciliter le traitement des demandes subséquentes portant sur les mêmes documents. Cette pratique aide peut-être à répondre aux besoins des entreprises (qui commandent régulièrement des formulaires, des enveloppes et du papier à en-tête), mais conserver des renseignements personnels — y compris des curriculum vitæ et des documents juridiques comme des ententes de divorce ou de garde — sous prétexte qu'ils pourraient servir un jour contrevient au principe de la limitation de la conservation.

54. Sous le régime de la LPRPDE, Bureau en gros est tenue d'éliminer les renseignements personnels dont elle n'a plus besoin aux fins pour lesquelles ils ont été recueillis. Lorsqu'une demande d'impression ou de photocopie a été traitée et que le client est satisfait de la qualité, l'objectif de la cueillette a été atteint. Par la suite, le document devrait seulement être conservé si le client accorde son consentement explicite à cette fin.

Il n'y a aucun suivi pour vérifier si les données enregistrées sur des machines de bureau louées ont été supprimées

55. Les points de vente au détail de Bureau en gros louent des photocopieuses pour leurs services de copie et d'impression. Certaines de ces machines comportent des disques durs intégrés qui conservent des images des documents photocopiés. À la fin du bail ou lorsqu'il faut remplacer les machines parce qu'elles ne peuvent être réparées, les photocopieuses sont renvoyées au fournisseur. Nous avons vérifié si des mécanismes de contrôle avient été mis en place pour garantir que les disques durs de ces machines étaient nettoyés ou détruits.

56. Nous avons examiné les documents liés aux ententes de location et interviewé les employés des centres de copie et d'impression de Bureau en gros. Selon les documents, le fournisseur est chargé de protéger l'intégrité des données enregistrées sur le matériel, ce qui a été confirmé par le personnel. Il doit notamment veiller à ce que les disques durs soient nettoyés avant d'être éliminés, recyclés ou réutilisés. Bureau en gros a affirmé qu'elle se fie au fournisseur à cet égard; elle n'effectue aucun suivi indépendant pour s'assurer que les données des clients ont bel et bien été effacées.

57. Pour surveiller le respect des ententes de location, il est nécessaire de mettre en place un mécanisme permettant de faire le suivi du processus de nettoyage ou de destruction des données. Selon les ententes actuelles, les fournisseurs ne sont pas tenus de remettre une déclaration signée à Bureau en gros indiquant la date à laquelle le disque dur a été nettoyé ou détruit. En exigeant un certificat de destruction, Bureau en gros ferait preuve de la diligence requise pour protéger les renseignements personnels de ses clients.

58. RECOMMANDATIONS

Conformément au code de pratiques équitables en matière de renseignements énoncé à l'annexe 1 de la LPRPDE, Bureau en gros :

- devrait informer ses clients de toutes les utilisations et communications que l'on peut faire de leurs renseignements personnels, dont le transfert dans des pays étrangers;

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise modifiera sa politique sur le droit à la vie privée en conséquence d'ici le 15 mai 2011.

- ne devrait pas conserver de photocopies de documents d'identité délivrés par le gouvernement dans le cadre de son programme de crédit interne;

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

La politique actuelle de l'entreprise interdit en toutes circonstances de reproduire et de conserver des documents d'identité délivrés par le gouvernement. L'entreprise l'a répété à ses succursales et continuera d'appliquer cette politique.

- devrait veiller à ce que les demandes de crédit interne soient traitées dans une zone privée;

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a envoyé une directive à toutes ses succursales pour rappeler à ses associés l'obligation de respecter la vie privée à toutes les étapes du processus de demande de crédit et continuera d'appliquer cette politique.

- devrait limiter la période de conservation des renseignements personnels associés aux commandes d'impression et de copie en ligne au temps nécessaire pour permettre au client de vérifier la qualité d'impression et de régler les problèmes s'il y a lieu;

Réponse de Bureau en gros :

L'entreprise convient que les clients devraient être informés du fait que leurs demandes en ligne seront conservées pendant un an.

L'entreprise croit que la conservation des demandes en ligne des clients pour une durée d'un an est utile aux clients et aux entreprises, car l'information est stockée de façon sécuritaire par un tiers et régie par des ententes et des restrictions appropriées. La seule personne pouvant entraîner la réutilisation ou la communication de l'information est le client lui-même. Toutefois, l'entreprise avisera dûment les clients de cette pratique, ce qui permettra à ces derniers de choisir les services de photocopie au comptoir s'ils le désirent.

- devrait veiller à ce que les ententes de location conclues avec des fournisseurs de matériel prévoient que ceux-ci remettront un certificat attestant la date à laquelle le disque dur a été nettoyé ou détruit.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise demandera des certificats de destruction à ses fournisseurs de matériel de photocopie. Cette demande a été communiquée aux fournisseurs actuels et sera ajoutée à toutes les prochaines ententes, nouvelles ou renouvelées, conclues avec les fournisseurs.

PROTÉGER LES DONNÉES PERSONNELLES DES CLIENTS

59. Les organisations assujetties à la LPRPDE sont tenues de protéger les renseignements personnels au moyen de mesures de sécurité correspondant au degré de sensibilité des renseignements détenus. Des mesures et des contrôles appropriés sont nécessaires pour éviter la consultation, l'utilisation, la communication, la modification ou la destruction non autorisées de renseignements personnels.

60. Nous nous attendions à ce que les mécanismes physiques, techniques et organisationnels de Bureau en gros suffisent à protéger l'intégrité et la confidentialité des renseignements personnels des clients. Nous avons examiné les politiques, les procédures, les processus, les ententes avec les tiers et les contrôles d'accès au système de TI. Nous avons aussi inspecté physiquement des succursales choisies.

Des renseignements personnels ont été décelés sur des dispositifs de stockage de données destinés à la revente

61. Comme il a été mentionné, le Commissariat a mené, à deux reprises, une enquête sur Bureau en gros à la suite d'allégations selon lesquelles l'entreprise n'avait pas protégé les renseignements personnels qu'elle avait sous son contrôle. Dans les deux cas, un dispositif de stockage de données ayant été retourné contenait des renseignements personnels au sujet du client. Bureau en gros a revendu les dispositifs sans supprimer ces données. Le Commissariat a découvert que l'entreprise n'avait pas protégé adéquatement les renseignements personnels du plaignant et que ces atteintes à la vie privée étaient dues à l'inefficacité des procédures et des mécanismes de contrôle pour la gestion des dispositifs de stockage de données. En réponse à la dernière plainte, Bureau en gros a accepté de mettre en place une procédure de nettoyage et de restauration, à laquelle allaient être soumis tous les dispositifs de stockage de données. Par conséquent, nous nous attendions à ce que l'entreprise ait instauré un processus efficace pour atténuer les risques d'atteintes à la sécurité des renseignements personnels.

62. En novembre 2009, Bureau en gros a révisé ses procédures de gestion des dispositifs de stockage de données ayant été retournés. Selon les nouvelles procédures, un dispositif retourné est étiqueté et rangé dans un classeur en attendant une évaluation diagnostique, qui permet de déterminer si le dispositif peut être revendu ou s'il doit être retourné au fournisseur. Qu'il soit destiné à la revente ou à un retour au fournisseur, le dispositif subit le même traitement. Un technicien suit la procédure de nettoyage et de restauration et confirme par écrit que le travail a été parachevé. Le dispositif est ensuite envoyé à un gérant pour qu'il donne son approbation. La signature du gérant atteste que le dispositif a été traité en conformité avec les procédures établies. Une étiquette confirmant que la procédure a été suivie est ensuite apposée sur le dispositif, qui est remis en vente ou classé parmi les dispositifs à retourner au fournisseur.

63. Les procédures révisées comprennent un mécanisme de contrôle essentiel, mais elles ne sont pas toujours appliquées. Dans 15 des 17 succursales inspectées, nous avons observé des cas où des dispositifs de stockage de données :

- étaient remballés et faisaient l'objet d'une attestation confirmant qu'ils avaient été nettoyés, alors que ce n'était pas le cas;
- n'étaient pas vérifiés par un gérant avant d'être remis en vente;
- étaient placés directement parmi les dispositifs à renvoyer au fournisseur, sans avoir été traités (nettoyés) par un technicien.

64. Nous avons effectué une vérification à chacune des succursales inspectées. À cette fin, 149 dispositifs de stockage de données qui avaient été emballés pour la revente et subi le processus de nettoyage et de restauration de Bureau en gros ont été choisis. L'échantillon comprenait des ordinateurs de bureau, des ordinateurs portatifs,

des disques durs externes et internes, des clés USB et des cartes mémoire.

65. Chaque dispositif était branché à un ordinateur portatif et examiné à l'aide de l'explorateur Windows[MC]. Sur certains d'entre eux, des dossiers comprenant des renseignements personnels étaient facilement accessibles. Les autres dispositifs semblaient avoir été nettoyés et ne contenaient donc pas de données de clients (c'est-à-dire des données stockées dans le dispositif, intentionnellement ou non, par le client ou pour celui-ci). Ceux qui semblaient avoir été nettoyés ont ensuite été examinés à l'aide d'un logiciel facile à obtenir (gratuiciel) téléchargé sur Internet, pour voir s'ils contenaient des données cachées.

Le processus de nettoyage écrase le contenu de l'espace où se trouvaient des données. Si un dispositif n'est pas nettoyé, les données « supprimées » peuvent être récupérées à l'aide d'outils facilement accessibles qui les restaurent dans un format lisible.

66. En général, quand les données sont « supprimées » d'un dispositif de stockage de données, elles ne sont pas vraiment effacées. L'endroit où se trouvent les données devient tout simplement un espace libre. Autrement dit, c'est l'information dont le disque dur a besoin pour trouver les données qui est supprimée et non pas les données elles-mêmes. Pour que les données soient effacées de façon sécuritaire, le dispositif doit être nettoyé. Des outils et des logiciels de sécurité sont offerts — ou peuvent être développés — à cette fin. Nous avons testé chaque dispositif de l'échantillon de vérification pour déterminer si le nettoyage était effectué. Les résultats se trouvent dans le tableau suivant.

67. Nous avons constaté que 54 des 149 dispositifs testés contenaient des données. Un certain nombre d'entre eux contenaient des renseignements personnels, y compris des numéros d'identité délivrés par le gouvernement, des courriels, des lettres et des photographies personnelles, des documents d'immigration, des curriculum vitæ, des états financiers, des ententes de garde et des listes de contacts.

68. Nous avons aussi examiné des appareils photo numériques, des systèmes de positionnement global (GPS), des lecteurs médias portables et des assistants numériques personnels. Les appareils photo et les lecteurs médias ne contenaient pas de données résiduelles, mais deux des huit GPS n'avaient pas été remis dans leur état initial, ce qui révélait les déplacements et les adresses des anciens propriétaires.

69. La vérification démontre que Bureau en gros ne s'assure pas que les dispositifs de stockage de données sont parfaitement nettoyés avant de les

Dispositif	Dispositifs vérifiés	Entièrement nettoyés	Partiellement nettoyés
Ordinateurs (de bureau et portatifs)	20	3	17
Disques durs externes	55	36	19
Disques durs internes	10	9	1
Clés USB	20	12	8
Cartes mémoire	44	35	9
Total	149	95	54

revendre. Deux facteurs contribuent à ce problème : comme nous l'avons mentionné au paragraphe 63, les procédures à suivre en ce qui a trait au traitement des dispositifs retournés ne sont pas toujours suivies; de plus, la procédure varie selon le fabricant du dispositif et, dans certains cas, elle ne permet pas d'effacer toutes les données. En résumé, nos essais démontrent que les procédures révisées n'ont pas comblé les lacunes qui étaient présentes en 2008. La vie privée des clients de Bureau en gros demeurera menacée jusqu'à ce que ce problème soit réglé.

70. RECOMMANDATION

- Bureau en gros devrait examiner ses procédures et processus de nettoyage des dispositifs de stockage et mettre en place des mécanismes de contrôle améliorés pour éliminer les risques que des renseignements personnels soient communiqués.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

À la suite d'une plainte déposée en 2008, l'entreprise a instauré une politique de nettoyage et de restauration, avant la revente, de tout dispositif de stockage d'information ayant été retourné. Pour nettoyer et restaurer les ordinateurs de bureau et les ordinateurs portatifs, l'entreprise suit les procédures et utilise les outils fournis par les fabricants. Ces procédures ne préservent que le logiciel d'origine expédié par l'usine. Contrairement aux avertissements du fabricant selon lesquels ce processus effacera tous les fichiers, les données peuvent être récupérées à l'aide d'un logiciel judiciaire. Aucun fabricant ne conseille d'écraser les données dans le cadre du processus de nettoyage et de restauration recommandé. Le processus d'écrasement peut endommager le disque dur de l'ordinateur et détruire le logiciel original expédié par l'usine (y compris les outils de nettoyage et de restauration), ce qui fait que l'utilisation généralisée de ce processus n'est pas commercialement rentable.

À l'aide d'un logiciel judiciaire, l'équipe de vérification du Commissariat à la protection de la vie privée a été en mesure de récupérer les données de certains ordinateurs qui avaient subi le processus de nettoyage et de restauration recommandé par le fabricant. Elle a recommandé un processus de nettoyage et de restauration qui « écrase » toutes les données des clients et fait en sorte que les données soient impossibles à récupérer.

L'entreprise est en train de tester des moyens de nettoyer les données sur un produit retourné (pour que les données ne puissent être récupérées à l'aide d'un logiciel judiciaire) sans endommager ou détruire les disques durs, les systèmes d'exploitation utiles et d'autres outils fournis par le fabricant.

Renseignements personnels trouvés sur des dispositifs emballés pour la revente :

- noms, adresses, numéros d'assurance sociale, cartes d'assurance maladie provinciales et numéros de passeport
- antécédents professionnels, diplômes et relevés de notes
- investissements personnels, renseignements bancaires, relevés de carte de crédit et dossiers d'impôt
- permis de conduire, cartes de résident permanent et visas d'étudiant

Les documents contenant des renseignements personnels sur les clients ne sont pas toujours rangés dans un endroit sécurisé

71. Les points de vente au détail et les actifs de Bureau en gros sont contrôlés au moyen de diverses techniques, y compris des caméras de sécurité, des systèmes d'alarme, des dispositifs antivol, des classeurs verrouillés et d'autres techniques pour restreindre l'accès dans certaines zones.

72. Les données des clients sont généralement conservées au centre technique, dans les bureaux de la direction et dans les aires d'expédition et de réception. À l'exception de ces aires, l'accès est

contrôlé au moyen de portes verrouillées, de clés ou de terminaux de contrôle d'accès.

73. Selon la politique de Bureau en gros, tous les renseignements personnels doivent être rangés dans un endroit sécurisé, c'est-à-dire des classeurs ou des pièces verrouillés, lorsqu'ils ne servent pas. Cependant, 12 des 17 magasins que nous avons visités ne respectaient pas cette politique : nous y avons trouvé des formulaires de livraison, de transfert et de commande spéciale dans des classeurs non verrouillés.

74. Dans environ le tiers des succursales visitées, les formulaires de retour et de réparation n'étaient pas suffisamment protégés. De plus, les dispositifs de stockage de données retournés étaient conservés dans des classeurs non verrouillés ou sur des étagères ouvertes, ou laissés sans surveillance aux comptoirs de service. Ces articles sont particulièrement vulnérables puisqu'ils ne sont équipés d'aucune protection antivol. Ils risquent d'être subtilisés lorsqu'ils sont laissés sans surveillance dans un endroit non sécurisé.

Des données sur les clients sont jetées dans des poubelles ou des bacs de recyclage

75. Les organisations sont tenues d'éliminer les renseignements personnels de façon sécuritaire. Nous avons examiné les procédures de gestion des documents qui ne sont plus utiles chez Bureau en gros. Les données des clients sont généralement détruites dans les succursales de l'entreprise, qui ont recours aux services d'une entreprise spécialisée dans la destruction de documents. Les succursales sont équipées de déchiqueteuses verrouillées à cette fin. Il arrive cependant que des formulaires de commande contenant des renseignements personnels soient jetés dans des poubelles ou des bacs de recyclage plutôt que dans une déchiqueteuse.

76. Des atteintes à la protection des renseignements personnels en raison de mauvaises pratiques de destruction des documents se sont aussi produites dans d'autres organisations. Les organisations sont tenues de protéger les renseignements personnels tout au long de leur cycle de vie — depuis la collecte jusqu'à l'élimination au moyen d'une méthode sûre. Le problème ne semble pas être systémique, mais des faits démontrent que certains employés ne sont pas conscients de l'importance de traiter les renseignements personnels avec soin.

Des noms d'utilisateur et des mots de passe communs menacent la sécurité des données des clients

77. Le contrôle de l'accès au système de TI et aux données qui y sont enregistrées constitue un élément essentiel de la protection de la vie privée. Ne donner l'accès qu'à ceux qui en ont légitimement besoin atténue les risques que peut encourir l'intégrité des renseignements personnels, c'est-à-dire que les renseignements soient utilisés, communiqués, modifiés ou supprimés de façon inappropriée. Nous nous attendions à ce que les droits d'accès au système respectent le principe du besoin de savoir et soient contrôlés par un processus d'authentification de l'utilisateur (un nom d'utilisateur et un mot de passe).

78. Bureau en gros nous a informés que les droits d'accès sont accordés aux employés en fonction de leur rôle et de leurs responsabilités. Le profil du gérant est différent de celui d'un technicien en entretien et en réparation. De la même façon, les employés des ventes ont accès aux commandes d'achat et de livraison, mais ils ne peuvent accéder aux commandes de réparation ou aux documents générés par les centres de copie et d'impression.

79. Les profils d'accès au système jouent un rôle crucial dans la gestion de la sécurité de la TI, mais ils doivent être complétés par un processus d'authentification des utilisateurs rigoureux pour être efficaces. Des comptes d'utilisateur communs ont été créés dans divers services, les employés partageant le même nom d'utilisateur et le même mot de passe. Dans la majorité des succursales visitées, il y avait au moins un poste informatique où la légitimation d'authentification

(le nom d'utilisateur et le mot de passe) était collée sur l'écran ou à la vue des clients. En outre, nous avons vu des postes dans la zone des ventes qui étaient laissés ouverts et sans surveillance (avec une session ouverte).

80. Les activités liées à l'ouverture de session des utilisateurs doivent être enregistrées pour déterminer si les droits d'accès sont exercés correctement. Bureau en gros se prive de cette capacité en attribuant des noms d'utilisateur et des mots de passe communs. Ne disposant d'aucun moyen de surveiller l'accès au système, Bureau en gros ne peut affirmer, avec un degré de certitude raisonnable, que les données des clients sont toujours utilisées et communiquées à des fins légitimes.

81. RECOMMANDATIONS

Pour protéger les renseignements sur les clients, Bureau en gros devrait :

- s'assurer que les renseignements personnels sont conservés dans des classeurs verrouillés ou des zones sécurisées, comme le prévoit la politique de l'entreprise;

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a réitéré sa position et continuera d'appliquer ses politiques relatives au stockage des renseignements personnels. Elle a ajouté cette question à ses procédures de vérification interne.

- veiller à ce que les employés connaissent l'importance d'employer des méthodes sûres pour détruire les renseignements des clients;

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a réitéré sa position et continuera d'appliquer ses politiques relatives à la destruction des renseignements des clients. Elle a ajouté cette question à ses procédures de vérification interne.

- faire en sorte que les employés aient des codes d'accès uniques pour favoriser la responsabilisation des utilisateurs et atténuer le risque d'accès non autorisé aux données des clients.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise continue de chercher des solutions pratiques pour sécuriser l'accès et il est prévu qu'une application en cours de développement permette un accès personnalisé et sécurisé.

Soulignons que la politique actuelle de l'entreprise interdit de stocker des renseignements permettant d'identifier une personne sur un réseau partagé, sauf pour les systèmes devant être utilisés à des fins opérationnelles. De plus, des politiques de contrôle d'accès relatives au serveur du point de vente situé dans les bureaux d'accueil des magasins sont en place et font l'objet d'une vérification. Les systèmes de l'entreprise permettent la fermeture de session automatique et l'alternance de mots de passe génériques.

Conclusion

82. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE ou la Loi) impose des obligations aux entreprises privées en matière de gestion des renseignements personnels. Elle établit un équilibre entre le droit à la vie privée des personnes et la nécessité pour les entreprises de recueillir, d'utiliser et de communiquer des renseignements personnels à des fins légitimes.

83. Dans le cadre de ses activités, Bureau en gros traite une grande quantité de renseignements personnels. Bien que les coordonnées des clients — noms, adresses, numéros de téléphone et données liées au paiement — soient au cœur de ses activités de collecte, l'entreprise traite également des renseignements personnels qui vont au-delà de ses besoins opérationnels courants. Les demandes de copie et d'impression en ligne peuvent comprendre des curriculum vitæ ou des documents juridiques comme des ententes de divorce et de garde. Un ordinateur retourné ou en réparation peut renfermer des renseignements sur le niveau de scolarité, l'état de santé ou la situation financière du propriétaire.

84. En vertu de la LPRPDE, les organisations sont tenues de gérer les renseignements personnels en fonction des dix principes prévus à l'annexe 1 et elles sont responsables des renseignements personnels en leur possession. À cet effet, Bureau en gros a instauré des politiques et des procédures pour gérer les renseignements qu'elle possède. Les rôles et les responsabilités sont clairement définis et bien compris dans l'ensemble de l'organisation. Divers mécanismes, dont une formation obligatoire, sensibilisent les employés à l'importance de la protection de la vie privée. Bureau en gros pourrait cependant tirer avantage d'une stratégie de surveillance permanente pour veiller à ce que ces pratiques soient respectées dans l'ensemble de l'entreprise.

85. Les pratiques de collecte, d'utilisation, de conservation et d'élimination de Bureau en gros sont généralement conformes aux exigences de la LPRPDE. À quelques exceptions près, Bureau en gros recueille et utilise seulement les renseignements personnels nécessaires à des fins commerciales et elle obtient le consentement explicite d'une personne avant d'utiliser les

renseignements à des fins secondaires de marketing. Toutefois, Bureau en gros manque de transparence relativement à l'acheminement de renseignements personnels dans un pays étranger aux fins de traitement. La LPRPDE n'interdit pas la circulation transfrontalière des données, mais elle exige que les organisations soient transparentes à ce chapitre.

86. Des processus et des procédures inefficaces liés aux dispositifs de stockage de données ont fait en sorte que le Commissariat a reçu deux plaintes contre Bureau en gros. Ces plaintes portaient sur des atteintes à la protection des données : des renseignements personnels enregistrés sur des dispositifs de stockage de données n'avaient pas été effacés correctement avant la revente, ce qui a entraîné la communication inappropriée de renseignements personnels à d'autres clients. Bureau en gros s'est engagée à prendre des mesures correctives, y compris l'instauration d'une procédure complète de nettoyage et de restauration de tous les dispositifs de stockage de données ayant été retournés. En réaction aux plaintes, l'entreprise a amélioré ses procédures et ses mécanismes de contrôle. Toutefois, selon notre vérification, ceux-ci n'ont pas toujours été efficaces. En résumé, les lacunes observées en 2008 persistent et les renseignements personnels sont toujours menacés. Tant que ces problèmes ne seront pas réglés et que les recommandations formulées dans ce rapport ne seront pas mises en œuvre, Bureau en gros contreviendra à ses obligations en vertu de la LPRPDE.

Au sujet de la vérification

AUTORITÉ

L'article 18 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE ou la Loi) autorise le commissaire à la protection de la vie privée à procéder à la vérification des pratiques de gestion des renseignements personnels d'une organisation s'il a des motifs raisonnables de croire qu'il y a infraction à la Loi.

OBJECTIF

L'objectif de la vérification était d'évaluer si Bureau en gros avait instauré des mécanismes de contrôle adéquats pour protéger les renseignements personnels de ses clients (notamment ceux enregistrés sur des dispositifs de stockage de données ayant été retournés) et si ses politiques, processus et pratiques de gestion de ces renseignements sont conformes aux dix principes de protection de la vie privée prévus à l'annexe 1 de la LPRPDE.

CRITÈRES

Nous nous attendions à ce que Bureau en gros ait mis en œuvre des politiques et des processus qui satisfont aux exigences en matière de collecte, de consentement, d'utilisation, de communication et de conservation énumérés à l'annexe 1 de la LPRPDE (voir l'annexe B), notamment les suivants :

- les fins de la collecte des renseignements personnels doivent être déterminées avant la collecte ou au moment de celle-ci;
- le consentement de la personne concernée doit être obtenu avant la collecte, l'utilisation ou la communication des renseignements personnels;
- l'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées par l'organisation;
- les renseignements personnels ne peuvent être utilisés ou communiqués qu'aux fins pour lesquelles ils ont été recueillis, à moins que la personne concernée n'y consente ou que la loi ne l'exige;
- les renseignements personnels ne peuvent être conservés qu'aussi longtemps que nécessaire.

Conformément au principe sur les mesures de sécurité de la LPRPDE, Bureau en gros est tenue de prendre des mesures appropriées pour protéger les renseignements personnels qu'elle détient.

Enfin, selon les principes sur la responsabilité et la transparence de la LPRPDE, Bureau en gros doit :

- définir les rôles et assigner les responsabilités relativement au respect de la vie privée dans l'ensemble de l'organisation;
- instaurer des politiques et des procédures qui permettent d'appliquer les dix principes prévus à l'annexe 1 de la Loi, notamment la formation du personnel;
- donner facilement accès à de l'information précise sur ses politiques et ses procédures de gestion des renseignements personnels.

PORTÉE ET APPROCHE

La vérification a commencé par une enquête sur les pratiques de gestion des renseignements personnels de Bureau en gros. Cette étape comprenait des discussions avec des dirigeants au siège social de Bureau en gros et des visites dans deux points de vente au détail. Un échantillon choisi à dessein a été utilisé pour

établir le programme de la vérification. La situation géographique et la taille des succursales étaient prises en considération. Deux établissements régionaux de réparation, un centre d'appel, un service offrant des rabais en ligne et dix-sept succursales ont été choisis pour la vérification.

Dans le cadre de la vérification, divers moyens ont permis de recueillir des preuves, généralement des visites sur place, des entrevues et des renseignements obtenus dans des lettres. Nous avons aussi examiné les politiques, les procédures, les ententes, les documents décrivant le déroulement des opérations, les documents de formation et les contrôles d'accès au système de TI. Enfin, nous avons testé les dispositifs de stockage de données retournés qui devaient être revendus ou renvoyés au fournisseur pour vérifier s'ils contenaient des renseignements personnels (s'ils étaient correctement nettoyés et restaurés).

Le Commissariat n'a pas évalué les pratiques de gestion des renseignements personnels de Bureau en gros ni comparé celles-ci avec les pratiques ou les normes pouvant être en vigueur chez d'autres détaillants.

Les activités de vérification ont été menées dans la région de la capitale nationale et dans sept provinces. Le 31 décembre 2010, les travaux étaient en majeure partie finalisés.

NORMES

La vérification a été effectuée en conformité avec les pratiques, les politiques et le mandat législatif du Commissariat à la protection de la vie privée du Canada, et conformément à l'esprit des normes de vérification recommandées par l'Institut canadien des comptables agréés.

ÉQUIPE DE LA VÉRIFICATION

Directeur général : Steven Morgan

Garth Cookshaw
Dan Bourgeault
Bill Wilson

Annexe A : Recommandations et réponses

RECOMMANDATION

1. Prévoir des examens de conformité en matière de protection de la vie privée dans le cadre du programme de vérification interne.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a modifié sa liste de vérification visant à empêcher les pertes afin d'aborder plus en détail le stockage, la collecte, la conservation et l'élimination des renseignements personnels et d'autres aspects relatifs à la protection de la vie privée.

L'entreprise a mis sur pied un programme prévoyant l'inspection hebdomadaire des salles de technologie pour garantir le respect de la vie privée. En outre, elle offre des formations dans toutes ses succursales sur la protection de la vie privée dans les salles de technologie afin de renforcer les pratiques exemplaires de protection de la vie privée en ce qui a trait aux produits retournés par les clients ou à réparer. L'entreprise a créé une formation sur le code d'éthique et sur la gestion des renseignements personnels qui est obligatoire pour tous les associés, ce qui permet de mettre l'accent sur les priorités en matière de protection de la vie privée.

L'entreprise a centralisé ses services de récupération de données pour éviter que les succursales conservent des renseignements sur les clients dans la zone des services techniques. Elle a poursuivi le développement et la diffusion d'une application automatique qui repère les fichiers (pouvant appartenir aux clients) enregistrés par erreur sur les ordinateurs de la salle de technologie. Tous les fichiers repérés par cette application sont supprimés, conformément à la politique de l'entreprise de ne jamais conserver des données appartenant aux clients dans ses magasins.

L'entreprise continuera d'établir de nouveaux examens de conformité pour soutenir ses politiques en matière de protection de la vie privée. Une équipe de gouvernance interfonctionnelle a été créée pour veiller au respect de la vie privée.

RECOMMANDATION

2. Bureau en gros devrait informer ses clients de toute utilisation et communication de leurs renseignements personnels, dont le transfert dans des pays étrangers.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise modifiera sa politique sur le droit à la vie privée en conséquence d'ici le 15 mai 2011.

RECOMMANDATION

3. Bureau en gros ne devrait pas conserver de photocopies de documents d'identité délivrés par le gouvernement dans le cadre de son programme de crédit interne.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

La politique actuelle de l'entreprise interdit en toutes circonstances de reproduire et de conserver des documents d'identité délivrés par le gouvernement. L'entreprise a réitéré cette politique à ses succursales et continuera de l'appliquer.

RECOMMANDATION

4. Bureau en gros devrait veiller à ce que les demandes de crédit interne soient traitées dans une zone privée.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a envoyé une directive à toutes ses succursales pour rappeler à ses associés l'obligation de respecter la vie privée à toutes les étapes du processus de demande de crédit et continuera d'appliquer cette politique.

RECOMMANDATION

5. Bureau en gros devrait limiter la période de conservation des renseignements personnels associés aux demandes d'impression et de copie en ligne au temps nécessaire pour permettre au client de vérifier la qualité d'impression et de régler les problèmes s'il y a lieu.

Réponse de Bureau en gros :

L'entreprise convient que les clients devraient être informés du fait que leurs demandes en ligne seront conservées pendant un an.

L'entreprise croit que la conservation des demandes en ligne des clients pour une durée d'un an est utile aux clients et aux entreprises, car l'information est stockée de façon sécuritaire par un tiers et régie par des ententes et des restrictions appropriées. La seule personne pouvant provoquer la réutilisation ou la communication de l'information est le client lui-même. Toutefois, l'entreprise informera dûment les clients de cette pratique, ce qui permettra à ces derniers de choisir les services de photocopie au comptoir s'ils le désirent.

RECOMMANDATION

6. Bureau en gros devrait veiller à ce que les ententes de location conclues avec des fournisseurs de matériel exigent que ceux-ci remettent un certificat attestant la date à laquelle le disque dur a été nettoyé ou détruit.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise demandera des certificats de destruction à ses fournisseurs de matériel de photocopie. Cette demande a été communiquée aux fournisseurs actuels et sera ajoutée à toutes les prochaines ententes, nouvelles ou renouvelées, conclues avec les fournisseurs.

RECOMMANDATION

7. Bureau en gros devrait examiner ses procédures et processus de nettoyage des dispositifs de stockage et mettre en place des mécanismes de contrôle améliorés pour éliminer tout risque de communication des renseignements personnels.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

À la suite d'une plainte déposée en 2008, l'entreprise a instauré une politique de nettoyage et de restauration de tout dispositif de stockage d'information ayant été retourné avant la revente. Pour nettoyer et restaurer les ordinateurs de bureau et les ordinateurs portatifs, la compagnie suit les procédures et utilise les outils fournis par les fabricants. Ces procédures ne préservent que le logiciel d'origine expédié par l'usine. Contrairement à ce que stipule les avertissements du fabricant, selon lesquels ce processus effacera tous les fichiers, les données peuvent être récupérées à l'aide d'un logiciel judiciaire. Aucun fabricant ne conseille d'écraser les données dans le cadre du processus de nettoyage et de restauration recommandé. Le processus d'écrasement peut aussi endommager le disque dur de l'un ordinateur et détruire le logiciel original expédié par l'usine (y compris les outils de nettoyage et de restauration); l'utilisation généralisée de ce processus n'est donc pas commercialement rentable.

À l'aide d'un logiciel judiciaire, l'équipe de vérification du Commissariat à la protection de la vie privée a été en mesure de récupérer les données de certains ordinateurs qui avaient subi le processus de nettoyage et de restauration recommandé par le fabricant. Elle a recommandé la mise en place d'un processus de nettoyage et de restauration permettant d'« écraser » toutes les données des clients et de faire en sorte qu'il soit impossible de récupérer les données.

L'entreprise est en train de tester des moyens de nettoyer les données se trouvant sur un produit retourné (pour que les données ne puissent être récupérées à l'aide d'un logiciel judiciaire) sans endommager ou détruire les disques durs, les systèmes d'exploitation utiles et d'autres outils fournis par le fabricant.

RECOMMANDATION

8. Bureau en gros devrait s'assurer que les renseignements personnels sont conservés dans des classeurs verrouillés ou des zones sécurisées, comme le prévoit la politique de l'entreprise.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a réitéré sa position et continuera d'appliquer ses politiques relatives au stockage des renseignements personnels. Elle a ajouté cette question à ses procédures de vérification interne.

RECOMMANDATION

9. Bureau en gros devrait veiller à ce que les employés connaissent l'importance d'employer des méthodes sûres pour détruire les renseignements des clients.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise a réitéré sa position et continuera d'appliquer ses politiques relatives à la destruction des renseignements des clients. Elle a ajouté cette question à ses procédures de vérification interne.

RECOMMANDATION

10. Bureau en gros devrait faire en sorte que les employés aient des codes d'accès uniques pour favoriser la responsabilisation des utilisateurs et atténuer le risque d'accès non autorisé aux données des clients.

Réponse de Bureau en gros :

L'entreprise a accepté la recommandation.

L'entreprise continue de chercher des solutions pratiques pour sécuriser l'accès. Il est prévu qu'une application en cours de développement permette un accès personnalisé et sécurisé.

Soulignons que la politique actuelle de l'entreprise interdit de stocker des renseignements permettant d'identifier une personne sur un réseau partagé, sauf les systèmes qui doivent être utilisés à des fins opérationnelles. De plus, des politiques de contrôle d'accès relatives au serveur du point de vente situé dans les bureaux d'accueil des magasins sont en place et font l'objet d'une vérification. Les systèmes de l'entreprise permettent la fermeture de session automatique et l'alternance de mots de passe génériques.

Annexe B : Principes de l'annexe 1 de la LPRPDE pris en considération pendant la vérification

4.1 PREMIER PRINCIPE — RESPONSABILITÉ

Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

4.1.1

Il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidiens des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées.

4.1.2

Il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.

4.1.3

Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

4.1.4

Les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris :

a) la mise en œuvre des procédures pour protéger les renseignements personnels;

b) la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;

c) la formation du personnel et la transmission au personnel de l'information relative aux politiques et pratiques de l'organisation; et

d) la rédaction des documents explicatifs concernant leurs politiques et procédures.

4.2 DEUXIÈME PRINCIPE — DÉTERMINATION DES FINS DE LA COLLECTE DES RENSEIGNEMENTS

Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

4.2.1

L'organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe de la transparence (article 4.8) et au principe de l'accès aux renseignements personnels (article 4.9).

4.2.2

Le fait de préciser les fins de la collecte de renseignements personnels avant celle-ci ou au moment de celle-ci permet à l'organisation de déterminer les renseignements dont elle a besoin pour réaliser les fins mentionnées. Suivant le principe de la limitation en matière de collecte (article 4.4), l'organisation ne doit recueillir que les renseignements nécessaires aux fins mentionnées.

4.2.3

Il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ils sont destinés. Selon la façon dont se fait la collecte, cette précision peut être communiquée de vive voix ou par écrit. Par exemple, on peut indiquer ces fins sur un formulaire de demande de renseignements.

4.2.4

Avant de se servir de renseignements personnels à des fins non précisées antérieurement, les nouvelles fins doivent être précisées avant l'utilisation. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant d'utiliser les renseignements à cette nouvelle fin. Pour obtenir plus de précisions sur le consentement, se reporter au principe du consentement (article 4.3).

4.2.5

Les personnes qui recueillent des renseignements personnels devraient être en mesure d'expliquer à la personne concernée à quelles fins sont destinés ces renseignements.

4.2.6

Ce principe est étroitement lié au principe de la limitation de la collecte (article 4.4) et à celui de la limitation de l'utilisation, de la communication et de la conservation (article 4.5).

4.3 TROISIÈME PRINCIPE — CONSENTEMENT

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Note : Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu de la personne concernée et sans son consentement. Par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité, il peut être impossible ou peu réaliste d'obtenir le consentement de la personne concernée. Lorsqu'on recueille des renseignements aux fins du contrôle d'application de la loi, de la détection d'une fraude ou de sa prévention, on peut aller à l'encontre du but visé si l'on cherche à obtenir le consentement de la personne concernée. Il peut être impossible ou inopportun de chercher à obtenir le consentement d'un mineur, d'une personne gravement malade ou souffrant d'incapacité mentale. De plus, les organisations qui ne sont pas en relation directe avec la personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une œuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels cas, à ce que l'organisation qui fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels.

4.3.1

Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis. Généralement, une organisation obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte. Dans certains cas, une organisation peut obtenir le consentement concernant l'utilisation ou la communication des renseignements après avoir recueilli ces renseignements, mais avant de s'en servir, par exemple, quand elle veut les utiliser à des fins non précisées antérieurement.

4.3.2

Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

4.3.3

Une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

4.3.4

La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.

4.3.5

Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé. Le consentement ne doit pas être obtenu par un subterfuge.

4.3.6

La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur).

4.3.7

Le consentement peut revêtir différentes formes. Par exemple :

a) on peut se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisés;

b) on peut prévoir une case où la personne pourra indiquer en cochant qu'elle refuse que ses nom et adresse soient communiqués à d'autres organisations. Si la personne ne coche pas la case, il sera présumé qu'elle consent à ce que les renseignements soient communiqués à des tiers;

c) le consentement peut être donné de vive voix lorsque les renseignements sont recueillis par téléphone; ou

d) le consentement peut être donné au moment où le produit ou le service est utilisé.

4.3.8

Une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait.

4.4 QUATRIÈME PRINCIPE — LIMITATION DE LA COLLECTE

L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

4.4.1

Les organisations ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées. Conformément au principe de la transparence (article 4.8), les organisations doivent préciser la nature des renseignements recueillis comme partie intégrante de leurs politiques et pratiques concernant le traitement des renseignements.

4.4.2

L'exigence selon laquelle les organisations sont tenues de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis. Cette obligation suppose que le consentement à la collecte de renseignements ne doit pas être obtenu par un subterfuge.

4.4.3

Ce principe est étroitement lié au principe de détermination des fins auxquelles la collecte est destinée (article 4.2) et à celui du consentement (article 4.3).

4.5 CINQUIÈME PRINCIPE — LIMITATION DE L'UTILISATION, DE LA COMMUNICATION ET DE LA CONSERVATION

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

4.5.1

Les organisations qui se servent de renseignements personnels à des fins nouvelles doivent documenter ces fins (voir article 4.2.1).

4.5.2

Les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation. On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès à l'information après que la décision a été prise. Une organisation peut être assujettie à des exigences prévues par la loi en ce qui concerne les périodes de conservation.

4.5.3

On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

4.5.4

Ce principe est étroitement lié au principe du consentement (article 4.3), à celui de la détermination des fins auxquelles la collecte est destinée (article 4.2), ainsi qu'à celui de l'accès individuel (article 4.9).

4.7 SEPTIÈME PRINCIPE — MESURES DE SÉCURITÉ

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

4.7.1

Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

4.7.2

La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.

4.7.3

Les méthodes de protection devraient comprendre :

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;

b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et

c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

4.7.4

Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

4.7.5

Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3).

4.8 HUITIÈME PRINCIPE — TRANSPARENCE

Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

4.8.1

Les organisations doivent faire preuve de transparence au sujet de leurs politiques et pratiques concernant la gestion des renseignements personnels. Une personne doit pouvoir obtenir sans efforts déraisonnables de l'information au sujet des politiques et des pratiques d'une organisation. Ces renseignements doivent être fournis sous une forme généralement compréhensible.

4.8.2

Les renseignements fournis doivent comprendre :

a) le nom ou la fonction de même que l'adresse de la personne responsable de la politique et des pratiques de l'organisation et à qui il faut acheminer les plaintes et les demandes de renseignements;

b) la description du moyen d'accès aux renseignements personnels que possède l'organisation;

c) la description du genre de renseignements personnels que possède l'organisation, y compris une explication générale de l'usage auquel ils sont destinés;

d) une copie de toute brochure ou autre document d'information expliquant la politique, les normes ou les codes de l'organisation; et

e) la définition de la nature des renseignements personnels communiqués aux organisations connexes (par exemple, les filiales).

4.8.3

Une organisation peut rendre l'information concernant sa politique et ses pratiques accessibles de diverses façons. La méthode choisie est fonction de la nature des activités de l'organisation et d'autres considérations. Par exemple, une organisation peut offrir des brochures à son établissement, poster des renseignements à ses clients, offrir un accès en ligne ou établir un numéro de téléphone sans frais.