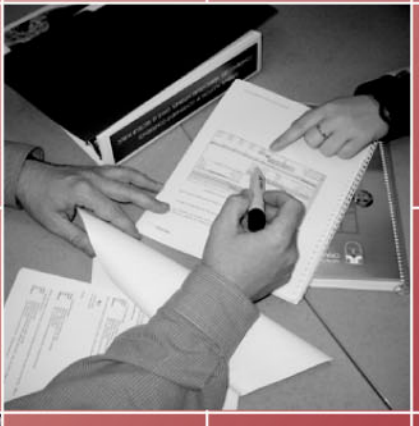
Services de vérification interne

Vérification de la gestion des renseignements personnels



Gouvernement du Canada
Government of Canada

Ressources humaines et Développement des compétences Canada
Human Resources and Skills Development Canada

Développement social Canada
Social Development Canada

Canada

SP-603-07-04F

Vérification de la gestion des renseignements personnels

No de projet : 6562/02

Équipe de projet

Directeur général:	*J.K. Martin*
Directeur de vérification :	*G. Duclos*
Chef d'équipe :	*S. Auguste*
Équipe de vérification :	*J. Clément*
	M. Gagnon
	K. Gourlay
	G. Lavergne
	J. Levesque
	S. Malichanh
	A. Markowitz
	C. Tremblay

APPROUVÉ:

DIRECTEUR:	*Gilles Duclos*	*14 juillet 2004*
	Nom	Date
DIRECTEUR GÉNÉRAL:	*James K. Martin*	*15 juillet 2004*
	Nom	Date

mai 2004

SP-603-07-04F
(also available in English)

Papier
ISBN : 0-662-77475-2
Cat. No.: HS3-1/603-07-04F

PDF
ISBN : 0-662-77476-0
Cat. No.: HS3-1/603-07-04F-PDF

HTML
ISBN : 0-662-77477-9
Cat. No.: HS3-1/603-07-04F-HTML

TABLE DES MATIÈRES

SOMMAIRE

Cette vérification a débuté à Développement des ressources humaines Canada (DRHC), qui a été réorganisé en deux nouveaux ministères – Ressources humaines et Développement des compétences Canada (RHDCC) et Développement social Canada (DSC). Les acronymes RHDCC ou DSC sont utilisés dans ce rapport lorsque les constatations ou les recommandations s'appliquent seulement à l'un des deux nouveaux ministères, et RHDCC/DSC est utilisé lorsqu'il s'agit des deux ministères. RHDCC/DSC est aussi utilisé pour designer l'ancien ministère.

Le **but** de cette vérification est de donner l'assurance que la gestion des renseignements personnels à RHDCC/DSC est en conformité avec *La Loi sur la protection des renseignements personnels*, particulièrement les articles *4 à 8* (communément désignés sous le nom *Code des pratiques équitables en matière d'information*) et que l'utilisation, la divulgation, la conservation et l'élimination des renseignements personnels respectent les politiques du Secrétariat du Conseil du Trésor (SCT) et celles du ministère.

Le travail de vérification sur le terrain à l'échelle nationale a été mené d'avril à décembre 2003. La vérification a mis l'accent sur les renseignements personnels reçus de l'Agence du revenu du Canada (ARC, autrefois connue sous le nom de Agence des douanes et du revenu du Canada – ADRC) et utilisés par Assurance-Emploi (AE), les Programmes de la sécurité du revenu (PSR), les Services financiers et administratifs – Systèmes ministériels des comptes débiteurs (SFA-SMCD) et la Politique stratégique (PS). Lorsque c'était approprié, la vérification s'est aussi penchée sur les renseignements personnels recueillis par RHDCC/DSC ou en provenance d'autres sources.

La **portée** de la vérification a été basée sur les objectifs opérationnels suivants :

- La manipulation et la protection des renseignements personnels sont incorporées au Cadre de gestion ministériel;
- La conservation, la protection et l'élimination des renseignements personnels sont conformes aux politiques gouvernementales en matière de sécurité;
- Les renseignements personnels sont accessibles seulement aux personnes autorisées et utilisés aux fins pour lesquelles l'information a été recueillie;
- Les renseignements personnels sont divulgués conformément à la *Loi sur la protection des renseignements personnels* et à d'autres législations, règlements, politiques et ententes applicables;
- L'information sur la nature et l'utilisation des renseignements personnels est mise à la disposition du public;
- Les personnes ont accès aux renseignements personnels les concernant, et des procédures sont en place pour gérer les plaintes.

Les critères associés à ces objectifs sont présentés à l'annexe A.

Des vérifications futures traiteront des aspects suivants de la gestion des renseignements personnels :

- L'échange de renseignements personnels avec d'autres organisations, ministères ou ordres de gouvernement par entente ou protocole d'entente (PE);
- La collecte, la manutention et la protection de renseignements personnels par RHDCC/DSC au sujet des ses propres employés;
- La collecte de renseignements personnels sur des demandeurs et clients pour l'administration de programmes de RHDCC/DSC.

Méthodologie

L'équipe de vérification a recueilli les données probantes des façons suivantes :

- Examen de politiques, procédures et initiatives documentées;
- Entrevue avec des employés et gestionnaires clés des politiques et des opérations à l'AC et dans les régions;
- Entrevue avec la direction et le personnel opérationnel des bureaux visités;
- Analyse des procédures et des contrôles existants;
- Tests et observation.

Cette vérification interne a été menée selon la politique du Secrétariat du Conseil du Trésor sur la vérification interne et de l'Institut des normes des vérificateurs internes pour la pratique de la vérification interne.

Principales constatations et conclusions de la vérification

Dans le présent rapport, le terme « Renseignements personnels » est utilisé soit au sens générique pour désigner la gestion en général des renseignements personnels et le cadre législatif et administratif qui le soutient.

L'information personnelle est définie comme l'information qui est ou peut être liée à un individu identifiable.

La confidentialité est l'attribut des renseignements personnels ou non personnels qui devraient être vus seulement par les personnes qui ont un droit et une raison légitime pour cela. La confidentialité soutient les notions de « besoin de savoir » et de « furetage » utilisées dans le rapport.

De l'avis des vérificateurs, la sensibilisation à la responsabilisation et à l'imputabilité en matière de renseignements personnels s'accroît à RHDCC/DSC. Trois nouveaux comités ont été mis sur pied pour fournir une orientation générale et des conseils sur les questions de protection des renseignements personnels :

- Comité directeur du cadre de gestion de la protection des renseignements personnels;

- Comité d'examen des bases de données;
- Comité de gestion de la sécurité de la technologie de l'information.

L'ébauche d'un cadre de responsabilisation pour la manipulation des renseignements personnels est en voie d'élaboration. Une fois terminé, ce document devrait être communiqué à tous les niveaux en tenant compte des interrelations et du partage des renseignements personnels entre les deux ministères.

Les politiques et les procédures sur la protection des renseignements personnels et la sécurité sont disponibles sur intranet et Internet. Les employés sont informés des politiques et des procédures. Les politiques et les procédures qui combinent sécurité et protection des renseignements personnels devraient être examinées pour que l'on puisse s'assurer que la partie concernant les renseignements personnels est couverte adéquatement et suffisamment.

L'entente signée par les télétravailleurs devrait être normalisée pour assurer que les clauses traitant de la confidentialité des renseignements personnels couvrent les politiques et les procédures applicables. Les membres du conseil arbitral devraient être régis par une entente similaire.

Une formation portant spécifiquement sur les renseignements personnels a été donnée aux coordinateurs. La plupart des employés qui prennent part à la manipulation ou à la divulgation des renseignements personnels ont reçu divers degrés de formation et d'information sur les renseignements personnels. Un plan national de communication et de formation stratégique devrait être élaboré pour garantir que tous les employés reçoivent une formation et une information opportunes et adéquates sur l'utilisation et la protection des renseignements personnels dans leur secteur d'activités.

La direction devrait s'assurer que ceux qui donnent ou ont accès aux renseignements personnels connaissent et comprennent la nature et l'application du principe du « besoin de savoir » ainsi que les conséquences des violations comme le « furetage » et les divulgations illégales.

Les renseignements personnels sont généralement conservés pour le temps prescrit avant d'être détruits ou archivés. Lorsque du matériel contenant des renseignements personnels sur les clients du ministère ou d'autres individus est envoyé ou détruit par des entreprises dans le cadre d'un contrat, ce contrat doit indiquer spécifiquement la responsabilité de l'entreprise de protéger la confidentialité des renseignements personnels sous son contrôle. Les numéros d'assurance sociale au complet ne devraient pas être écrits sur les boîtes expédiées par le Ministère.

L'accès aux dossiers des clients et aux bandes contenant des renseignements personnels est limité et contrôlé, mais le degré de protection contre l'accès non autorisé varie selon les régions et les programmes. La protection physique contre l'accès non autorisé ou le retrait de matériel imprimé contenant des renseignements personnels varie selon l'endroit où les documents contenant des renseignements personnels sont conservés; des évaluations individuelles de risque et de contrôles devraient donc être menées sur ces sites.

Les employés sont généralement informés des règlements qui concernent la modification des renseignements personnels, mais les règles et les procédures pour enregistrer la source et la raison des modifications apportées aux renseignements personnels ainsi que pour conserver les documents probants devraient être clarifiées.

Les diverses étapes de l'attribution, de la maintenance et la suppression des codes d'accès[1] devraient être révisées pour garantir que la responsabilité et l'imputabilité des identificateurs sont clairement définies, bien comprises et acceptés.

Un test destiné à fournir l'assurance que les codes d'accès existants limitent l'accès aux renseignements personnels requis par l'utilisateur pour remplir des tâches légitimes a dû être reporté. Les conditions qui permettront la réalisation efficace et efficiente de ce test devraient être établies aussitôt que possible.

PROTÉGÉ

Le guide sur la classification et la manipulation de documents contenant des renseignements personnels devrait être complété et appuyé par des conseils pratiques concernant les documents électroniques et papier contenant des renseignements personnels les plus souvent utilisés. Des contrôles internes devraient être mis en place pour assurer que les documents protégés sont identifiés et manipulés selon la classification appropriée.

Le processus à suivre par les gestionnaires et les employés qui deviennent informés de violations possibles relatives aux renseignements personnels doit être clarifié et communiqué.

On devrait tenir compte de la nature et du caractère délicat des renseignements divulgués pour établir une distinction entre la divulgation officielle et non officielle, et les règles pour documenter la divulgation devraient être révisées.

Les employés comprennent généralement leur responsabilité en ce qui concerne la divulgation de renseignements personnels (vérification d'identité ou de délégation et exemptions) mais les règles concernant la documentation dans le dossier du client des requêtes non officielles devraient être clarifiées.

[1] Les codes d'accès sont définis à la section 3.2.2

L'information sur la nature et l'utilisation de renseignements personnels est disponible au public dans Info Source, et les clients sont informés de leur droit d'accès au contenu de leur dossier. Des mécanismes pour gérer la protection des renseignements personnels relativement aux plaintes sont en place dans toutes les régions visitées.

Opinion générale

Nous sommes d'opinion, à la lumière de notre vérification, que des progrès importants ont été réalisés et continuent de l'être dans la gestion des renseignements personnels.

Des améliorations supplémentaires sont cependant nécessaires, comme l'indiquent nos recommandations.

La gestion a développé un plan d'action adéquat (Annexe B) pour répondre à ces recommandations. Sa réalisation, particulièrement en ce qui concerne les recommandations 9 à 12, devrait résulter dans la mise en place des contrôles requis pour une gestion appropriée des renseignements personnels au sein de RHDCC et de DSC.

Selon notre jugement professionnel, des procédures de vérification adéquates ont été suivies et des preuves suffisantes ont été recueillies pour supporter les conclusions de ce rapport. Ces conclusions sont basées sur une comparaison de la situation qui existait au moment de la vérification avec les critères de vérification. Les conclusions ne s'appliquent que sur la gestion des renseignements personnels pour les activités examinées.

Cette vérification interne a été conduite en conformité avec la politique du Conseil du Trésor sur la vérification interne et les standards de l'Institut des vérificateurs internes sur les pratiques professionnelles.

Réponse générale de la direction

Le directeur général de Protection des renseignements personnels, conjointement avec les coordonnateurs pour RHDCC et DSC, ainsi que plusieurs directeurs généraux ont examiné la vérification de la gestion de la protection des renseignements personnels et ont collaboré à la préparation du plan d'action de gestion qui l'accompagne.

Les préoccupations exprimées par les Canadiens au sujet des renseignements personnels continuent de croître. La large disponibilité des offres de services intégrées, souvent offertes par le biais des nouveaux canaux électroniques, en est un des facteurs contributifs. Les Canadiens veulent avoir l'assurance que leurs renseignements personnels sont gérés soigneusement selon des paramètres bien définis. La Loi sur la protection des renseignements personnels et les autorités des programmes concernés définissent l'obligation de protéger les renseignements personnels et d'en assurer la cueillette, l'utilisation et la divulgation de manière appropriée. Ces autorités législatives sont appuyées par des politiques, des procédures et des outils qui ont fait l'objet de cette vérification.

La vérification interne et le plan d'action de gestion représentent une étape clé de la mise en oeuvre du Cadre de gestion de la protection des renseignements personnels (CGPRP) qui a été primé. Ce cadre et ses quatre piliers de planification et gouvernance stratégiques, de gestion du risque, de changements culturels et d'assurance de conformité, concentrent l'attention ministérielle sur les questions qui ont trait à la vie privée. Des progrès considérables ont été réalisés et les initiatives des ministères ont été reconnues.

Ensemble, le CGPRP et cette vérification servent à démontrer de quelle manière nous remplissons notre obligation de protéger les renseignements personnels des Canadiens. Pour les deux dernières années, DRHC a reconnu la protection des renseignements personnels comme une priorité ministérielle stratégique dans le cadre de son objectif d'excellence du service. C'est une reconnaissance explicite, au plus haut niveau du ministère, de l'importance des renseignements personnels pour les Canadiens et leurs attentes à l'égard du gouvernement pour leur protection. Les Canadiens s'attendent à ce que RHDCC et DSC maintiennent cet engagement de gérer efficacement les renseignements personnels et de l'incorporer comme une composante intrinsèque de leurs cultures respectives. Comme la vérification l'a clairement démontré, la gestion efficace des renseignements personnels n'est pas différente de celle des autres actifs stratégiques. C'est pourquoi les contrôles sont en train d'être renforcés là où c'est nécessaire et un plan de formation national est en élaboration.

Tandis que RHDCC et DSC débutent la mise en œuvre de ce plan d'action de gestion, nous prenons l'engagement de déployer des efforts coordonnés pour remplir notre rôle de gardiens des renseignements personnels et maintenir la confiance que les Canadiens et les Canadiennes ont placée en nous.

1. INTRODUCTION

Contexte

Cette vérification a débuté à Développement des ressources humaines Canada (DRHC), qui a été réorganisé en deux nouveaux ministères – Ressources humaines et Développement des compétences Canada (RHDCC) et Développement social Canada (DSC). Les acronymes RHDCC ou DSC sont utilisés dans le rapport lorsque les constatations ou les recommandations s'appliquent seulement à l'un des deux nouveaux ministères, et RHDCC/DSC est utilisé lorsqu'il s'agit des deux ministères. RHDCC/DSC est aussi utilisé pour designer l'ancien ministère.

Dans le cadre de ses activités, RHDCC/DSC recueille et utilise des renseignements personnels concernant ses clients et reçoit des renseignements personnels en provenance d'autres sources, comme l'Agence du revenu du Canada (ARC — anciennement appelée Agence des douanes et du revenu). En juin 2001, l'ARC a demandé à RHDCC/DSC de lui donner l'assurance que les renseignements personnels qu'elle transférait au Ministère étaient manipulés conformément à la *Loi sur la protection des renseignements personnels* et aux politiques connexes.

Dans son plan d'activités ministériel annuel pour 2003-2004, RHDCC/DSC a fait remarquer que les Canadiens, tout au long de leur vie, sont amenés à confier au Ministère des renseignements personnels sensibles. Le Ministère s'est engagé à garantir que la gestion de ces renseignements demeure conforme:

- à toutes les exigences et les mesures relatives à la protection des renseignements personnels régies par la loi;
- aux normes les plus élevées de respect de la vie privée et des renseignements personnels;
- aux normes de sécurité les plus élevées concernant les systèmes qui recueillent et emmagasinent ces renseignements et soit perçue ainsi.

RHDCC/DSC a reconnu qu'il fallait respecter ces critères si l'on souhaitait que les clients demeurent disposés à transmettre des renseignements personnels les concernant, à plus forte raison depuis que les ministères ont commencé à mettre sur pied de nouvelles voies de communication permettant aux citoyens d'effectuer des opérations électroniques aussi bien en personne, par téléphone et par courrier.

Compte tenu de l'importance d'une saine gestion des renseignements personnels, RHDCC/DSC a amorcé la mise en œuvre d'un Cadre de gestion de la protection des renseignements personnels en 2000.

Afin de maintenir la confiance des Canadiens à l'égard de son utilisation des renseignements personnels, le Ministère a chargé, en 2003, les Services de vérification interne d'effectuer la présente vérification afin de donner l'assurance que l'accessibilité, l'utilisation, la conservation, la divulgation et l'élimination des renseignements personnels :

- sont conformes à la *Loi sur la protection des renseignements personnels*;
- respectent les politiques du Ministère et du Conseil du Trésor.

Portée de la vérification

Auparavant, RHDCC/DSC n'avait jamais effectué de vérification de la gestion des renseignements personnels. Pour déterminer les objectifs et les critères de la vérification, les vérificateurs ont donc mené des consultations extensives avec le Secrétariat du Conseil du Trésor (SCT), l'ARC et le Commissariat à la protection de la vie privée (SPVP). Des consultations internes ont également eu lieu avec la direction de la protection des renseignements personnels de RHDCC/DSC et les représentants des programmes et des services ministériels concernés.

La gestion des renseignements personnels est un domaine particulièrement complexe. Les renseignements personnels sont diffusés matériellement et électroniquement entre les systèmes, les secteurs de programme, les bureaux et les régions. RHDCC/DSC compte 320 points de service personnels dans les collectivités, 21 centres d'appel et quatre centres régionaux des technologies de l'information. Ses activités essentielles touchent chaque jour des millions de Canadiens qui comptent sur les programmes et les services du Ministère. Par conséquent, des renseignements personnels apparaissent, de façon au moins éphémère, sur :

- les documents transmis aux clients;
- les dossiers des clients de RHDCC/DSC;
- la mise en mémoire informatique sur bandes et sur disques;
- les écrans d'ordinateur auxquels ont accès des employés de tout le pays pour servir les clients.

En outre, les politiques, les procédures et les mesures de contrôle actuelles relatives à la protection des renseignements personnels sont intégrées dans les politiques de sécurité, ce qui accroît encore la complexité de la gestion des renseignements personnels. La sécurité est une condition préalable à la protection des renseignements personnels, mais sa présence ne suffit pas à garantir la confidentialité. Par exemple, le principe selon lequel les employés doivent n'avoir accès qu'aux renseignements personnels nécessaires à l'exercice de leurs fonctions (besoin de savoir) est lié à l'attribution et au maintien des codes d'accès. Or, l'attribution et le maintien de ces codes relèvent essentiellement des technologies de l'information qui vont au delà de la portée de cette vérification. ¨Par ailleurs, l'accès logique aux renseignements personnels établit souvent une distinction entre l'accès passif (lecture seule) et le mode actif (possibilité d'écrire et de modifier les données); cette caractéristique se rapporte directement à la sécurité, mais n'a que peu d'incidence sur la protection des renseignements personnels.

En avril 2003, à la suite de consultations et d'évaluations des risques, le Comité de vérification et d'évaluation a convenu d'axer la vérification sur quatre principaux secteurs de programmes :

- l'assurance-emploi (AE);
- la Sécurité de la vieillesse et le Régime de pensions du Canada (RPC);
- les Services financiers et administratifs — Systèmes ministériels des comptes débiteurs (SFA-SMCD);
- la Politique stratégique (données utilisées dans l'analyse des politiques, la recherche et les activités d'évaluation).

Le Comité a également approuvé les objectifs suivants[2] :

- la manutention et la protection des renseignements personnels sont incorporées au Cadre de gestion ministériel;
- la conservation, la protection et l'élimination des renseignements personnels respectent les politiques de sécurité du gouvernement;
- les renseignements personnels sont accessibles seulement aux personnes autorisées et utilisés dans le but pour lequel ils ont été recueillis;
- les renseignements personnels sont divulgués dans le respect de la *Loi sur la protection des renseignements personnels* et autres lois, règlements, politiques et ententes applicables;
- l'information sur la nature et l'utilisation des renseignements personnels est à la disposition du public;
- les personnes ont accès à leurs propres renseignements personnels et les procédures sont mises en place pour traiter les plaintes.

L'annexe A contient une description détaillée des critères qui nous ont permis de déterminer si le Ministère avait réalisé ces objectifs. Dans le cadre de la vérification, on a mené des travaux sur le terrain à l'administration centrale (AC), dans six régions, dans six bureaux régionaux (BR), dans les quatre centres des technologies de l'information (CTI) et dans 34 bureaux et points de service, entre avril et décembre 2003 (voir l'annexe C pour plus de détails).

[2] Il y avait à l'origine dix objectifs. Deux de ces objectifs, portant sur la collecte des renseignements personnels, ont été laissés de côté en vue d'une vérification ultérieure. On a ensuite regroupé les huit autres pour former les six objectifs énumérés ci-dessus pour faciliter de rédaction de ce rapport.

Méthodologie

L'équipe de vérification a recueilli les données probantes des façons suivantes:

- Examen de politiques, procédures et initiatives documentées;
- Entrevue avec des employés des politiques et des opérations et de la direction à l'AC et des régions;
- Entrevue avec la direction et le personnel opérationnel des bureaux visités;
- Analyse des procédures et des contrôles existants;
- Tests et observation.

Des comptes rendus dont été donnés au terme du travail sur le terrain dans les régions visitées. Le rapport national se fonde sur des constatations qui s'appliquent à un grand nombre de régions et/ou qui ont une incidence à l'échelle nationale.

2. CONSTATATIONS DE LA VÉRIFICATION

Toutes les constatations importantes liées à la vérification sont décrites dans la présente section et respectent les objectifs et les critères de vérification détaillés à l'annexe A Objectifs, critères et méthodologie de la vérification. Une déclaration de fiabilité est incluse pour chacun des critères, même lorsqu'on n'a pas répondu aux attentes en matière de rendement.

Dans le présent rapport, l'expression « Renseignements personnels » est utilisée au sens générique pour désigner la gestion en général des renseignements personnels et le cadre législatif et administratif qui la soutient.

Les renseignements personnels se définissent comme étant de l'information qui est ou peut être liée à un individu identifiable.

La confidentialité est l'attribut des renseignements personnels ou non personnels qui devraient être vus seulement par les personnes qui ont un droit et une raison légitime pour cela. La confidentialité soutient les notions de « besoin de savoir » et de « furetage » utilisées dans le rapport.

Objectifs de la vérification

Le but de cette vérification est de donner l'assurance que la gestion des renseignements personnels à RHDCC/DSC est en conformité avec *La Loi sur la protection des renseignements personnels*, particulièrement les articles *4 à 8* (communément désignés sous le nom *Code des pratiques équitables en matière d'information*) et que l'utilisation, la divulgation, la conservation et l'élimination des renseignements personnels respectent les politiques du Secrétariat du Conseil du Trésor (SCT) et celles du ministère.

2.1 Objectif 1 : La manutention et la protection des renseignements personnels sont intégrées au Cadre de gestion ministériel

Critères de la vérification

- La responsabilité de la protection et des usages judicieux des renseignements personnels est définie et documentée.
- Les politiques, les lignes directrices et les procédures relatives à la manutention et à la protection des renseignements personnels sont disponibles, et les employés en sont informés et (ou) ont reçu une formation pertinente à ces questions.
- La vérification, le contrôle, l'évaluation des risques et des contrôles liés à la manutention et à la protection des renseignements personnels sont faits régulièrement.

2.1.1 Responsabilité et imputabilité

Au cours des entrevues, une sensibilisation accrue des gestionnaires et des employés à l'égard de leurs responsabilités envers la protection de la vie privée et des renseignements personnels a été rapportée.

RHDCC/DSC a déployé des efforts concertés dans le but d'améliorer la manipulation des renseignements personnels; on a mis en œuvre plusieurs projets afin d'établir des politiques, une orientation et des procédures plus claires en matière de protection des renseignements personnels.

1. On a mis sur pied le Comité directeur du cadre de gestion de la protection des renseignements personnels. Celui-ci dirige l'élaboration et la mise en œuvre du Cadre de gestion de la protection des renseignements personnels, lequel définit l'obligation de rendre compte et les responsabilités du sous-ministre en matière de protection des renseignements personnels à l'égard des employés et dans tous les programmes. Le Comité directeur a également le mandat de superviser les mesures prises en rapport avec les questions de principes ministérielles concernant la protection des renseignements personnels.

2. Le Comité d'examen des bases de données est un comité de niveau supérieur qui a été chargé d'examiner toutes les analyses des politiques, les recherches et les activités d'évaluation du Ministère exigeant l'établissement de liens entre les banques de données et (ou) l'utilisation de codes d'identification personnels non masqués (non anonymisés).

3. Le Comité de gestion de la sécurité de la technologie de l'information a été chargé d'effectuer une surveillance opportune et efficace, et de fournir des directives, des conseils et une orientation à la fonction de sécurité de la technologie de l'information de RHDCC/DSC.

Plusieurs secteurs des nouveaux ministères (RHDCC et DSC) sont interreliés. Par exemple, la prestation des services d'AE (et la manipulation des renseignements personnels connexes) est effectuée par les centres de traitement (RHDCC) et les centres d'appel (DSC). Certains services ministériels financiers et administratifs se retrouvent dans différents secteurs. Il est donc de plus en plus nécessaire d'établir un cadre d'imputabilité qui tiendra compte de cette réalité et fournira un soutien et une orientation aux deux ministères.

Recommandation 1 : (RHDCC/DSC)

On devrait élaborer, communiquer et mettre en œuvre à tous les niveaux et dès que possible un cadre d'imputabilité pour la manipulation des renseignements personnels tenant compte des interrelations et du partage des renseignements personnels entre les deux ministères.

Réponse de la direction :

Le rapport de vérification a montré qu'il était important que les deux ministères disposent d'un cadre redditionnel en rapport avec la manipulation et la protection des renseignements personnels. Au cours des dernières années, RHDCC/DSC a affiché une attitude proactive en élaborant et en appliquant un cadre détaillé de gestion de la protection des renseignements personnels. Ce cadre comprend quatre piliers : la planification et la gouvernance stratégiques, la gestion du risque, les changements culturels et l'assurance de conformité. La mise en œuvre du Cadre de gestion de la protection des renseignements personnels appuie l'engagement des deux ministères à l'égard de la protection des renseignements personnels. Le Comité directeur du cadre de gestion de la protection des renseignements personnels a donc approuvé, en matière de protection des renseignements personnels et de sécurité, des obligations de rendre compte à l'échelle de RHDCC/DSC qui touchent notamment les agents supérieurs de la protection des renseignements personnels. La mise en œuvre de ce mécanisme formalisera les responsabilités existantes des sous-ministres et de chaque employé en matière de protection des renseignements personnel et de sécurité.

D'autres projets ont été mis en œuvre en vue d'accroître la sensibilisation des gestionnaires et du personnel. Par exemple, on rédigera une déclaration globale relative à la protection des renseignements personnels précisant les engagements des ministères envers la manipulation appropriée des renseignements personnels, et on élaborera des modules d'éducation qui complèteront les plans de formation ministériels et opérationnels.

2.1.2 Politiques, procédures et lignes directrices

Les politiques et les procédures concernant la protection des renseignements personnels et la sécurité sont accessibles sur l'intranet et Internet. Les employés sont informés à ce sujet par courrier électronique et au moyen de notes de service.

Les politiques et les procédures actuelles concernent l'accès par les personnes aux renseignements personnels les concernant et qui sont détenus par RHDCC/DSC, de même que la divulgation de ces renseignements à eux-mêmes ou à leurs représentants. Cependant, les vérificateurs estiment que les politiques et les procédures de gestion des renseignements personnels sont généralement axées sur l'aspect sécurité plutôt que sur la protection des renseignements personnels. Par exemple, l'accès est souvent défini en termes de « lecture seule » (souvent appelé « interrogation ou visualisation ») ou de « rédaction et modification » (parfois appelé « mise à jour, décision ou approbation »). Ces privilèges se rapportent davantage à la sécurité qu'à la confidentialité des renseignements personnels. Dans le même ordre d'idées, les entrevues ont amené les vérificateurs à conclure que les prescriptions liées à l'expédition de documents contenant des renseignements personnels par des transporteurs publics concernaient davantage la sécurité que la protection de la confidentialité.

Recommandation 2 : (RHDCC/DSC)

Les politiques et les procédures de gestion des renseignements personnels devraient être revues pour s'assurer que l'aspect de la protection de la confidentialité est suffisamment et convenablement couvert.

Réponse de la direction :

Le rapport met en lumière le besoin d'améliorer la mise en œuvre des volets sécurité et protection des renseignements personnels des politiques et des procédures de manipulation des renseignements personnels. Les politiques et les procédures actuelles de manipulation des renseignements personnels mettent à contribution les experts de la protection des renseignements personnels, de la gestion de l'information et de la sécurité à RHDCC/DSC. Les experts de la protection des renseignements personnels dirigent les activités de collecte, d'utilisation, de divulgation et d'élimination; les experts de la gestion de l'information se chargent plus précisément des questions de la conservation; et les experts de la sécurité s'intéressent aux aspects techniques de l'accès, de l'entreposage, de la transmission et de l'élimination. Cette structure reflète les politiques et les lignes directrices du Conseil du Trésor sur la protection des renseignements personnels et des données, sur la gestion des renseignements détenus par le gouvernement, et sur la sécurité gouvernementale, de même que les politiques, les procédures et les lignes directrices ministérielles au niveau opérationnel et au niveau de l'organisation. Avec l'aide des experts de la protection des renseignements personnels, les directions générales de RHDCC/DSC examineront, conformément au Cadre de gestion de la protection des renseignements personnels, la justesse et la suffisance de leurs politiques et de leurs procédures de manipulation des renseignements personnels.

Même si, de l'avis des vérificateurs, les lignes directrices et les procédures visant les télétravailleurs (les employés autorisés à apporter des documents à la maison pour y travailler) sont, elles aussi, principalement axées sur la sécurité, la protection des renseignements personnels est généralement traitée convenablement. Le *Manuel des politiques et méthodes de sécurité des Centres de ressources humaines du Canada* fournit des directives spécifiques pour le transport et la protection des documents sensibles à la maison. Il contient un paragraphe précisant les précautions à prendre pour s'assurer que les dossiers sensibles dans le lieu de télétravail ne soient pas accessibles aux personnes non autorisées, par exemple aux concierges dans des locaux loués, aux membres de la famille ou aux invités. Les télétravailleurs doivent signer une entente concernant le respect des règlements relatifs à la sécurité et à la protection des renseignements personnels. Ces ententes varient d'une région à l'autre, et certaines insistent davantage que d'autres sur l'obligation de protéger la confidentialité des renseignements et sur les règles à suivre à ce chapitre.

Les membres des conseils arbitraux de l'AE (un tribunal administratif composé de personnes qui ne sont pas des employées du Ministère et qui entend les appels relatifs aux décisions de l'assurance-emploi) emportent généralement chez eux des dossiers d'appel contenant des renseignements personnels pouvant se révéler sensibles. Ils signent un document dans lequel ils s'engagent à faire preuve de discrétion en évitant de discuter du

contenu des dossiers d'appel en dehors de la salle du conseil et ils s'engagent à remettre leurs exemplaires des dossiers d'appel au greffier du conseil à la fin de chaque séance quotidienne pour être déchiquetés. Cependant, les membres du conseil arbitral ne signent aucune entente formelle sur la manutention et la protection des dossiers d'appel de la même nature que celle signée par la plupart des télétravailleurs.

Recommandation 3 : (RHDCC/DSC)

Les ententes signées par les télétravailleurs devraient être normalisées pour s'assurer que les clauses portant sur la confidentialité des renseignements personnels portent spécifiquement sur l'obligation de protéger la confidentialité des renseignements et les règles à suivre à ce chapitre. Les membres des conseils arbitraux de l'AE devraient être tenus de signer une entente semblable.

Réponse de la direction :

Bien que le rapport précise que des exigences adéquates en matière de protection des renseignements personnels sont en place dans le cas des télétravailleurs, ils soulignent également le besoin d'adopter une approche normalisée. Avec l'aide des experts de la protection des renseignements personnels et de la sécurité, la Direction générale des ressources humaines examinera l'utilisation des dispositions courantes concernant les télétravailleurs afin de garantir une protection constante des renseignements personnels à l'extérieur des locaux ministériels.

En ce qui concerne le conseil arbitral, cet organe est indépendant et n'est pas soumis à RHDCC ni à la Commission de l'assurance-emploi du Canada. RHDCC n'a aucun pouvoir hiérarchique sur le conseil arbitral ou sur ses membres. Ces derniers sont soumis à une enquête de sécurité et doivent signer un engagement avant leur nomination. Une fois nommés, les membres du conseil reçoivent la Politique et administration des conseils arbitraux (sujet 16 du Guide de la politique des services d'assurance), qui précise :

> *« Les présidents et les membres des conseils doivent en tout temps se préoccuper du fait que les dossiers d'appels renferment des renseignements personnels protégés. Ainsi, au terme de la séance de la journée, les membres du conseil arbitral doivent remettre leur copie des dossiers d'appel au greffier du Conseil pour qu'il la déchiquette avec les rebuts confidentiels. »*

De plus, au cours des derniers mois, la Direction générale de l'assurance a poursuivi l'élaboration et la mise en œuvre des politiques et des procédures dans le but de garantir que les membres du conseil sont informés de leur obligation de protéger les renseignements provenant de dossiers d'appel, des audiences et des décisions.

2.1.3 Information et formation

La connaissance et la compréhension des attentes constituent un aspect important du Cadre de gestion de la protection des renseignements personnels. Les entrevues ont montré que les gestionnaires et les employés comprenaient mieux qu'avant leurs

responsabilités relativement à la protection des renseignements personnels concernant les clients et d'autres personnes.

La *Loi sur l'emploi dans la fonction publique* précise que tout nouvel employé doit signer un Serment professionnel et engagement au secret professionnel. En outre, les employés qui doivent accéder à des renseignements personnels ont déclaré qu'on leur avait décrit les enjeux liés à la protection des renseignements personnels au cours de leur formation initiale, en insistant sur la divulgation des renseignements personnels et les conflits d'intérêts (p. ex., dans le cas de la gestion du dossier d'un ami ou d'un parent).

Une formation officielle portant plus particulièrement sur la protection des renseignements personnels est offerte. On a affiché de l'information sur Internet afin d'aider les coordonnateurs de la protection des renseignements personnels de l'AE à offrir de la formation, et les PSR sont en train de renforcer les modules sur la protection des renseignements personnels, qu'ils afficheront sur leur site collégial à l'été 2004. Les responsables de la PS ont également élaboré une présentation Internet — protocole sur la protection des renseignements personnels pour la recherche — en vue de l'organisation de séances d'information internes.

Les coordonnateurs de la protection des renseignements personnels ont reçu une formation appropriée. Au moment de la vérification, une formation portant précisément sur la protection des renseignements personnels était en voie d'être offerte aux gestionnaires et aux employés des secteurs de l'AE, des PSR, de la PS et des SFA (SMCD). Les employés et les gestionnaires ont déclaré que l'on discutait maintenant plus fréquemment des questions relatives à la protection des renseignements personnels pendant les réunions du personnel et les séances d'information.

Au moment de la vérification, des plans de communication et de formation en matière de protection des renseignements personnels étaient en place. Cependant, ces plans n'étaient pas stratégiques, et leur portée variait d'une région à l'autre et d'un programme à l'autre.

Recommandation 4 : (RHDCC/DSC)

Un plan stratégique national de formation et de communication devrait être développé pour s'assurer que tous les employés qui ont ou pourraient avoir accès à des renseignements personnels reçoivent une formation et des informations opportunes et appropriées sur la législation, les politiques et les procédures concernant l'utilisation et la protection des renseignements personnels dans leur secteur d'activité.

Réponse de la direction :

Le rapport de vérification recommande l'élaboration d'un plan national de formation et de communication, afin de compléter la formation opérationnelle fournie par la direction générale et les régions. Au cours des trois dernières années, RHDCC/DSC a prôné le renforcement d'une vision commune des valeurs et de l'éthique des employés et de l'organisation. La Direction générale des ressources humaines orchestre l'établissement d'un plan de formation national qui permettra d'évaluer les besoins en matière d'apprentissage, et de concevoir et d'adapter les produits d'apprentissage afin de fournir une formation opportune et appropriée sur l'utilisation et la protection des renseignements personnels.

Ce plan sera mis en œuvre conjointement avec les directions générales et les bureaux régionaux du Ministère, et mettra à contribution les directions de l'AIPRP et la sécurité des SFA.

Jusqu'à une époque récente, les coordonnateurs régionaux et locaux de la protection des renseignements personnels traitaient surtout des demandes officielles visant la divulgation des renseignements personnels et des demandes d'accès à l'information (AIPRP). L'un des coordonnateurs régionaux de la protection des renseignements personnels interrogés dans le cadre de la vérification a réagi de façon proactive à l'évolution des enjeux liés à la protection des renseignements personnels en établissant une formation et des documents de référence, et en lançant un débat à ce sujet. D'autres, plus conservateurs, ont précisé qu'ils attendaient d'obtenir des directives pour modifier de façon significative la nature et la portée de leurs activités.

Afin d'évaluer le degré de prise de conscience et de compréhension par les gestionnaires et les employés des principes fondamentaux de la protection des renseignements personnels, les vérificateurs ont utilisé, pendant les entrevues, l'expression « besoin de savoir ». Cette expression illustre le principe selon lequel un employé ne devrait pas avoir accès à des renseignements personnels s'il n'en a pas besoin pour remplir ses fonctions actuelles. Par exemple, le fait de permettre aux employés d'accéder à des écrans contenant des renseignements financiers personnels touchant les clients ne respecte pas le principe du « besoin de savoir » si les employés n'ont pas besoin de ces renseignements pour établir une période de prestation ou rendre une décision.

Pour les besoins de la vérification, on a appelé « furetage » un type particulier de violation du principe du besoin de savoir. Le furetage a été défini comme étant la consultation de renseignements personnels sur un individu pour des motifs autres que des motifs professionnels légitimes. Le furetage n'est pas autorisé à RHDCC/DSC et serait considéré comme une infraction, même si l'employé n'a obtenu aucun avantage personnel en consultant les renseignements ou n'avait pas l'intention d'utiliser les renseignements à des fins illicites. La plupart des employés savaient que dans le cas où une personne accédait à des renseignements dans un but contraire à l'éthique, comme l'obtention d'un avantage personnel, le furetage deviendrait une infraction grave pouvant entraîner des sanctions sévères.

Pendant les entrevues, les employés et les gestionnaires ont mentionné qu'il n'était pas convenable de consulter le dossier d'un ami ou d'un parent. Lorsqu'on leur a posé la question spécifiquement, ils ont précisé qu'il était inopportun de consulter tout dossier ou écran contenant des renseignements personnels à des fins autres que des fins professionnelles valables.

À la suite des entrevues avec les gestionnaires et les employés, les vérificateurs ont conclu que la compréhension et la sensibilisation à l'égard des violations éventuelles du principe de « besoin de savoir » pouvaient être renforcées.

La plupart des gestionnaires et des superviseurs interrogés n'avaient pas une connaissance précise de la nature et la quantité des renseignements personnels auxquels leurs employés avaient accès. Lorsqu'ils formulent une demande d'accès pour un nouvel employé ou un employé qui remplit de nouvelles fonctions, ils copient souvent la plus récente demande établie à l'intention d'un employé exécutant des tâches semblables (une pratique généralement désignée sous le nom de « clonage »). On trouvera sous l'objectif 3 une description plus détaillée du processus d'attribution de l'accès.

Recommandation 5 : (RHDCC/DSC)

La direction devrait s'assurer que les personnes qui donnent et qui obtiennent l'accès à des renseignements personnels comprennent la nature et l'application du principe du « besoin de savoir », de même que les conséquences de violation telles le « furetage » et les divulgations illicites.

Réponse de la direction :

Nous souscrivons à la recommandation du rapport selon laquelle le principe du besoin de savoir et les conséquences entraînées par la violation de ce principe devraient être bien compris. En plus du plan de formation national élaboré par la Direction générale des ressources humaines, la sécurité des SFA organisera des séances de sensibilisation régulières afin de garantir que ce principe et les conséquences de sa violation sont clairement compris.

RHDCC/DSC s'engage à protéger les renseignements personnels. Le Ministère veillera à ce que les renseignements qu'il recueille et génère soient manipulés conformément à la Loi sur la protection des renseignements personnels et aux autres lois applicables en matière de protection de la confidentialité. Le Comité directeur du cadre de gestion de la protection des renseignements personnels a approuvé l'ébauche de politique et de lignes directrices concernant la mise en œuvre et la surveillance de pistes de vérification à RHDC, ce qui permettra d'attester que seules les personnes présentant un besoin de savoir manifeste et ayant fait l'objet d'une enquête de sécurité au niveau approprié ont accès aux renseignements personnels.

De plus, les secteurs de l'AE, des PSR et des SFA-SMCD procèdent à la mise en œuvre d'autres projets afin de garantir l'existence d'un rapport entre l'accès de l'utilisateur et le profil d'utilisateur. L'examen des profils d'utilisateurs se rapporte aux mesures prises à l'appui de la recommandation 10, laquelle concerne l'attribution, le maintien et l'élimination des codes d'accès.

Les responsables de l'AE, des PSR et des SSA ont pris les mesures suivantes :

- *On procède à l'élaboration des profils d'utilisateurs de l'AE afin de garantir que les utilisateurs ne pourront accéder qu'aux renseignements dont ils ont besoin dans l'exercice de leurs fonctions. La Direction générale de l'assurance procède à la rédaction d'un plan d'action et d'un énoncé de travail détaillé en vue d'analyser et d'examiner ces politiques et ces procédures.*
- *La Direction générale des PSR a examiné et mis à jour un système d'accès aux PSR, qui se fonde sur les profils d'utilisateurs. La Direction générale procédera également à*

l'examen et à la mise à jour de ces lignes directrices opérationnelles pour les demandes d'accès, y compris du guide et du formulaire de demande d'accès d'utilisateur des PSR utilisés par les gestionnaires.

- *Les responsables des SFA-SMCD examineront la grille de sécurité actuelle afin de garantir que les fonctions, les tâches et la matrice de sécurité connexe correspondent aux renseignements accessibles. Cette mesure exigera un examen des écrans associés aux éléments contenus dans la matrice de sécurité. Compte tenu des résultats de l'examen, on établira de nouvelles exigences opérationnelles, dans le but d'élaborer, s'il y a lieu, une nouvelle matrice de sécurité. De plus, à l'appui de la présente recommandation, on examinera les politiques et les procédures en place afin de relever des lacunes.*

2.1.4 Évaluation du risque et des contrôles

RHDCC/DSC et l'ARC ont conclu un protocole d'entente selon lequel chacune des organisations doit vérifier de façon régulière la gestion des renseignements personnels qu'elle a reçus de l'autre organisation. Il s'agit de la première vérification effectuée à RHDCC/DSC en vertu de cette entente.

Des évaluations du risque et des contrôles liés à la manipulation et à la protection des renseignements personnels ont été effectuées par l'AE et par les PSR à l'échelle nationale et régionale, et par les responsables de la PS avant la vérification.

Depuis que le Secrétariat du Conseil du Trésor a promulgué la nouvelle Politique sur l'évaluation des facteurs relatifs à la vie privée en mai 2002, les nouveaux systèmes, programmes et procédures doivent être examinés et leur incidence sur la collecte, l'utilisation et l'élimination des renseignements personnels évaluée. Cette politique favorisera la connaissance et la prise en charge des risques reliés aux renseignements personnels lors de l'adoption ou de la modification de systèmes, de procédures et de programmes.

2.2 Objectif 2 : La conservation, la protection et l'élimination des renseignements personnels respectent la politique du gouvernement en matière de sécurité

Critères de vérification

- Les renseignements personnels sont conservés et éliminés en conformité avec les politiques du gouvernement en matière de sécurité.
- Des contrôles internes sont en place pour garantir que les renseignements personnels sont protégés contre tout effacement, toute modification et toute destruction non autorisés.
- Les bases de données électroniques contenant des renseignements personnels sont protégées contre toute visualisation, reproduction et destruction non autorisées; les bandes magnétiques et les autres supports physiques contenant des renseignements personnels sont protégés, gardés en lieux sûrs, et seules les personnes autorisées y ont accès.

- Les renseignements personnels sont mis à jour rapidement lorsque requis et la source de l'information utilisée pour modifier ces renseignements est conservée au dossier.

2.2.1 Conservation et élimination

En vertu des exigences ou des politiques juridiques, on doit conserver au moins six ans les documents et les autres supports contenant des renseignements personnels, comme les dossiers des clients.

Dans les bureaux visités, les dossiers des clients étaient conservés sur les lieux pendant une période minimale d'un an suivant la dernière mesure administrative. Les dossiers étaient ensuite envoyés aux Archives nationales (AN) pour y être détruits sur approbation officielle du Ministère au terme de la période prévue.

Les dossiers inactifs étaient généralement conservés avec les dossiers actifs jusqu'à ce qu'ils soient prêts à être envoyés aux AN. Ils étaient emballés dans des boîtes juste avant leur expédition. Les AN prévoient le scellage des boîtes contenant les anciens dossiers des clients lorsque le bureau d'origine est situé à l'extérieur de la ville où se trouvent les AN. Lorsque le bureau et les AN sont dans la même ville, on se contente de plier le rabat supérieur des boîtes. Celles-ci sont cependant emballées ensemble avec une pellicule de plastique transparente. Pour avoir accès à un dossier, on doit retirer la pellicule (mais elle peut être remise en place par la suite).

Conformément aux procédures des AN, on doit écrire sur chaque boîte le numéro du premier et du dernier dossier qu'elle contient. Dans les bureaux visités, on utilisait le numéro d'assurance sociale (NAS) comme identificateur. Les responsables de trois régions visitées écrivaient le NAS complet des clients auxquels se rapportaient le premier et le dernier dossier contenus dans la boîte; quiconque voyait ou manipulait les boîtes pouvait donc prendre note de NAS valides et parfois non-utilisés. Dans l'une des régions, on n'inscrivait que les trois derniers chiffres. Les pratiques dans les deux autres régions n'ont pas été vérifiées.

RHDCC/DSC utilise plusieurs méthodes pour éliminer les renseignements personnels. Les bandes magnétiques et les disques contenant des renseignements personnels électroniques peuvent être effacés ou détruits. Les responsables de tous le bureaux visités ont déclaré utiliser des techniques sécuritaires d'élimination ou d'effacement. Cependant, les bandes magnétiques reçues de l'ARC ou d'autres ministères sont retournées dans des enveloppes sans être effacées ou détruites.

Le déchiquetage des documents contenant des renseignements personnels (imprimés d'ordinateurs, lettres, notes, etc.) est effectué sur place par des employés de RHDCC/DSC ou par un entrepreneur utilisant son propre équipement. On fait appel à des entreprises spécialisées pour déchiqueter les documents à l'extérieur.

RHDCC/DSC retient les services de différents transporteurs pour expédier à un autre endroit les documents contenant des renseignements personnels afin qu'ils soient archivés ou éliminés. Dans les villes où elles ont une succursale, les Archives nationales ramassent les documents et assument la responsabilité et la gestion des documents, une fois ceux-ci chargés dans son camion. Là où les AN ne sont pas présentes, RHDCC/DSC utilise des transporteurs cautionnés (bonded) pour expédier les documents, les notes et autre matériel de nature délicate. Dans l'un des bureaux visités, un employé de RHDCC/DSC était chargé d'accompagner l'expédition mais cette pratique n'a été signalée nulle part ailleurs.

Le vérificateurs ont obtenu et examiné trois exemplaires de contrats de transport et cinq exemplaires de contrats touchant le déchiquetage de documents ou de notes contenant des renseignements personnels. L'un des trois contrats de transport contenait une disposition générale sur la protection des renseignements personnels en transit ou sous la responsabilité du transporteur :

> L'entrepreneur devra respecter, pendant et après la durée du contrat, le caractère confidentiel de tout renseignement confidentiel touchant les affaires de l'État, et auquel ses employés ou ses représentants ont accès.

Trois des cinq contrats de déchiquetage contenaient une disposition très générale concernant la protection des renseignements personnels.

Sauf dans les cas ci-dessus, les responsables des bureaux visités n'étaient pas en mesure de produire des contrats officiels relatifs à l'expédition ou au déchiquetage des documents contenant des renseignements personnels. Certains bureaux ont pu produire des ententes d'offres à commande ou des bons de commande généraux concernant le transport, mais ceux-ci ne contenaient pas de dispositions liées à la protection des renseignements personnels.

Le groupe de protection de la vie privée a établi des dispositions générales sur la protection des renseignements personnels qui doivent être incluses dans les contrats de services entraînant une manipulation des renseignements personnels. Toutefois, aucun des contrats de ce type qui ont été examinés par les vérificateurs ne concernait le déchiquetage ou le transport des renseignements personnels.

Selon les Services juridiques, l'absence d'une disposition spécifique et exécutoire sur la protection des renseignements personnels dans un contrat d'expédition ou de déchiquetage pourrait rendre le Ministère vulnérable en cas de litige concernant l'utilisation ou la divulgation illicite.

Recommandation 6 : (RHDCC/DSC)

Toutes les situations où l'on fait appel à une société ouverte pour le transport ou l'élimination des documents contenant des renseignements personnels devraient faire l'objet d'un contrat établissant et précisant la responsabilité de l'entreprise relativement à la protection de la confidentialité des renseignements personnels qu'elle contrôle.

Seuls les trois derniers chiffres du numéro d'assurance sociale devraient être inscrits sur les boîtes expédiées aux Archives nationales.

Réponse de la direction :

La vérification a mis en lumière certaines incohérences dans les contrats de services visant l'expédition et l'élimination des documents contenant des renseignements personnels, et a montré qu'il fallait inclure des dispositions générales dans tous les contrats de ce type. La Direction de l'accès à l'information et de la protection des renseignements personnels (AAIPRP) de RHDCC/DSC œuvre à la mise au point de ces dispositions générales, conjointement avec les Services juridiques. Les responsables de la sécurité des SFA procéderont pour leur part à un examen des questions de sécurité relatives à ces contrats. La Gestion du matériel des SFA et Travaux publics et Services gouvernementaux Canada (TPSGC) procèderont à des échanges de vues dans le but de s'entendre sur la formulation des dispositions utilisées dans les contrats attribués au nom de RHDCC/DSC et d'influencer l'établissement des clauses générales de TPSGC pour les offres à commandes. De plus, on est en train de mettre en œuvre une stratégie et des procédures de communication afin d'enseigner l'application des dispositions appropriées aux agents d'approvisionnements et aux coordonnateurs de la protection des renseignements personnels des deux ministères.

Le rapport souligne qu'on ne devrait pas inscrire le numéro d'assurance sociale complet sur les boîtes expédiées ou entreposées à l'extérieur des installations de RHDCC/DSC. On a modifié les lignes directrices de gestion des dossiers, en précisant qu'on ne devrait jamais inscrire les NAS au complet sur les faces extérieures des boîtes, mais qu'on devrait plutôt indiquer uniquement les trois derniers chiffres des NAS utilisés pour répertorier les dossiers.

2.2.2 Accès aux systèmes

Tel que mentionné précédemment, il existe, dans toutes les régions, des renseignements personnels portant sur des millions de clients et conservés sous diverses formes (dossiers, papiers, documents, bandes magnétiques et disques). On trouve également des renseignements personnels dans différents systèmes auxquels des utilisateurs de tout le pays peuvent accéder par ordinateur.

RHDCC/DSC doit protéger la confidentialité et garantir l'utilisation légitime de ces renseignements. À titre de gardien des renseignements personnels, le Ministère doit également protéger les informations confidentielles contre la modification, l'effacement et l'élimination non autorisés ou inappropriés. Lorsqu'une modification légitime est requise, le Ministère doit s'assurer que celle-ci est effectuée dans les plus brefs délais et dûment enregistrée. Dans les systèmes informatiques, les mots de passe constituent les mécanismes de contrôle fondamentaux assurant la protection de l'accès aux renseignements personnels.

L'accès logique aux systèmes des PSR, de l'AE, de la PS et des FFA-MCD exige un mot de passe associé à un code d'accès. Le mot de passe est une combinaison de lettres et de chiffres que seul le propriétaire est censé connaître. Le code d'accès est un code attribué à une personne et constitué d'une série de caractères. Il n’est toutefois pas secret, et plusieurs personnes peuvent l'utiliser successivement (les codes d'accès inutilisés sont parfois recyclés).

Bien que le processus d'attribution des mots de passe soit d'abord et avant tout destiné à garantir la sécurité, il est traité dans le présent rapport puisque la sécurité est une condition préalable à la protection des renseignements personnels.

Lorsqu'un employé obtient un code d'accès pour la première fois, il reçoit un mot de passe temporaire qu'il ne peut utiliser qu'une seule fois pour accéder à l'écran de gestion des mots de passe. L'employé choisit un mot de passe personnel secret et l'enregistre dans le système. Au cours de ce processus, l'employé est généralement prévenu de ne dévoiler son mot de passe à personne ni de donner des indices qui pourraient permettre à quelqu'un d'autre de la découvrir ou de le deviner. Lorsque ces procédures et ces lignes directrices sont correctement suivies, l'employé est la seule personne à connaître le mot de passe secret associé à son code d'accès et est donc le seul à pouvoir accéder aux systèmes à l'aide de ce code.

De nombreux employés de RHDCC/DSC doivent mémoriser de multiples mots de passe pour accéder à différents systèmes et ce, sans compter les autres mots de passe qu'ils utilisent dans d'autres sphères de leur vie quotidienne. Bon nombre de ces mots de passe sont modifiés de façon périodique. Comme l'oubli d'un mot de passe entraîne des inconvénients et des retards, les employés peuvent être tentés d'écrire leur mot de passe sur un bout de papier et de le cacher quelque part dans leur lieu de travail. Il est alors risqué qu'une autre personne le découvre et l'utilise à des fins non justifiées.

Une agente de sécurité interrogée était consciente des risques encourus et avait trouvé une façon de renforcer la confidentialité des mots de passe. Elle demandait aux employés d'écrire leur mot de passe sur un bout de papier et de mettre ce morceau de papier dans une enveloppe cachetée. Puis, elle rangeait les enveloppes en lieu sûr. Si un employé oubliait son mot de passe, il pouvait aller chercher son enveloppe scellée au bureau de l'agente de sécurité, l'ouvrir, retrouver son mot de passe et répéter le processus. Il s'agit là d'une façon simple et efficace de réduire les risques de vol de mots de passe.

La réinitialisation ou la réactivation des mots de passe dans les systèmes informatiques centraux peut constituer une autre source de risques. Un mot de passe doit être réinitialisé ou réactivé lorsque l'employé l'a oublié (p. ex., après s'être absenté du travail) ou l'a entré incorrectement plusieurs fois de suite. Pour réinitialiser ou réactiver un mot de passe, il faut d'abord appeler l'un des Bureaux de service national. Au cours de leurs visites, les vérificateurs se sont fait dire que, dans certains cas, l'identité de l'appelant n'était pas certifiée et qu'aucun gestionnaire ne participait au processus. Si c'est le cas, le risque existe qu'une personne obtienne un nouveau mot de passe donnant accès à des renseignements personnels en se faisant passer pour une personne absente. L'équipe de la technologie de l'information (TI) des IAS se penche actuellement sur cette question en procédant à une vérification de sécurité de la TI, dans le but de confirmer l'existence et la nature du risque en question. Le cas échéant, on formulera des observations et des recommandations spécifiques à la fin de cet exercice.

2.2.3 Protection matérielle des dossiers

La protection matérielle et l'accès contrôlé sont les processus de base qui permettent de protéger les dossiers papiers contenant des renseignements personnels. On trouve de tels dossiers papiers à l'AE (RHDCC), aux PSR et aux SFA-SMCD (DSC).

Dans les bureaux des PSR (DSC) visités, les dossiers des clients étaient conservés dans des salles verrouillées. Dans trois régions, l'accès était réservé au personnel de gestion des dossiers, tandis qu'ailleurs, la plupart des employés pouvaient entrer dans ces salles. Les documents consultés étaient généralement laissés sur des bureaux et pouvaient être vus par toute personne qui se trouvait sur l'étage.

Dans deux bureaux visités des SFA-SMCD (DSC), on a déclaré que les dossiers actifs étaient conservés dans un classeur ou dans une salle qui n'étaient pas verrouillés la nuit.

À l'AE (RHDCC), les dossiers sont le plus souvent conservés sur des étagères ouvertes dans la zone de traitement des demandes, exception faite de l'un des bureaux, où les dossiers sont gardés dans une salle qui doit être verrouillée la nuit. On s'attend à ce que les employés qui prennent des dossiers enregistrent leur retrait à l'aide d'un système de dépistage des documents (SDD). Cependant, ce système n'est pas conçu pour empêcher le retrait non autorisé d'un dossier, du fait qu'il ne contient pas de mécanisme de contrôle permettant de garantir l'enregistrement de tout retrait de dossier.

Dans les bureaux qui fournissent un service en personne, la règle est que le public n'est pas autorisé à pénétrer dans les secteurs où sont détenus les dossiers, mais on note certaines exceptions. Les clients peuvent être invités à entrer pour une entrevue ou une enquête, et les fournisseurs de services ont accès aux lieux pour effectuer des réparations et des travaux d'entretien et les règles des établissements précisent que ces personnes doivent être accompagnées lorsqu'elles se trouvent dans les zones interdites au public. Les employés d'entretien peuvent généralement accéder sans escorte à la plupart des secteurs des établissements. Dans le cadre de la présente vérification, on n'a pu déterminer dans quelle mesure les mécanismes de limitation de l'accès étaient appliqués, et s'ils étaient appliqués de façon uniforme. Cependant, à l'occasion d'une autre vérification, les membres de l'équipe de vérification ont déclaré qu'ils étaient entrés dans une zone d'accès restreint et qu'ils y étaient restés plusieurs minutes avant d'être interpellés.

Les établissements visités pendant la vérification étaient aménagés de différentes façons et offraient une protection variable contre l'accès non autorisé aux documents contenant des renseignements personnels. Dans certains bureaux, une porte munie d'un verrou activé par un code électronique séparait les zones publiques des zones à accès restreint, tandis qu'ailleurs, on ne trouvait qu'une barrière. Dans l'une des régions, on n'a remarqué aucune séparation physique entre la zone publique et la zone d'accès restreint.

Dans trois des régions visitées où RHDCC/DSC partage des installations avec des partenaires, les employés ont précisé qu'il était difficile d'empêcher ces partenaires de voir des renseignements personnels détenus par le Ministère, et que ceci créait parfois des situations embarrassantes.

Recommandation 7 : (RHDCC/DSC)

Compte tenu du grand nombre de situations exigeant la protection de la confidentialité des dossiers des clients, on recommande à RHDCC et à DSC d'effectuer des évaluations individuelles des risques et des contrôles dans les locaux où sont conservés les documents contenant des renseignements personnels, afin de déterminer si le niveau de protection contre l'accès non autorisé aux dossiers des clients ou le retrait de ces dossiers est approprié.

Réponse de la direction :

Les agents de sécurité effectuent des évaluations des menaces et des risques (EMR) concernant les locaux du Ministère et examinent notamment la protection matérielle des dossiers des clients. De plus, la Sécurité des SFA recommencera à vérifier régulièrement les installations de l'AC afin d'évaluer leur conformité avec les politiques et les procédures de protection et de transmission des renseignements désignés et classifiés. Des séances régulières de formation et de sensibilisation à la sécurité sont également offertes aux employés.

2.2.4 Modification et mise à jour

Trois motifs justifient la modification ou la mise à jour des renseignements personnels concernant un client à l'AE (RHDCC), aux PSR et aux SFA-SMCD (DSC) :

- De nouvelles données ont été reçues conformément à une entente, par exemple un PE avec l'ARC.
- L'agent recueille de nouveaux renseignements au cours d'une enquête.
- Un client ou son représentant présente une demande de mise à jour ou de modification d'un dossier.

Dans les deux premiers cas, la modification est effectuée immédiatement et le client n'est pas nécessairement informé des changements, sauf si ceux-ci ont une incidence sur son admissibilité aux prestations.

Dans le troisième cas, la demande de changements formulée par le client ou par son représentant peut être reçue en personne, par téléphone ou par écrit. Si c'est en personne, généralement dans un Centre des ressources humaines du Canada — CRHC), les employés déclarent qu'ils vérifient l'identité des demandeurs en leur posant des questions appropriées et (ou) en leur demandant une pièce d'identité.

De façon générale, ce sont les télécentres qui reçoivent les demandes téléphoniques. Les employés ont précisé qu'ils demandaient aux appelants de fournir des renseignements personnels comme le NAS, la date de naissance, le nom de jeune fille de la mère ou, pour l'AE, l'indicatif d'accès téléphonique (IAT). Si l'employé doute de l'identité du client, il peut lui demander des renseignements supplémentaires normalement connus de lui seul, comme le taux des prestations, la date de la demande, le type de prestations et l'état de la demande.

S'il doute toujours de l'identité de l'appelant, l'employé peut renvoyer le cas à un agent d'un centre de traitement ou d'un CRHC.

Les demandes présentées par écrit sont envoyées dans des centres de traitement. Les employés de ces centres ont déclaré qu'ils appariaient les renseignements contenus dans la demande et les données incluses dans les systèmes ou dans les dossiers du client, y compris la signature, si elle est disponible.

Lorsque la demande de changement est formulée par un représentant du client, les employés doivent demander qu'on leur remette une délégation de pouvoir écrite ou une autorisation de divulgation signée par le client.

Dans la plupart des cas, une fois l'identité du client attestée, le changement demandé est effectué immédiatement, sans être contesté ni faire l'objet de vérifications supplémentaires, à plus forte raison s'il s'agit d'une demande de changement d'adresse, la demande la plus fréquente.

Les politiques des PSR visant la modification des renseignements personnels prévoient qu'on doit inclure au dossier des preuves à l'appui des mesures prises, afin de justifier les changements apportés aux documents du client. Par exemple, les employés devraient conserver au dossier une lettre ou les notes relatives à un appel téléphonique du client ou de son représentant, de même que tout document justificatif. Dans cinq des six bureaux de PSR (DSC) et dans quatre des cinq bureaux des SFA-SMCD (DSC), les employés ont déclaré qu'ils étayaient les motifs des changements dans les dossiers des clients et qu'ils conservaient au dossier un exemplaire de tout document pertinent.

À l'AE (RHDCC), les vérificateurs n'ont trouvé aucune politique ou procédure concernant la documentation des changements dans les dossiers des clients, et les pratiques d'enregistrement déclarées variaient. Dans certaines régions, les agents reçoivent la consigne d'étayer le motif des changements et de conserver au dossier les documents de preuve fournis par le client ou un exemplaire de ces documents. Ailleurs, on laisse le soin aux employés de traiter les demandes selon leur jugement, en leur rappelant l'objectif de réduire la quantité de documents papiers.

Dans certains cas, le manque de documentation à l'appui d'un changement apporté au dossier d'un client peut présenter un risque. Il est possible que le changement effectué soit injustifié ou inexact, que la demande de changement ait été présentée par une personne autre que le client ou son représentant autorisé, ou qu'une erreur factuelle se soit glissée comme cela peut se produire dans tout processus de modification. Si ce genre de situations venait à entraîner des difficultés ou affecte l'intégrité du programme, il serait difficile, en l'absence de documents, de retracer les origines du changement.

Tous les employés ont déclaré que les demandes de modification des renseignements personnels étaient presque toujours traitées immédiatement. Dans les télécentres, la plupart des modifications sont apportées au moment même de l'appel. Les demandes de changement que les employés des télécentres ne sont pas en mesure ou n'ont pas le droit de traiter sont transmises à un CRHC par courrier électronique. Dans les bureaux, le délai

de traitement des modifications peut varier, mais le processus est normalement exécuté en moins de 48 heures.

Recommandation 8 : (RHDCC)

On devrait clarifier les règles et les procédures touchant l'enregistrement des sources et des motifs des changements apportés aux renseignements personnels, de même que la conservation des documents de preuve, afin de réduire les risques de modifications inappropriées, qui pourraient entraîner des préjudices.

Réponse de la direction :

Bien que le rapport de vérification souligne que les demandes de modification des renseignements personnels contenues dans les dossiers des clients sont traitées de façon opportune, il précise du même coup que les procédures liées à ces modifications varient d'un programme à l'autre. En ce qui concerne l'AE, on établira une directive nationale afin de clarifier les politiques et les procédures touchant la documentation des sources et des motifs de changement. Les responsables des PSR continueront à veiller à ce que leurs politiques et leurs procédures de modification des renseignements personnels demeurent conformes aux observations de la vérification.

2.3 Objectif 3 : Les renseignements personnels d'une personne sont accessibles seulement aux personnes autorisées et sont utilisés dans le but pour lequel ils ont été recueillis.

Critères de vérification

Des contrôles internes adéquats et efficaces sont en place afin de fournir l'assurance que :

- les demandes d'accès ou de modification de l'accès aux renseignements personnels proviennent d'une personne autorisée;
- le niveau d'accès demandé correspond au poste et aux fonctions actuels de la personne pour qui l'accès est demandé;
- le profil d'accès d'un employé dont le statut, le poste ou la fonction a changé est modifié, suspendu ou supprimé, si nécessaire;
- l'utilisation des renseignements personnels est directement liée à une activité ou à un programme opérationnel et est en accord avec le but pour lequel les renseignements ont été obtenus ou compilés;
- la visualisation des renseignements personnels est surveillée régulièrement à l'aide de pistes de vérification ou d'autres moyens de contrôle appropriés pour détecter tout accès non autorisé ou injustifié;
- l'anonymat des renseignements personnels utilisés pour l'analyse de politiques, la recherche et l'évaluation est préservé avant l'utilisation ou la divulgation, à moins qu'il n'y ait dispense;

- les renseignements personnels utilisés à des fins administratives ou de gestion de programme dont l'anonymat n'est pas préservé sont protégés contre toute utilisation ou tout accès non autorisé;
- la comparaison de données et le couplage des dossiers correspondent au but pour lequel les renseignements ont été obtenus ou compilés;
- les comparaisons de données à des fins administratives et le couplage de dossiers à des fins non administratives et de recherche nécessitant l'utilisation de renseignements personnels respectent les exigences des politiques applicables — la politique du Conseil du Trésor sur la comparaison des données et les politiques de RHDCC/DSC sur le couplage de dossiers;
- les documents contenant des renseignements personnels portent la mention « Protégé » et sont manipulés conformément à la législation relative à la protection des renseignements personnels, la politique gouvernementale en matière de sécurité et d'autres lois, règlements et politiques applicables;
- des procédures existent pour traiter les cas de violation de la sécurité ou de divulgation de renseignements personnels par erreur.

2.3.1 Attribution, maintenance et élimination des codes d'accès

RHDCC/DSC détient des renseignements personnels au sujet de ses clients et d'autres personnes sous différents formats (dossiers papiers, bandes et disques), mais la plupart du temps dans les différents systèmes conçus pour soutenir les programmes et les activités des PSR, de l'AE et des SFA-SMCD. La protection des dossiers papiers a été abordée à la section 3.2.3 du rapport. La présente section porte sur l'accès aux renseignements enregistrés dans les systèmes et leur utilisation.

Les mots de passe et les codes d'accès ont été définis dans la section 3.2.2 du rapport, et la nécessité de protéger la confidentialité des mots de passe y a été précisée. Dans la section 3.1.3, on a examiné le principe du « besoin de savoir ». Le profil associé au code d'accès constitue un autre concept clé du mécanisme de contrôle de l'accès aux renseignements personnels. Le profil est un ensemble d'instructions électroniques liées à un code d'accès qui permettent d'accéder aux écrans et des programmes requis pour l'exécution de tâches comme le calcul ou l'établissement d'une période de prestations d'AE. Les vérificateurs estiment que l'établissement de profils associé aux codes d'accès constitue d'abord et avant tout un mécanisme de contrôle de sécurité puisqu'il sert à établir la répartition des tâches et à limiter l'accès à certaines fonctions, mais qu'il constitue également un mécanisme de contrôle de la protection des renseignements personnels puisqu'il détermine le type de renseignements auxquels un employé peut avoir accès.

Le principe du « besoin de savoir » exige que le profil ne permette aux employés que d'accéder aux renseignements personnels dont ils ont besoin pour remplir leurs fonctions présentes légitimes. Par conséquent, le profil doit être correctement établi au départ, puis rajusté lorsqu'un changement apporté au statut ou à la fonction de l'employé modifie ces exigences.

Du point de vue de la protection des renseignements personnels, l'établissement de profils appropriés implique le recensement des écrans contenant des renseignements personnels pour chaque système et programme et la détermination des écrans auxquels un employé doit accéder pour exécuter ses fonctions. La question de l'accès légitime au dossier d'un client déterminé a été examinée dans la section 3.1.3.

Les paragraphes suivants présentent un aperçu du processus d'établissement de profil, d'attribution et de conservation des codes d'accès. La description détaillée de ce processus complexe dépasse la portée de la présente vérification. Aussi, seuls les aspects touchant directement la protection des renseignements personnels y seront traités.

À l'AE (RHDCC) et aux SFA-SMCD (DSC), au moins trois personnes sont impliquées dans le traitement des demandes de codes d'accès : l'employé, un superviseur ou un gestionnaire et un agent de sécurité de la technologie de l'information (TI) d'un des quatre Centres des technologies de l'information (CTI). Dans un bureau, seule une personne désignée/agent local de sécurité a le droit de transmettre la demande au CTI. Cette personne peut être le gestionnaire ou le superviseur de l'employé, un membre du personnel administratif ou un spécialiste du soutien micro-informatique (SFM).

Pour les PSR (DSC), en plus des trois parties susmentionnées, un agent responsable de la sécurité des accès (ARSA), intervient dans le traitement de la demande puisqu'il est le seul employé autorisé à la transmettre au CTI.

Les gestionnaires, les personnes désignées, les agents de sécurité sur place et les ARSA des PSR, de l'AE et des SFA-SMCD ont déclaré aux vérificateurs qu'ils suivaient la procédure et utilisaient les formulaires électroniques pour demander à un CTI de modifier ou d'annuler une permission d'accès, sauf lorsque les demandes étaient transmises à un CTI particulier, qui acceptait les demandes préventives sous d'autres formes.

Du côté de la PS, l'employé, son gestionnaire ou son superviseur, un agent de sécurité des systèmes très secrets d'élaboration des données, de même qu'un agent ministériel de la sécurité des Systèmes à l'AC prennent part au processus. Lorsque le secteur de programme désire accéder à des renseignements personnels détenus par Élaboration des données, l'agent de sécurité des SPF d'Élaboration des données agit à titre d'intermédiaire autorisé de la PS entre les programmes et les systèmes. La PS stocke les données dans l'ordinateur central des Services gouvernementaux de télécommunications et d'informatique (SGTI) et doit obtenir l'approbation du SMA pour accéder à cet ordinateur.

On a interrogé des représentants de l'AE, des PSR et des SFA-SMCD pour évaluer dans quelle mesure chacun d'entre eux connaissait l'ampleur de ses responsabilités et les responsabilités des autres participants au processus. La majorité des superviseurs et des gestionnaires comprenaient qu'ils étaient ultimement responsables du niveau d'accès accordé à leurs employés. Ils ont précisé qu'ils disposaient de documents de référence généraux concernant l'accès aux systèmes accordé aux titulaires de différents postes, mais que ces documents ne mentionnaient pas le niveau d'accès approprié qu'on devait accorder aux employés pour respecter les exigences en matière de protection des renseignements personnels. Tel que précisé dans la section 3.1.3, peu de gestionnaires et de superviseurs connaissent la nature et la quantité exactes des renseignements

personnels auxquels leurs employés ont accès. La plupart d'entre eux se fiaient sur la personne désignée ou sur l'agent de sécurité de la TI du CTI pour déterminer et attribuer le niveau d'accès approprié. Dans les bureaux visités, les nouvelles demandes d'accès étaient généralement des copies de la plus récente demande établie à l'intention d'un employé exécutant des tâches semblables (une pratique désignée sous le nom de « clonage »).

Dans les CTI, les agents de sécurité de la TI connaissaient les profils habituellement associés aux différentes fonctions, mais ignoraient le type précis de renseignements (personnels ou non) auxquels un utilisateur pouvait accéder avec un profil déterminé. Lorsque le profil demandé semblait inhabituel, les agents de sécurité de la TI pouvaient communiquer avec le demandeur pour effectuer une vérification mais en fin de compte, ils fournissaient le profil demandé en s'attendant à ce que le demandeur respecte les procédures applicables.

Recommandation 9 : (RHDCC/DSC)

On devrait définir clairement et mettre en pratique les responsabilités et les obligations redditionnelles de tout participant au processus de gestion de tous les codes d'accès et les profils qui permettent d'accéder à des renseignements personnels.

On devrait fournir de la documentation sur la nature des renseignements personnels auxquels les employés ont accès.

Réponse de la direction :

Dans cette recommandation, le rapport de vérification cerne la fonction des profils d'utilisateur dans l'attribution des codes d'accès. En se référant à la réponse fournie par la direction à la recommandation 5, les directions générales de l'AE, des PSR et des SFA-SMCD ont pris les mesures suivantes :

- *En plus des travaux d'amélioration des profils d'utilisateurs qui permettront de garantir que les utilisateurs n'ont accès qu'aux renseignements dont ils ont besoin pour remplir leurs fonctions, la Direction générale de l'assurance analyse et examine, conjointement avec la Direction générale des systèmes, les procédures et les politiques visant le renforcement des processus de création, de modification et d'effacement des codes d'accès.*
- *Les PSR procéderont à l'examen approfondi de tous les profils d'utilisateur.*
- *Les responsables du SFA-SMCD afficheront sur leur site intranet un document définissant clairement les rôles des personnes préposées à l'établissement d'un code d'accès pour le SMCD.*

Les gestionnaires et les employés interrogés à l'AE, aux PSR et aux SFA-SMCD étaient d'avis que les employés détenaient un niveau d'accès correspondant à leur poste et (ou) à leur statut, et que tous les niveaux d'accès étaient modifiés ou annulés au besoin. Un test partiel mené pendant la vérification a montré que le statut des employés n'était pas toujours tenu à jour. Un test approfondi est prévu pour déterminer l'ampleur du problème (voir la section 3.3.2 ci-dessous).

L'AE (RHDCC), les PSR et les SFA-SMCD (DSC) ont amorcé un examen approfondi de tous les profils d'accès afin de garantir que les membres de tous les groupes et que les titulaires de toutes les fonctions obtiennent un accès approprié aux renseignements personnels, conformément au principe du « besoin de savoir ». Au moment de la rédaction du présent rapport, aucun de ces secteurs n'avait terminé l'exercice.

Dans le cas de la PS, les permissions d'accès sont accordées pour une période limitée prédéterminée.

Recommandation 10 : (RHDCC/DSC)

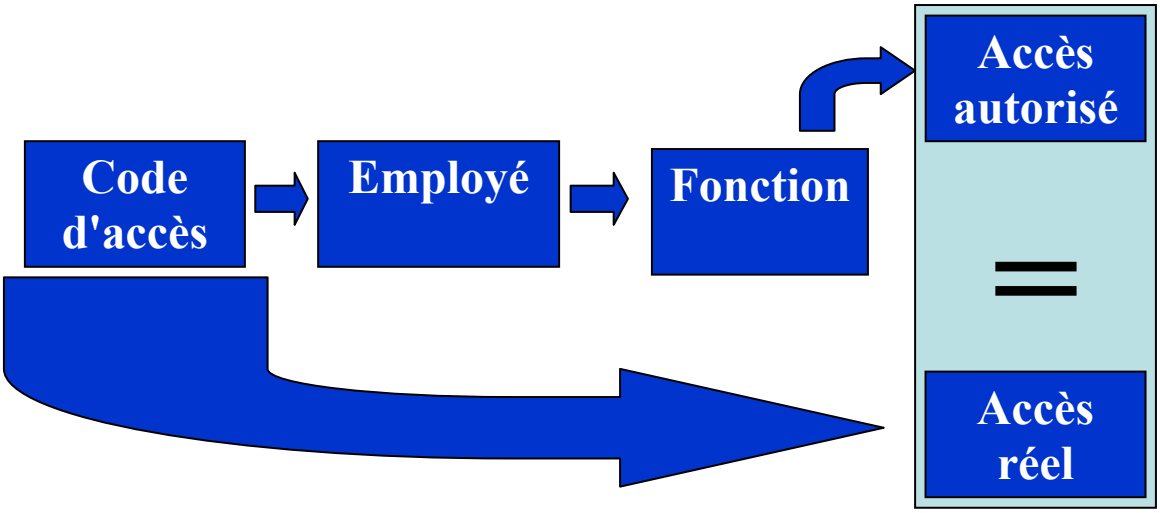
On devrait définir, comprendre et reconnaître les responsabilités et les obligations redditionnelles liées à l'attribution des codes d'accès et respectant les exigences en matière de protection des renseignements personnels.

Réponse de la direction :

La vérification a montré qu'un examen approfondi des profils d'utilisateurs permettrait de garantir la délivrance et la conservation appropriées des codes d'accès. À ce propos, la Direction générale des systèmes, avec l'aide de la Sécurité des SFA et de la Direction générale des ressources humaines, procède à l'examen des procédures et des documents existants concernant tous les aspects de la délivrance et de la conservation des codes d'accès afin de garantir leur conformité avec la Loi sur la protection des renseignements personnels, les politiques du Ministère et du Conseil du Trésor, et les pratiques exemplaires de l'industrie. Cette procédure permettra de soutenir d'autres recommandations formulées dans le rapport de vérification en vue de renforcer l'accès aux systèmes selon le principe du besoin de savoir et en relation avec les profils d'utilisateur. On a également inclus les responsabilités relatives aux profils d'utilisateurs et aux codes d'accès dans les responsabilités ministérielles en matière de protection des renseignements personnels et de sécurité, lesquelles ont été approuvées par le Comité directeur du cadre de gestion de la protection des renseignements personnels.

2.3.2 Test

À l'origine, l'équipe de vérification avait prévu réaliser un test afin de donner l'assurance que le niveau d'accès aux systèmes d'AE, des PSR et des SFA-SMCD correspondait au principe du « besoin de savoir » lié à la protection des renseignements personnels. On n'a pas inclus la PS dans ce test, du fait que ses responsables n'ont pas accès à l'ordinateur central et que leurs activités diffèrent de celles des autres programmes sélectionnés. Le concept et la méthodologie qui sous-tendent ce projet de test sont illustrés et décrits ci-dessous :



1. Un échantillon aléatoire et représentatif est créé à partir de l'ensemble des codes d'accès actifs qui permettent d'accéder aux programmes de l'AE, des PSR et des SFA-SMCD contenant des renseignements personnels.
2. On détermine le bon titulaire (le titulaire légitime) du code d'accès.
3. La fonction exercée par le titulaire pour une période donnée est déterminée.
4. On compare l'accès réel (fourni par le profil du code d'accès) à l'accès autorisé pour ce poste et pour cette période conformément au principe de la protection des renseignements personnels.
5. Si les deux niveaux d'accès concordent, alors le principe du « besoin de savoir » est respecté.

Dès les premières phases du test, on a relevé plusieurs difficultés liées à :

- l'établissement et l'obtention d'une liste attestée de tous les codes d'accès qui permettent d'accéder aux programmes et aux bases de données de l'AE, des PSR et des SFA-SMCD contenant des renseignements personnels;
- l'identification précise des titulaires d'un code d'accès, lorsqu'on trouve deux homonymes ou plus (de façon générale, on n'utilise pas l'identificateur unique des employés de RHDCC/DSC, le CIDP, pour les codes d'accès);
- la détermination de la fonction exercée par certains des titulaires du code d'accès pour la période de référence. La terminologie utilisée pour décrire la fonction n'est pas

uniforme et les vérificateurs ont recensé plus de 100 titres de postes, alors qu'il existe beaucoup moins de fonctions distinctes dans le secteur examiné;

- l'obtention de grilles reliant les fonctions et les niveaux d'accès en conformité au principe du « besoin de savoir ».

Après quelques semaines, on a constaté que la réalisation du test aurait exigé l'utilisation d'une quantité excessive de ressources et que, même si on réussissait à mener à bien le projet, l'exactitude des résultats ne pourrait être garantie. Il a donc été décidé de reporter le test jusqu'à ce que les Services de vérification interne soient en mesure de le réaliser de façon efficace et efficiente et de produire des résultats exacts et complets. La réalisation de ces conditions permettra en outre à l'AE, aux PSR et aux SFA-SMCD d'effectuer leur propre surveillance des niveaux d'accès par la suite.

Recommandation 11 : (RHDCC/DSC)

Pour permettre aux gestionnaires de surveiller de façon efficace et efficiente l'accès aux renseignements personnels, et pour faciliter l'administration de vérifications périodiques, on devrait prendre les mesures suivantes dès que possible :

1. *Établir une liste de tous les codes d'accès qui permettent d'accéder aux programmes et aux bases de données de l'AE, des PSR ou des SFA (SMCD) contenant des renseignements personnels, certifiée par le niveau décisionnel approprié (qui sera précisé dans le cadre de responsabilisation en matière des renseignements personnels en cours d'élaboration).*
2. *Établir un processus pratique pour déterminer avec certitude l'identité du titulaire de chaque code d'accès énuméré en (1).*
3. *Établir un processus pratique pour déterminer avec certitude la fonction exercée par chaque titulaire recensé en (2).*
4. *Établir des grilles reliant chaque fonction relevée en (3) avec un profil d'accès qui respecte les exigences en matière de protection des renseignements personnels.*

Réponse de la direction :

La direction souscrit à la recommandation concernant la surveillance de l'accès aux renseignements personnels et a pris des mesures en ce sens. La Direction générale des systèmes établira une liste de tous les codes d'accès, y compris ceux qui permettent l'accès à l'AE ou au SMCD, afin de vérifier les travaux de gestionnaire de CR, et mettra en œuvre, conjointement avec la Sécurité des SFA, des processus concrets afin de déterminer l'identité de tous les titulaires de codes d'accès. À des fins de vérification, la Direction générale des systèmes précisera aux gestionnaires les capacités d'accès des utilisateurs qui relèvent de leur autorité. Les directions générales sont chargées d'approuver et de limiter les renseignements qui peuvent être consultés ou modifiés dans leur secteur. Tel que mentionné dans la réponse de la direction concernant l'examen des profils d'utilisateurs dans la recommandation 9, les directions générales de l'AE, des PSR et des SFA-SMCD examineront leurs profils d'utilisateurs et détermineront le profil de chacun des utilisateurs. Puis, la Direction générale des systèmes effectuera le

rapprochement entre ces renseignements et le code d'accès approprié dans le cadre de la Procédure d'entrée unique et de l'administration de la sécurité.

En ce qui concerne le SMCD, on a déjà établi la liste de tous les utilisateurs qui peuvent accéder à la base de données, et un code d'accès ne peut être attribué que lorsqu'un CIPD y a été associé. De plus, la fonction remplie par chaque utilisateur du SMCD est indiquée dans le profil d'utilisateur, et on a élaboré une matrice de sécurité afin de mettre les fonctions et les tâches en rapport avec les permissions d'accès.

2.3.3 Utilisation et visualisation

Tous les gestionnaires et les employés interrogés ont convenu que l'accès aux renseignements personnels devait être limité, et que ces renseignements ne devaient être consultés que pour les besoins de l'exécution des programmes et des services de RHDCC/DSC.

Des politiques et des procédures de règlement des conflits d'intérêts sont en place. Les gestionnaires et les employés ont précisé qu'il fallait éviter toute situation éventuelle de conflit d'intérêts. Les dossiers des membres de la famille ou des amis doivent être traités par d'autres employés, dans un autre bureau si nécessaire, et doivent être conservés dans des classeurs verrouillés auxquels les employés ont un accès limité.

Les employés ont également mentionné leur devoir de ne pas divulguer des renseignements personnels à des personnes non autorisées. Les politiques et les procédures spécifiques existantes touchant la divulgation des renseignements personnels sont examinées un peu plus loin.

Dans la section 3.1.3, on a défini le principe du « besoin de savoir » relatif à la protection des renseignements personnels et la violation de ce principe, appelée « furetage ». Selon les vérificateurs, la procédure la plus efficace pour détecter et prévenir le furetage consiste à surveiller l'accès aux renseignements personnels au moyen d'une piste de vérification semblable à celle décrite ci-dessous.

2.3.4 Protégé

PROTÉGÉ

PROTÉGÉ

Recommandation 12 : (RHDCC/DSC)

PROTÉGÉ

Réponse de la direction :

PROTÉGÉ

PROTÉGÉ

2.3.5 Préservation de l'anonymat des renseignements personnels

Afin de garantir que l'accès respecte le principe du besoin de savoir, la PS (principale utilisatrice de données pour des activités d'analyse des politiques, de recherche et d'évaluation) a élaboré un protocole pour la manipulation et l'utilisation des bases de données contenant des renseignements personnels.

À la PS, seulement six responsables de l'Exploitation des données (cinq programmeurs et un adjoint administratif) peuvent accéder aux dossiers et voir les renseignements personnels avant l'anonymisation (masquage) des données. Chacun d'entre eux a accès au projet qui lui a été attribué.

Lorsque la PF reçoit des dossiers d'autres ministères comme l'ARC, le programmeur entre les données dans les systèmes et les rend anonymes par le masquage, le cryptage ou le remplacement. Chaque banque de données est masquée d'une façon différente, de sorte qu'il n'est pas possible d'établir un lien entre les dossiers et l'identité d'une personne. Les données anonymes peuvent être utilisées dans le cadre d'enquête, de recherche ou d'analyses. Les demandes d'accès doivent être présentées de façon individuelle, pour chaque employé et chaque projet. Les documents d'origine sont retournés aux expéditeurs, et les renseignements qui n'ont pas été anonymisés ne sont pas conservés à la Direction générale de l'exploitation des données.

2.3.6 Couplage de données et de dossiers

Tous les couplages identifiés des données et des dossiers sont effectués à l'administration centrale. Ces couplages, réalisés essentiellement pour Enquêtes et contrôle et pour les activités de la PS, doivent être clairement autorisés et faire l'objet d'une entente spécifique.

Selon la politique du SCT, on doit consulter le Commissariat à la protection de la vie privée (CPVP) lorsque de nouveaux couplages sont demandés à l'AE et aux PSR, et seul le directeur de l'accès à l'information et de la protection des renseignements personnels est habilité à approuver un couplage de données. Dans la plupart des cas, on effectue un couplage entre les données financières reçues de l'ARC et les données du programme recueillies par RHDCC/DSC. En général, les activités des couplages des données sont récurrentes et automatisées. La plupart des couplages de données sont effectués de façon systématique, surtout à des fins d'enquête et de contrôle.

À la PS, les couplages de dossiers à des fins de recherche ne constituent pas une procédure courante. Chaque couplage doit être examiné par le CRD et le CPVP, et approuvé par le sous-ministre (SM).

2.3.7 Étiquetage des renseignements personnels

Un Guide de classification de l'information publié par la Direction générale de la sécurité, des enquêtes et des mesures d'urgence a été distribué à tous les employés de RHDCC/DSC en 2002. Ce guide fournit des définitions et des directives concernant le niveau de protection, de même les garanties et les procédures à suivre en rapport avec différents types de documents contenant des renseignements personnels.

Nous avons constaté que les participants interprétaient le Guide de différentes manières. Par exemple, le Guide fournit des définitions générales concernant le niveau de protection « A » et « B », mais, bien souvent, il s'agit d'une question de jugement. Nous avons également remarqué que les directives du Guide n'étaient pas appliquées de façon uniforme. On a notamment précisé que, dans certains bureaux, le personnel utilisait un télécopieur non protégé pour transmettre des renseignements relatifs aux clients. Ailleurs, les responsables transmettaient les renseignements liés aux clients par télécopieur, mais ils ne pouvaient pas confirmer que celui-ci était protégé. Cette pratique ne permet pas d'assurer la protection des renseignements personnels, dans le cas où les documents sont envoyés au mauvais endroit. On a déclaré que les CRHC transmettaient des renseignements protégés aux clients et des décisions relatives à une assurabilité à l'ARC en les insérant dans une seule enveloppe.

Les dossiers de clients sont régulièrement transférés d'un centre de traitement à un autre. On a précisé que les dossiers expédiés étaient insérés dans deux enveloppes.

Au cours d'une évaluation préliminaire, les participants ont déclaré aux vérificateurs que l'insertion des documents protégés dans deux enveloppes était considérée comme une « pratique exemplaire », mais qu'il ne s'agissait pas d'une procédure obligatoire.

La PS a établi des directives pour la protection des renseignements personnels qu'elle utilise dans le cadre d'activités d'analyse de politiques, de recherche et d'évaluation. Ces directives ont été communiquées au personnel et examinées au cours de séances

d'information. À la PS, les CD portent la mention « Protégé B », et les renseignements envoyés à l'extérieur de RHDCC/DSC sont étiquetés « Protégé » au niveau approprié.

Recommandation 13 : (RHDCC/DSC)

On devrait compléter le Guide de classification de l'information par un ensemble de directives pratiques pour la classification et la manipulation des principaux documents contenant des renseignements personnels utilisés par les responsables des différents programmes.

On devrait mettre en place des mécanismes de contrôle interne afin de garantir que les documents protégés sont désignés comme tels et manipulés selon le niveau de protection qu'on leur a attribué.

Réponse de la direction :

Le rapport de vérification souligne que le Guide de classification de l'information publié par la Sécurité n'était pas toujours bien compris. À l'AC, la Sécurité des SFA a amorcé l'élaboration de lignes directrices afin d'expliquer clairement toutes les facettes de la manipulation, de la sauvegarde, de la transmission et de l'élimination des renseignements personnels et autres renseignements sensibles. De plus, la sécurité des SFA recommencera à vérifier régulièrement les installations de l'AC afin d'évaluer leur conformité avec les politiques et les procédures de protection et de transmission des renseignements désignés et classifiés. Des séances régulières de formation et de sensibilisation à la sécurité sont également offertes aux employés.

2.3.8 Règlement des violations

Les gestionnaires régionaux et locaux ont précisé qu'ils étaient prêts à signaler toute violation de la sécurité ou divulgation de renseignements personnels par erreur à la Direction générale de la sécurité ou des ressources humaines, selon le cas. À l'AC, les gestionnaires ont mentionné que la procédure à suivre pour régler ce genre de problèmes n'était pas claire pour eux.

Recommandation 14 : (RHDCC/DSC)

On devrait préciser et communiquer la procédure que le gestionnaire et les employés doivent suivre lorsqu'ils prennent connaissance d'une violation possible de la protection des renseignements personnels.

Réponse de la direction :

Les lignes directrices ministérielles pour la conduite d'enquêtes administratives, qui ont été révisées récemment, clarifient la politique et les procédures que les employés et les gestionnaires doivent suivre pour signaler des cas présumés de violations de la protection des renseignements personnels ou d'autres délits administratifs ou criminels. Ces lignes directrices ont été transmises aux bureaux régionaux et sont affichées sur l'intranet.

2.4 Objectif 4 : Les renseignements personnels sont divulgués dans le respect de la Loi sur la protection des renseignements personnels et autres lois, règlements, politiques et ententes applicables.

Critères de vérification

- L'autorisation de divulguer les renseignements personnels est clairement établie et documentée, le processus de divulgation respecte les politiques et procédures applicables, et la nature et la quantité de renseignements personnels divulgués n'excèdent pas l'objectif de la divulgation.

2.4.1 Divulgation des renseignements personnels[3]

L'autorisation de divulguer, ou de ne pas divulguer, des renseignements personnels aux clients est précisée dans la législation et dans les règlements des programmes de RHDCC/DSC, de même que dans les protocoles d'entente lorsque les renseignements sont reçus d'un tiers.

Les demandes d'accès aux renseignements personnels sont considérées comme étant formelles ou informelles. Une demande formelle est une demande reçue par écrit et fondée sur la *Loi sur la protection des renseignements personnels* ou une demande qu'on a présentée en utilisant le formulaire officiel d'Info Source. On doit répondre aux demandes formelles dans un délai de 30 jours. La réponse doit préciser le droit du client de porter plainte et de demander la correction des renseignements détenus par RHDCC/DSC.

Le coordonnateur local de la protection des renseignements personnels traite les demandes formelles de divulgation. Le Ministère se réserve le droit, dans des circonstances particulières, de ne pas divulguer certains renseignements personnels. Cette procédure porte le nom d'exemption. Les exemptions concernent notamment les renseignements reçus au cours d'enquêtes ou d'application de la loi, ceux concernant une autre personne, les dossiers médicaux et les renseignements qui pourraient compromettre la sécurité de certaines personnes. En ce qui concerne l'AE (RHDCC), l'AC a déclaré que tous les coordonnateurs régionaux de la protection des renseignements personnels étaient autorisés à gérer les exemptions, mais a précisé que certains d'entre eux ne désiraient pas se voir confier une telle responsabilité. Deux coordonnateurs régionaux interrogés par les vérificateurs ont mentionné qu'ils n'étaient pas autorisés à traiter les exemptions. Dans les cas des PSR (DSC), toutes les exemptions doivent être gérées à l'AC, sauf si ce pouvoir a été délégué au coordonnateur local ou régional de la protection des renseignements personnels.

L'examen a montré que les bureaux régionaux et les coordonnateurs régionaux de la protection des renseignements personnels respectaient les procédures à suivre pour répondre aux demandes formelles de divulgation. Seuls les renseignements demandés

[3] La présente section porte sur la divulgation, par RHDCC/DSC, de renseignements personnels à des personnes. La divulgation de renseignements personnels à d'autres organisations, ministères ou ordres de gouvernement fera l'objet de vérifications futures.

étaient divulgués. Dans cinq des six régions, la lettre transmise mentionnait le droit du client de porter plainte et de demander des corrections.

Une demande informelle est une demande formulée verbalement ou par écrit, mais qui ne fait pas référence à la *Loi sur la protection des renseignements personnels*, ou une demande qui n'a pas été présentée sur le formulaire officiel d'Info Source. Il est à noter que la nature des renseignements à divulguer n'est pas prise en considération, malgré le fait que ces renseignements peuvent être aussi sensibles, selon plus, que les renseignements divulgués à la suite d'une demande formelle. À l'échelle locale, les demandes informelles sont traitées par n'importe quel membre du personnel ou parfois par le coordonnateur de la protection des renseignements personnels.

Les demandes informelles verbales concernant la divulgation ne sont pas documentées. Les entrevues ont montré que les procédures de documentation des demandes informelles écrites variaient entre les différents programmes et bureaux. Or, la divulgation inopportune de renseignements personnels pouvait entraîner les mêmes conséquences négatives que la modification inappropriée des renseignements personnels, sujet abordé plus haut. Par conséquent, les demandes de divulgation devraient elles aussi être documentées dans certains cas.

Les employés interrogés reconnaissaient qu'ils étaient responsables de ne pas divulguer de renseignements personnels à des personnes non autorisées. Un processus d'identification semblable à celui décrit à la section 3.2.4 pour déterminer l'identité d'un client ou d'un représentant qui formule une demande de changement est utilisé. Les renseignements sont divulgués lorsque l'identité du client a été vérifiée, sauf s'ils répondent à un critère d'exemption.

À l'AE (RHDCC), le coordonnateur local de la protection des renseignements personnels conserve un registre de toutes les demandes formelles qu'il transmet au coordonnateur régional de la protection des renseignements personnels une fois par mois. Celui-ci additionne les résultats annuels reçus des différents bureaux locaux et transmet ces statistiques à l'AC. Aux PSR (DSC), le coordonnateur local de la protection des renseignements personnels rassemble les demandes une fois par mois et les envoie à l'AC, qui compile les statistiques obtenues des régions une fois par année. Les statistiques concernant les demandes formelles et informelles sont transmises au sous-ministre adjoint (SMA) du programme, et seules les statistiques concernant les demandes formelles sont envoyées au Parlement.

Recommandation 15 : (RHDCC/DSC)

On devrait tenir compte de la nature et de la sensibilité des renseignements divulgués pour établir la distinction entre la divulgation formelle et informelle, et on devrait examiner les règles sur la documentation des divulgations.

Les règles et les procédures à suivre pour enregistrer la source et le motif de la divulgation informelle de renseignements personnels devraient être clarifiées.

Réponse de la direction :

On examinera les documents de formation et les politiques et les lignes directrices actuelles des directions générales, afin de s'assurer qu'ils traitent de la documentation des demandes non officielles, y compris les demandes verbales de renseignements, entraînant la divulgation de renseignements personnels.

2.5 Objectif 5 : L'information sur la nature et l'utilisation des renseignements personnels est à la disposition du public.

Critères de vérification

- Tous les fonds de renseignements personnels détenus par DRHC sont décrits de manière exacte dans les publications Info Source du Secrétariat du Conseil du Trésor.
- Tous les nouveaux problèmes ou services, ou tout changement important apporté à des programmes ou à des services existants, qui comprennent la collecte, l'utilisation ou la divulgation de renseignements personnels et qui touchent la vie privée, sont conformes à la Politique d'évaluation des facteurs relatifs à la vie privée.
- Les résumés des évaluations des secteurs relatifs à la vie privée (EFVP) sont accessibles au public.
- Le cas échéant, une stratégie de communication est mise en œuvre dans le but de faire face aux préoccupations et aux perceptions du public en ce qui concerne la vie privée.

2.5.1 Info Source

L'information sur la nature et l'utilisation des renseignements personnels est accessible au public par l'intermédiaire d'Info Source, qui décrit la structure du gouvernement du Canada et ses fonds de renseignements. Ceux-ci incluent les dossiers de programme et les fichiers de renseignements personnels.

Le rapport concernant chaque fichier de renseignements personnels contient leur description et des énoncés sur leur utilisation et leur divulgation. Le gouvernement utilise une procédure normalisée pour mettre ces rapports à jour. Chaque année, le groupe de la protection des renseignements personnels est responsable de mettre en œuvre un processus qui permettra à tous les programmes d'examiner leur secteur de responsabilités. Le groupe de la protection des renseignements personnels compile un rapport consolidé qu'il transmet au SCT. On procède également à la mise à jour d'Info Source si une EFVP l'exige.

2.5.2 Évaluation des facteurs relatifs à la vie privée

À RHDCC/DSC, des responsables de différents niveaux partagent la responsabilité de déterminer le besoin d'effectuer une EFVP. Les cadres de direction de l'AC et des régions sont chargés de cerner les programmes et les activités qui exigent la soumission d'une EFVP,

tandis que les gestionnaires de programmes et de services sont responsables d'établir cette soumission. Les coordonnateurs ministériels de la protection des renseignements personnels participent à l'élaboration des soumissions d'EFVP. Le sous-ministre est responsable d'approuver l'EFVP, après avoir reçu une recommandation favorable du Comité directeur du cadre de gestion de la protection des renseignements personnels à cet égard. Les soumissions d'EFVP dont on recommande l'approbation sont également examinées par le Commissariat à la protection de la vie privée (CPVP).

Conformément à la politique du SCT, on doit publier un résumé de chaque EFVP. RHDCC/DSC commence tout juste la mise en œuvre de ce processus, et aucun résumé d'EFVP n'a été publié à ce jour.

2.5.3 Préoccupations du public

Les infractions éventuelles à la vie privée sont signalées conformément aux procédures de sécurité ministérielle et font l'objet d'une enquête menée par la Direction de la sécurité, des enquêtes et des mesures d'urgence. La Direction de l'accès à l'information et de la protection des renseignements personnels est informée de l'infraction éventuelle et détermine si le CPVP doit être mis au courant, selon la sensibilité de l'affaire en question. Le cas échéant, le CPVP décide ensuite des mesures à prendre.

Les responsables du secteur de programme où s'est produit l'infraction éventuelle doivent travailler avec les Communications à la rédaction d'info capsules.

2.6 Objectif 6 : Les personnes ont accès à leurs propres renseignements personnels, et des procédures sont mises en place pour traiter les plaintes.

Critères de vérification

- Les personnes sont informées de leur droit d'avoir accès à leurs renseignements personnels.
- Une personne peut avoir accès à son dossier, en discuter ou remettre en question sa véracité, selon un processus établi.
- Il y a un processus par lequel une personne est informée qu'un changement a été apporté à ses renseignements personnels.
- Les particuliers peuvent avoir accès à leurs renseignements personnels dans la langue officielle et dans le média de leur choix.
- Les procédures de plaintes sont conformes aux exigences de la législation.

2.6.1 Accès aux renseignements personnels

Selon les gestionnaires et les employés interrogés, les clients de RHDCC/DSC sont informés de leur droit d'accéder au contenu de leur dossier sur le site Web et dans les formulaires de demande. Ils peuvent aussi être informés verbalement, au besoin.

Comme nous l'avons mentionné, dans cinq régions, les lettres envoyées aux clients en réponse à des demandes officielles précisent le droit des clients d'examiner et de remettre en question le contenu de leur dossier. Dans les télécentres, ces précisions sont fournies verbalement, de façon informelle.

Tel que mentionné plus haut, les clients ne sont pas systématiquement informés des changements apportés à leur dossier, sauf si ces modifications ont une incidence directe et immédiate sur leur admissibilité aux prestations.

Les responsables de tous les bureaux visités s'engagent à fournir aux clients l'accès aux renseignements personnels les concernant dans la langue officielle de leur choix et dans le média désiré, mais ils ont précisé que, dans certains cas, le respect de ces préférences pouvait retarder le traitement des demandes.

2.6.2 Procédures de plaintes

Dans toutes les régions, les membres du personnel ont déclaré disposer d'un mécanisme de règlement des plaintes lié à la protection des renseignements personnels. Celles-ci sont généralement traitées par le CPVP. Les gestionnaires et les employés de certaines régions ont affirmé qu'ils agissaient de façon proactive en essayant de remédier à la situation avant de transmettre l'affaire au CPVP.

Les résultats des plaintes ne sont pas systématiquement communiqués aux régions, sauf s'ils donnent lieu à une recommandation du CPVP visant la modification des procédures. On a précisé aux vérificateurs que, dans de tels cas, toutes les régions sont mises au courant.

3. CONCLUSION

Les vérificateurs tirent les conclusions suivantes :

- RHDCC/DSC déploie des efforts concertés dans le but d'améliorer la manipulation des renseignements personnels qu'il détient au sujet de ses clients et d'autres personnes et plusieurs projets ont été mis en œuvre pour renforcer la protection des renseignements personnels et garantir qu'ils sont consultés et utilisés à des fins légitimes.
- Des politiques et des procédures couvrant tous les aspects de la gestion des renseignements personnels ont été mises en place; certaines sont autonomes et d'autres sont intégrées aux politiques et aux procédures de sécurité. Trois comités de niveau supérieur consacrés à la protection des renseignements personnels ont été crées. L'élaboration du Cadre de gestion de la protection des renseignements personnels permet une redéfinition et une clarification de la notion de reddition de comptes.
- Un plan national de communication et de formation est recommandé pour garantir que tous les employés reçoivent une formation et une information opportunes et adéquates sur la législation, les politiques et les procédures liées à l'utilisation et à la protection des renseignements personnels dans leur secteur d'activités.
- Les travaux amorcés au sujet des pistes de vérification, de l'établissement de profils et de la gestion des codes d'accès devraient être complétés pour garantir que tous les groupes et tous les types d'employés peuvent accéder comme il se doit aux renseignements personnels.

Opinion globale

Nous sommes d'opinion, à la lumière de notre vérification, que des progrès important ont été réalisés et continuent à l'être dans la gestion des renseignements personnels.

Des améliorations supplémentaires sont cependant nécessaires, comme l'indiquent nos recommandations.

La gestion a développé un plan d'action adéquat (Annexe B) pour répondre à ces recommandations. Sa réalisation, particulièrement en ce qui concerne les recommandations 9 à 12, devrait résulter dans la mise en place des contrôles requis pour une gestion appropriée des renseignements personnels au sein de RHDCC et de DSC.

Selon notre jugement professionnel, des procédures de vérification adéquates ont été suivies et des preuves suffisantes ont été recueillies pour supporter les conclusions de ce rapport. Ces conclusions sont basées sur une comparaison de la situation qui existait au moment de la vérification avec les critères de vérification. Les conclusions ne s'appliquent que sur la gestion des renseignements personnels pour les activités examinées.

Cette vérification interne a été conduite en conformité avec la politique du Conseil du Trésor sur la vérification interne et les standards de l'Institut des vérificateurs internes sur les pratiques professionnelles.

Réponse générale de la direction

Le directeur général de Protection des renseignements personnels, conjointement avec les coordonnateurs pour RHDCC et DSC, ainsi que plusieurs directeurs généraux ont examiné la vérification de la gestion de la protection des renseignements personnels et ont collaboré à la préparation du plan d'action de gestion qui l'accompagne.

Les préoccupations exprimées par les Canadiens au sujet des renseignements personnels continuent de croître. La large disponibilité des offres de services intégrées, souvent offertes par le biais des nouveaux canaux électroniques, en est un des facteurs contributifs. Les Canadiens veulent avoir l'assurance que leurs renseignements personnels sont gérés soigneusement selon des paramètres bien définis. La Loi sur la protection des renseignements personnels et les autorités des programmes concernés définissent l'obligation de protéger les renseignements personnels et d'en assurer la cueillette, l'utilisation et la divulgation de manière appropriée. Ces autorités législatives sont appuyées par des politiques, des procédures et des outils qui ont fait l'objet de cette vérification.

La vérification interne et le plan d'action de gestion représentent une étape clé de la mise en oeuvre du Cadre de gestion de la protection des renseignements (CGPRP) qui a été primé. Ce cadre et ses quatre piliers de planification et gouvernance stratégiques, de gestion du risque, de changements culturels et d'assurance de conformité, concentrent l'attention ministérielle sur les questions qui ont trait à la vie privée. Des progrès considérables ont été réalisés et les initiatives des ministères ont été reconnues.

Ensemble, le CGPRP et cette vérification servent à démontrer de quelle manière nous remplissons notre obligation de protéger les renseignements personnels des Canadiens. Pour les deux dernières années, DRHC a reconnu la protection des renseignements personnels comme une priorité ministérielle stratégique dans le cadre de son objectif d'excellence du service. C'est une reconnaissance explicite, au plus haut niveau du ministère, de l'importance des renseignements personnels pour les Canadiens et leurs attentes à l'égard du gouvernement pour leur protection. Les Canadiens s'attendent à ce que RHDCC et DSC maintiennent cet engagement de gérer efficacement les renseignements personnels et de l'incorporer comme une composante intrinsèque de leurs cultures respectives. Comme la vérification l'a clairement démontré, la gestion efficace des renseignements personnels n'est pas différente de celle des autres actifs stratégiques. C'est pourquoi les contrôles sont en train d'être renforcés là où c'est nécessaire et un plan de formation national est en élaboration.

Tandis que RHDCC et DSC débutent la mise en œuvre de ce plan d'action de gestion, nous prenons l'engagement de déployer des efforts coordonnés pour remplir notre rôle de gardiens des renseignements personnels et maintenir la confiance que les Canadiens et les Canadiennes ont placée en nous.

ANNEXE A : OBJECTIFS, CRITÈRES ET MÉTHODOLOGIE DE LA VÉRIFICATION

À l'origine, on a cerné dix objectifs en rapport avec la vérification. Deux de ces objectifs, qui portaient sur la collecte des renseignements personnels, ont été laissés de côté en vue d'une vérification ultérieure. Dans le but de faciliter la production de rapports, on a regroupé les huit autres pour former les six objectifs ci-dessous. Les 10 objectifs initiaux sont inclus dans le mandat publié en mars 2003.

Objectif 1 :

La manutention et la protection des renseignements personnels sont incorporées au Cadre de gestion ministériel. (Objectif 1 du mandat)

On a utilisé les critères suivants pour l'examen des pratiques relatives aux renseignements personnels afin de garantir que :

1.1 la responsabilité de la protection et de l'usage judicieux des renseignements personnels est définie et documentée;

1.2 les politiques, les lignes directrices et les procédures relatives à la manutention et à la protection des renseignements personnels sont disponibles;

1.3 les employés sont informés à ce sujet et (ou) ont reçu une formation pertinente à ces questions;

1.4 la vérification, le contrôle et l'évaluation des risques et des contrôles liés à la manutention et à la protection des renseignements personnels sont faits régulièrement.

Objectif 2 :

La conservation, la protection et l'élimination des renseignements personnels respectent la politique du gouvernement en matière de sécurité. (Objectifs 4 et 5 du mandat)

On a utilisé les critères suivants pour l'examen des pratiques relatives aux renseignements personnels afin de garantir que :

2.1 Les renseignements personnels sont conservés selon un calendrier établi et sont éliminés conformément à la politique du gouvernement en matière de sécurité;

2.2 Des contrôles internes sont en place pour garantir que les renseignements personnels sont protégés contre toute modification, suppression et destruction non autorisées;

2.3 Les bases de données électroniques contenant des renseignements personnels sont protégées contre toute visualisation, reproduction et destruction non autorisée; et les bandes magnétiques et autres supports physiques contenant des renseignements personnels sont protégés, gardés en lieu sûr et accessibles seulement aux personnes autorisées;

2.4 Les renseignements personnels, au besoin, sont mis à jour promptement, et l'enregistrement de la source de l'information utilisée pour modifier les renseignements personnels est conservé.

Objectif 3 :

Les renseignements personnels sont accessibles seulement aux personnes autorisées et sont utilisés dans le but pour lequel ils ont été recueillis. (Objectifs 6 et 7 du mandat)

On a utilisé les critères suivants pour l'examen des pratiques relatives aux renseignements personnels afin de garantir que :

3.1 Des contrôles internes adéquats et efficaces sont en place afin de fournir l'assurance que :

- les demandes d'accès ou de modification de l'accès aux renseignements personnels proviennent d'une personne autorisée;
- le niveau d'accès demandé correspond au poste et aux fonctions actuels de la personne pour qui l'accès est demandé;
- le profil d'accès d'un employé dont le statut, le poste ou la fonction a changé est modifié, suspendu ou supprimé, si nécessaire.

3.2 l'utilisation des renseignements personnels est directement liée à une activité ou à un programme opérationnel et est en accord avec le but pour lequel les renseignements ont été obtenus ou compilés;

3.3 la visualisation des renseignements personnels est surveillée régulièrement pour que l'on puisse détecter tout accès non autorisé ou injustifié par des pistes de vérification ou d'autres moyens de contrôle appropriés;

3.4 l'anonymat des renseignements personnels utilisés pour l'analyse de politiques, la recherche et l'évaluation est préservé avant l'utilisation ou la divulgation, sauf avis contraire;

3.5 les renseignements personnels utilisés à des fins administratives ou de gestion de programme dont l'anonymat n'est pas préservé sont protégés contre toute utilisation ou tout accès non autorisé;

3.6 la comparaison de données et le couplage des dossiers correspondent au but pour lequel les renseignements ont été obtenus ou compilés;

3.7 les comparaisons de données à des fins administratives et le couplage de dossiers à des fins non administratives et de recherche nécessitant l'utilisation de renseignements personnels respectent les exigences des politiques applicables — la politique du Conseil du Trésor sur la comparaison des données et les politiques de RHDCC/DSC sur le couplage de dossiers;

3.8 les documents contenant des renseignements personnels portaient la mention « Protégé » et sont manipulés conformément à la législation relative à la protection

des renseignements personnels, la politique gouvernementale en matière de sécurité et d'autres lois, règlements et politiques applicables;

3.9 des procédures existent pour traiter les cas de violation de la sécurité ou de divulgation de renseignements personnels par erreur.

Objectif 4 :

Les renseignements personnels sont divulgués dans le respect de la *Loi sur la protection des renseignements personnels* et autres lois, règlements, politiques et ententes applicables. (Objectif 8 du mandat)

On a utilisé les critères suivants pour l'examen des pratiques relatives aux renseignements personnels afin de garantir que :

4.1 L'autorisation de divulguer les renseignements personnels est clairement établie et documentée, le processus de divulgation respecte les politiques et procédures applicables, et la nature et la quantité des renseignements personnels divulgués sont limitées à l'objectif de la divulgation.

Objectif 5 :

L'information sur la nature et l'utilisation des renseignements personnels est à la disposition du public. (L'objectif 9 du mandat)

On a utilisé les critères suivants pour l'examen des pratiques relatives aux renseignements personnels afin de garantir que :

5.1 tous les fonds de renseignements personnels détenus par RHDCC/DSC sont décrits de manière exacte dans les publications Info Source du Secrétariat du Conseil du Trésor;

5.2 tous les nouveaux programmes ou services, ou tout changement important apporté à des programmes ou à des services existants, qui comprennent la collecte, l'utilisation ou la divulgation de renseignements personnels et qui touchent la vie privée sont conformes à la Politique sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor;

5.3 les résumés des évaluations des facteurs relatifs à la vie privée (EFVP) sont accessibles au public;

5.4 le cas échéant, une stratégie de communication est mise en œuvre dans le but de faire face aux préoccupations et aux perceptions du public en ce qui concerne la vie privée.

Objectif 6 :

Les personnes ont accès à leurs propres renseignements personnels et des procédures sont mises en place pour traiter les plaintes. (Objectif 10 du mandat)

On a utilisé les critères suivants pour l'examen des pratiques relatives aux renseignements personnels afin de garantir que :

6.1 les personnes sont informées de leur droit d'avoir accès à leurs renseignements personnels;

6.2 une personne peut avoir accès à son dossier, en discuter ou remettre en question sa véracité, selon un processus établi;

6.3 il existe un processus par lequel une personne est informée qu'un changement a été apporté à ses renseignements personnels;

6.4 les particuliers ont accès à leurs renseignements personnels dans la langue officielle et dans le média de leur choix;

6.5 les procédures de plaintes sont conformes aux exigences de la législation.

PORTÉE

La vérification a porté sur l'utilisation, le partage et la sécurité des renseignements personnels à l'assurance-emploi, aux Programmes de la sécurité du revenu, aux Systèmes ministériels des comptes débiteurs (SMCD) et à Politique stratégique.

La vérification a mis l'accent sur les renseignements personnels reçus de l'Agence des douanes et du revenu du Canada (ADRC), mais s'est étendue aux contrôles et aux systèmes plus vastes du Ministère lorsqu'il n'était pas possible ou pratique d'identifier ou de séparer la partie du contrôle ou de système qui est directement liée aux renseignements personnels reçus de l'ADRC. Cela comprend, mais sans s'y limiter, la production et l'attribution de ID utilisateurs donnant accès à des renseignements personnels, la protection des mots de passe qui y sont associés, la protection physique et logique des documents et de bases de données électroniques.

Ce projet s'étendait à l'AC, aux quatre centres de technologie de l'information et à des bureaux régionaux et à des points de service choisis dans tout le pays.

MÉTHODOLOGIE

Dans cette vérification, nous avons identifié et évalué la pertinence des contrôles internes reliés à la protection des renseignements personnels et nous avons déterminé si les objectifs et les critères applicables à la gestion des renseignements personnels, tels que définis dans le présent document, ont été atteints.

Cette vérification a utilisé des outils et une méthodologie standard incluant des entrevues individuelles et de groupe, des observations sur le terrain, l'examen et l'analyse documentaires, l'analyse statistique, des graphiques d'acheminement et des procédures de vérification analytiques.

ANNEXE B : PLAN D'ACTION LIÉ À LA GESTION

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
1) Compte tenu des interrelations et du partage des renseignements personnels entre les deux ministères, on devrait élaborer, communiquer et mettre en œuvre un cadre redditionnel pour la manipulation des renseignements personnels à tous les niveaux et dès que possible.	On officialisera les responsabilités ministérielles des sous-ministres et de tous les employés en matière de sécurité et de protection des renseignements personnels. On rédigera une déclaration globale relative à la vie privée et résumant, à l'intention des clients et du personnel, l'engagement du Ministère envers la manipulation appropriée de leurs renseignements personnels.	Deuxième trimestre de l'exercice 2004-2005	Direction des communications ministérielles (RHDCC) DG Affaires corporative et ministérielle (DSC)
2) On devrait examiner les politiques et les procédures de gestion des renseignements personnels pour s'assurer qu'elles tiennent compte suffisamment et convenablement des questions relatives à la protection des renseignements personnels.	Avec l'aide d'experts en matière de sécurité et de vie privée, les directions générales seront chargées, conformément au Cadre de gestion de la protection des renseignements personnels, d'examiner la justesse et la suffisance de leurs politiques et de leurs procédures de gestion des renseignements personnels.	Premier trimestre de l'exercice 2004-2005	Direction des communications ministérielles (RHDCC) DG Affaires corporative et ministérielle (DSC)
3) On devrait normaliser les ententes signées par les télétravailleurs afin de garantir que les clauses portant sur la confidentialité des renseignements personnels précisent l'obligation de protéger la confidentialité des renseignements et les règles à suivre à ce chapitre. Les membres du conseil arbitral de l'AE devraient être tenus de signer une entente semblable.	Examiner l'application uniforme des ententes visant les télétravailleurs. Avec l'approbation du commissaire, des politiques et des procédures seront élaborées et mises en œuvre dans le but de garantir que les membres du conseil arbitral sont informés de leur obligation de protéger les renseignements provenant de dossiers d'appel, d'audiences et de décisions, et qu'ils conviennent de respecter ces obligations.	30 octobre 2004 1er octobre 2004	DG, Direction des programmes des ressources humaines DG, Politique de l'assurance

*Mise à jour août 2004

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
4) On devrait établir un plan stratégique national de formation et de communication, afin de garantir que tous les employés qui ont ou pourraient avoir accès à des renseignements personnels reçoivent une formation et des informations opportunes et appropriées sur la législation, les politiques et les procédures concernant l'utilisation et la protection des renseignements personnels dans leur secteur d'activité.	Phase I — Effectuer une recherche pour évaluer les besoins en matière d'apprentissage, définir les objectifs d'apprentissage et cerner les lacunes. Phase II — Concevoir et (ou) adapter les produits d'apprentissage pour déterminer l'approche, la méthodologie et les outils d'apprentissage les plus appropriés en vue de réaliser l'objectif d'apprentissage. Phase III — Commencer à fournir des documents de formation aux formateurs qualifiés et travailler avec d'autres directions générales et d'autres régions afin de mettre en œuvre une méthode de « formation des formateurs ». Formation offerte par la Sécurité des SFA	30 septembre 2004 30 octobre 2004 31 décembre 2004 En cours	DG, Direction des programmes des ressources humaines DG, Services administratifs
5) La direction devrait s'assurer que les personnes qui donnent et qui obtiennent l'accès à des renseignements personnels comprennent la nature et l'application du principe du « besoin de savoir », de même que les conséquences de violation telles le « furetage » et les divulgations illicites.	Les mesures prises par l'AE sont précisées dans la recommandation 9. PSR • Poste de contrôle d'accès au système • Examiner les codes d'accès/les profils d'utilisateur actuels dans l'ancien système afin de garantir qu'ils sont exacts et à jour • Mettre en œuvre les lignes directrices opérationnelles nationales pour les demandes d'accès (profils d'emploi) • Appliquer les droits d'accès de l'ancien système des PSR au Système de prestation des PSR • Examiner et mettre à jour le guide d'accès de l'utilisateur des PSR/les procédures d'entrée et de sortie SFA-SMCD • Garantir que les descriptions de travail et la matrice de sécurité connexe correspondent aux renseignements accessibles	Deuxième trimestre de l'exercice 2004-2005 Deuxième trimestre de l'exercice 2004-2005 Deuxième trimestre de l'exercice 2004-2005 AC : Les travaux se poursuivent à mesure que la fonctionnalité augmente; fin du projet : 2007 Examen annuel 30 septembre 2004	DG, Direction de l'intégration stratégique, PSR DG, Services comptables

*Mise à jour août 2004

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
	• Examiner les écrans associés aux éléments contenus dans la matrice de sécurité • Compte tenu des résultats de l'examen, établir de nouvelles exigences opérationnelles dans le but d'élaborer, s'il y a lieu, une nouvelle matrice de sécurité • Évaluer l'incidence que ces changements auront sur les politiques actuelles relatives aux lignes directrices opérationnelles • Tous les nouveaux utilisateurs du SMCD recevront un document sur la législation, les politiques et les procédures relatives à l'utilisation et à la protection des renseignements personnels.	31 mars 2005 20 septembre 2005 Terminé Terminé	
6) Toutes les situations où l'on fait appel à une société ouverte pour le transport ou l'élimination des documents contenant des renseignements personnels devraient faire l'objet d'un contrat établissant et précisant la responsabilité de l'entreprise relativement à la protection des renseignements personnels qu'elle contrôle. Seuls les trois derniers chiffres du numéro d'assurance sociale devraient être inscrits sur les boîtes expédiées aux Archives nationales.	Établir des liens avec la protection des renseignements personnels afin de confirmer les dispositions applicables à utiliser, et assurer la liaison avec TPSGC. Élaborer des procédures et communiquer avec les agents d'approvisionnement régionaux et les coordonnateurs de la protection des renseignements personnels. On a modifié les lignes directrices, en précisant que seuls les trois derniers chiffres du NAS devaient être inscrits sur les faces extérieures des boîtes expédiées ou entreposées à l'extérieur de RHDCC/DSC.	Décembre 2004 Décembre 2004 Terminé	DG, Services administratifs.

*Mise à jour août 2004

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
7) Compte tenu du grand nombre de situations exigeant la protection de la confidentialité des dossiers des clients, on recommande à RHDCC et à DSC d'effectuer des évaluations individuelles des risques et des contrôles dans les locaux où sont conservés les documents contenant des renseignements personnels, afin de déterminer si le niveau de protection contre l'accès non autorisé aux dossiers des clients ou le retrait de ces dossiers est approprié.	On effectuera plusieurs évaluations de la menace et des risques (EMR) dans tout le Ministère. On augmentera la séquence des ratissages de sécurité et des séances de sensibilisation à la sécurité.	Portera sur l'ensemble du Ministère pour l'exercice 2004-2005.	DG, Services administratifs
8) On devrait clarifier les règles et les procédures touchant l'enregistrement des sources et des motifs des changements apportés aux renseignements personnels, de même que la conservation des documents de preuve, afin de réduire les risques de modifications inappropriées, qui pourraient entraîner des préjudices.	Le programme de l'AE fournira des directives nationales afin de clarifier les politiques et les procédures concernant la documentation des sources et des motifs des changements.	Septembre 2004	DG, Politique de l'assurance
9) On devrait définir clairement et mettre en pratique les responsabilités et les obligations redditionnelles de tout participant au processus de gestion de tous les codes d'accès et les profils qui permettent d'accéder à des renseignements personnels. On devrait fournir de la documentation sur la nature des renseignements personnels auxquels les employés ont accès.	Achever tous les profils d'emploi nationaux de l'AE (à l'heure actuelle, 75 % des profils ont été établis). Définir les rôles, les responsabilités et les obligations redditionnelles du gestionnaire de programmes de l'AE en rapport avec les profils et les codes d'utilisateurs. Mettre en œuvre les profils d'emploi. Les PSR mettront régulièrement à jour les rôles de l'utilisateur, du gestionnaire et de l'ARSA, et distribueront le guide de l'utilisateur de l'ARSA. Élaborer un document précisant clairement les rôles des personnes qui participent à l'établissement d'un code d'utilisateur dans le SMCD.	Terminé Deuxième trimestre de l'exercice 2004-2005 Voir la réponse fournie par la Direction générale des systèmes dans la recommandation 11 Octobre 2004 Septembre 2004	DG, Services de l'assurance DG, Direction de l'intégration stratégique, PSR DG, Services comptables

*Mise à jour août 2004

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
10) On devrait définir, comprendre et reconnaître les responsabilités et les obligations redditionnelles liées à l'attribution des codes d'accès et respectant les exigences en matière de protection des renseignements personnels.	Les Opérations de la TI/de la sécurité définiront et communiqueront tous les rôles et les responsabilités pour toutes les étapes liées à l'attribution, à la conservation et à l'annulation d'un code d'accès. Les lignes directrices concernant les examens annuels et les annulations des codes d'accès pour le SMCD seront élaborées conjointement avec le coordonnateur de l'accès régional.	Version préliminaire : septembre 2004 30 septembre 2004	DG principal, Direction des services de technologie DG principal, Opérations de la technologie de l'information DG, Services comptables
11) Pour permettre aux gestionnaires de surveiller de façon efficace et efficiente l'accès aux renseignements personnels, et pour faciliter l'organisation de vérifications véridiques, on devrait prendre les mesures suivantes dès que possible :			
1) Établir une liste de tous les codes d'accès qui permettent d'accéder aux programmes et aux bases de données de l'AE, des PSR ou des SFA (SMCD) contenant des renseignements personnels, certifiée par le niveau décisionnel approprié (qui sera précisé dans le cadre de responsabilités ministérielles des renseignements personnels en cours d'élaboration).	La Sécurité/les Opérations de la TI produiront un rapport qui sera vérifié par les gestionnaires de CR dans tous les secteurs de programme. Ce rapport indiquera le code d'accès, le nom, le CIDP et les capacités d'accès aux secteurs de programme auxquels le code d'accès en question permet d'accéder. Les PSR procéderont à l'élaboration et à la mise en œuvre d'un rapport national à l'intention des gestionnaires de CR. Les responsables du programme sont chargés de limiter l'accès dans leur secteur de programme.	Septembre 2004 Mise en œuvre prévue : septembre 2004.	DG principal, Direction des services de la technologie Gestionnaires de CR de la Direction de l'information stratégique des PSR
2) Mettre en œuvre des processus concrets en vue de déterminer avec certitude l'identité du titulaire de chaque code d'accès énuméré en (1).	Les activités susmentionnées entraîneront la vérification de la convivialité de tous les codes d'accès et l'examen de leur titulaire. Afin de garantir que l'information demeure exacte et à jour, on étudie les options suivantes : a) L'annulation automatique des codes d'accès inactifs b) L'établissement de liens avec la Sécurité des SFA pour garantir que son personnel est informé des changements apportés au statut des employés c) Mises à jour/examens trimestriels avec tous les gestionnaires de CR	4 octobre 2004	DG principal, Direction des services de la technologie

*Mise à jour août 2004

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
3) Mettre en œuvre des processus concrets afin de déterminer avec certitude la fonction exercée par chaque titulaire recensé en (2). 4) Établir des grilles mettant en rapport chaque fonction relevée en (3) avec un profil d'accès qui respecte les exigences en matière de protection des renseignements personnels.	Les activités énumérées en réponse aux points 1 et 2 de la recommandation 11 permettront de déterminer et de vérifier les capacités d'accès des employés. Les responsables des secteurs de programmes établiront les fonctions qui peuvent être exercées dans leur programme en se fondant sur la réponse de la direction à la recommandation 9.	Même délai que pour la recommandation 9, puis trois mois supplémentaires pour recenser le profil de chaque utilisateur et effectuer un rapprochement entre ces profils et le code d'accès.	DGP/ DST, DGP/OTI Secteurs de programmes
	Lorsque les secteurs de programme auront achevé la création des profils (groupes de codes de transactions), la Sécurité/les Opérations de la TI créeront un profil correspondant dans la Procédure d'entrée unique et de l'administration de la sécurité (PEUAS).	Même délai que pour la recommandation 9, puis trois mois supplémentaires pour recenser le profil de chaque utilisateur et effectuer un rapprochement entre ces profils et le code d'accès.	DGP/DST, DGP/OTI Secteurs de programmes
	Les secteurs de programme distingueront les profils de chaque utilisateur. La Sécurité/les Opérations de la TI rapprocheront les profils et les codes d'accès. Les rapports seront communiqués aux gestionnaires de CR, qui devront les vérifier.		
	AE		
	• Élaborer et mettre en œuvre un processus d'approbation visant l'autorisation de l'accès aux données de l'AE (demandes de l'AC)	Terminé	DG, Services de l'assurance
	• Élaborer un processus d'approbation visant l'autorisation de l'accès aux données de l'AE (demandes régionales)	Deuxième trimestre de l'exercice 2004-2005	
	• Mettre en œuvre un processus d'approbation pour l'AE à l'échelle régionale	À déterminer en collaboration avec les régions	

*Mise à jour août 2004

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
	• Élaborer un processus de surveillance afin de garantir la gestion efficace des codes d'utilisateurs conjointement avec la Sécurité du CTI. On inclura ce processus dans le plan des systèmes généraux afin d'examiner la documentation, les procédures et les processus actuels, indiqués dans la recommandation 10.	À déterminer en collaboration avec la sécurité du CTI	
	PSR		
	• Obtenir la liste des utilisateurs		
	• Harmoniser les données sur les utilisateurs avec la structure organisationnelle en place • Faire concorder les délégations de pouvoir avec les descriptions de travail • Faire concorder les descriptions de travail avec les accès • Examiner et approuver le processus (tâche de la direction) • Mettre à jour la liste d'utilisateurs (tâche de l'ARSA)	Les travaux se poursuivront à mesure que la fonctionnalité augmentera; date d'achèvement prévue : 2007	DG, Direction de l'intégration stratégique, PSR
	SMCD		
	• Établir une liste de tous les codes d'accès pour le SMCD	Terminé	DG, Services comptables
	• Effectuer un recoupement entre le nom des différentes personnes et l'accès au SMCD pour chaque CIDP	Septembre 2004	
	• Exiger que l'utilisateur entre son CIDP avant de délivrer un code d'accès	Terminé	
	• Établir une matrice de sécurité pour le SMCD, selon les différentes fonctions	Terminé	
	• Établir une matrice de sécurité incluant les descriptions de travail. Continuer de s'assurer que le SMCD contient des commandes d'édition qui empêchent la création d'un profil d'utilisateur à l'aide d'une matrice de sécurité invalide.	Terminé	

*Mise à jour août 2004

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU	RESPONSABILITÉ
PROTÉGÉ			

RECOMMANDATIONS DE LA VÉRIFICATION INTERNE	PLAN DE MESURES CORRECTIVES LIÉ À LA GESTION	DATE D'ACHÈVEMENT PRÉVU*	RESPONSABILITÉ
13) On devrait compléter le Guide de classification de l'information par un ensemble de directives pratiques pour la classification et la manipulation des principaux documents contenant des renseignements personnels utilisés par les responsables des différents programmes.	Produire un manuel/un guide pour aider les employés à manipuler, classer, transmettre et mettre en mémoire les renseignements classifiés et sensibles.	Terminé	DG, Services administratifs
On devrait mettre en place des mécanismes de contrôle interne afin de garantir que les documents protégés sont désignés comme tels et manipulés selon le niveau de protection qu'on leur a attribué.	Mettre à jour la formation et la sensibilisation à la sécurité, y compris les mesures de protection des renseignements délicats. Recommencer à effectuer des ratissages de sécurité.	Terminé	
14) On devrait préciser et communiquer la procédure que le gestionnaire et les employés doivent suivre lorsqu'ils prennent connaissance d'une violation possible de la protection des renseignements personnels.	Élaborer un manuel ministériel contenant des lignes directrices pour la conduite d'enquêtes administratives. Organiser des séances de sensibilisation concernant la conduite d'enquêtes administratives avec les intervenants (c.-à-d. SRH, Services juridiques et Sécurité).	Terminé Exercice 2004-2005	DG, Services administratifs
15) On devrait tenir compte de la nature et de la sensibilité des renseignements divulgués pour établir la distinction entre la divulgation officielle et non officielle, et on devrait examiner les règles sur la documentation des divulgations. On devrait clarifier les règles et les procédures à suivre pour enregistrer la source et le motif de la divulgation non officielle de renseignements personnels.	On examinera les documents de formation actuellement utilisés par les PSR à l'AC, afin de garantir qu'ils informent suffisamment les employés des questions relatives à l'enregistrement des communications de renseignements sensibles découlant de demandes non officielles, et notamment de demandes de renseignements verbales. On demandera également aux directions générales d'examiner leurs procédures en matière d'enregistrement des communications verbales et non officielles de renseignements.	Troisième trimestre de l'exercice 2004-2005	DG, Communications ministérielles

*Mise à jour août 2004

ANNEXE C : LISTE DES BUREAUX VISITÉS

Liste des bureaux visités			
C.-B.C	1	CT PSR	Victoria
	2	CT/CRHC AE	Victoria
	3	Télécentre des PSR	Vancouver
	4	COPA	Vancouver
		BR	Vancouver
	5	SMCD	Vancouver
Sask.	6	CRHC/CT AE	Regina
	7	Télécentre de l'AE	Regina
	8	SMCD	Regina
		BR	Regina
	9	CT PSR	Winnipeg
		CTI	Winnipeg
Î.-P.-É.	10	CT AE	Montague
	11	CRHC AE	Charlottetown
	12	CT PSR	Charlottetown
		BR	Charlottetown
N.-B.	13	Télécentre de l'AE	Bathurst
	14	Télécentre des PSR	Bathurst
	15	CT AE	Bathurst
	16	SMCD	Moncton
	17	COPA	Moncton
		CTI	Moncton
	18	CT PSR	Fredericton
		BR	Fredericton
Ont.	19	CT PSR	Chatham
	20	CRHC/CT	St.Catherines
	21	Satellite	Niagara Falls
	22	CRHC/CT	Mississauga
	23	Télécentre de l'AE	Toronto
	24	Télécentre des PSR/CT	Scarborough
		BR (PSR)	Toronto
		CTI	Belleville
	25	COPA	Belleville
	26	SMCD	Belleville
		BR (AE)	Belleville

Liste des bureaux visités			
Qué.	27 28 29 30 31 32 33 34 	CT PSR Satellite CT AE CT AE SMCD CTI Télécentre de l'AE Télécentre des PSR COPA BR	Québec Québec Sherbrooke Montréal Montréal Montréal Montréal Montréal Montréal Montréal
Total		34 bureaux 6 BR 4 CTI	
Vérification à l'AC		AE SFA PSR PS Systèmes	 (SMCD, Sécurité, protection des renseignements personnels, Services administratifs, Services juridiques)