Agriculture and Agri-Food Canada | Agriculture et Agroalimentaire Canada

Vérification de la protection des renseignements personnels

Rapport final

Bureau de la vérification et de l'évaluation

Novembre 2010

Canada

Le Comité de vérification d'AAC a recommandé, le 5 novembre 2010, que ce rapport de vérification soit approuvé par le sous-ministre.

Pour obtenir plus de renseignements sur le Bureau de la vérification et de l'évaluation, veuillez visiter le site suivant :
http://www.agr.gc.ca/aud_eval

AAC 11426F
ISBN 978-1-100-96993-0
No. de catalogue A34-18/2011F-PDF

Also available in English under the heading: Information Privacy

TABLE DES MATIÈRES

Page

RÉSUMÉ

Pour réaliser ses programmes et fournir ses services aux Canadiens, AAC doit recueillir et gérer un grand nombre de renseignements personnels de ses clients et des membres de son personnel. Le Ministère est assujetti à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes établies par le Secrétariat du Conseil du Trésor (SCT). Pour réaliser ses programmes, et en raison de la nature de son travail, AAC fait face au risque inhérent élevé de contrevenir aux dispositions de la *Loi sur la protection des renseignements personnels* ou aux politiques et directives du SCT. L'importance des activités d'atténuation des risques liés à la protection des renseignements personnels est aussi énoncée dans le profil de risque d'AAC.

Le Bureau de l'accès à l'information et de protection des renseignements personnels (AIPRP) d'AAC rend compte de ses activités au moyen des Services de gestion de l'information (SIG) et par l'entremise de la direction générale des Systèmes d'information (DGSI) et a le mandat de mettre en œuvre et d'administrer la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*. Le Bureau de l'AIPRP doit s'assurer que le cadre stratégique, les processus et les outils appropriés ont été mis en œuvre par AAC de manière à assurer le respect des exigences en matière de protection des renseignements personnels. Compte tenu du fait que la gestion des renseignements personnels a lieu au niveau du programme, les employés chargés du programme ont l'importante responsabilité de s'assurer que cette directive fondamentale sur la gestion des renseignements personnels est appliquée de manière appropriée.

Compte tenu des risques inhérents liés au respect de la *Loi sur la protection des renseignements personnels* dans un environnement comme celui d'AAC, le sous-ministre a approuvé une vérification de la conformité à la *Loi sur la protection des renseignements personnels* qui doit être intégrée au Plan de vérification axé sur les risques de 2009-2012 d'AAC.

La vérification visait à évaluer le caractère adéquat et l'efficacité du cadre de contrôle de la gestion existant pour assurer la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes du Conseil du Trésor.

La vérification a porté sur tous les renseignements personnels des clients et des membres du personnel d'AAC en format électronique et papier. La vérification a visé toutes les activités d'AAC liées à la conformité à la protection des renseignements personnels du 1er avril 2008 au 31 mars 2010. Les étapes de planification et de réalisation de la vérification ont eu lieu entre novembre 2009 et avril 2010.

Les critères de vérification utilisés pour évaluer le cadre de contrôle de la gestion ont été élaborés en fonction des exigences législatives et politiques en matière de protection des renseignements personnels d'AAC.

La vérification a conclu que le cadre actuel de contrôle de la gestion de la protection des renseignements personnels d'AAC nécessite quelques améliorations pour régler certains problèmes qui exposent AAC à des risques éventuels de non-conformité aux dispositions de la *Loi sur la protection des renseignements personnels* et aux directives et politiques

connexes du Conseil du Trésor et au risque accru que la collecte, l'utilisation ou la divulgation des renseignements personnels ne soient pas appropriées. La vérification a mis en évidence des problèmes dans les domaines suivants :

- Un organisme de gouvernance n'a pas reçu le mandat clair d'effectuer des activités de contrôle de la protection des renseignements personnels et les rôles et les responsabilités des personnes à l'extérieur du Bureau de l'AIPRP n'ont pas été clairement définies;
- On n'a pas élaboré une stratégie de formation et de sensibilisation axée sur la protection des renseignements personnels pour s'assurer que les exigences en matière de protection des renseignements personnels des postes clés d'AAC sont comprises par les titulaires des postes;
- Les contrôles visant à s'assurer que les tiers fournisseurs de services gèrent les renseignements personnels de manière appropriée sont inadéquats;
- Les contrôles visant à s'assurer que l'utilisation du numéro d'assurance sociale (NAS) est conforme aux exigences de la Directive sur l'utilisation du NAS du SCT sont inadéquats;
- Les risques liés à la protection des renseignements personnels n'ont pas été pris suffisamment en considération et n'ont pas été intégrés à l'élaboration du programme sur l'excellence du service d'AAC;
- L'examen des évaluations des facteurs relatifs à la vie privée (EFVP) n'a pas été effectué en temps opportun et on a négligé d'assurer le suivi pour déterminer si les mesures appropriées pour atténuer les risques ont été prises;
- Les renseignements électroniques qui peuvent inclure des renseignements personnels ne sont pas éliminés, en règle générale, conformément aux calendriers de disposition de documents.

La vérification a déterminé que les contrôles dans d'autres domaines sont satisfaisants et a mis en évidence un certain nombre de pratiques exemplaires. Par exemple, le Bureau de l'AIPRP a fait beaucoup de progrès au cours de la dernière année pour consolider son rôle au sein du Ministère et pour déterminer les ressources nécessaires pour respecter son mandat, notamment l'élaboration d'un certain nombre de politiques et le développement d'activités de formation et de sensibilisation axées sur la protection des renseignements personnels pour le Ministère. Le Bureau de l'AIPRP a aussi centralisé le processus de l'EFVP et s'est assuré qu'il est administré par le Bureau de l'AIPRP.

Pour les domaines visés par la vérification, y compris les deux domaines de programmes et la Direction générale des RH, les renseignements personnels sont recueillis par l'autorité compétente d'AAC et à des fins appropriées qui sont en harmonie avec l'administration du programme et du domaine fonctionnel.

Le dirigeant principal de la vérification a affirmé que les procédures de vérification ont été adéquates et suffisantes et que des éléments probants ont été réunis pour assurer l'exactitude de son opinion contenue dans le rapport détaillé.

1.0 INTRODUCTION

1.1 Contexte

Pour réaliser ses programmes et fournir ses services aux Canadiens, AAC doit recueillir et gérer un grand nombre de renseignements personnels de ses clients et des membres de son personnel. Le Ministère est assujetti à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes établies par le Secrétariat du Conseil du Trésor (SCT). La *Loi sur la protection des renseignements personnels* vise à protéger les renseignements personnels détenus par les organismes gouvernementaux et à accorder aux citoyens le droit d'accéder à leurs renseignements personnels et de corriger toute erreur. Il existe un certain nombre de politiques et de directives du SCT sur les pratiques appropriées de protection des renseignements personnels détenus par le Ministère, y compris des directives précises sur l'utilisation du numéro d'assurance sociale (NAS) et sur les méthodes pour effectuer les évaluations des facteurs relatifs à la vie privée (EFVP). Les EFVP fournissent un cadre fondé sur les risques pour déterminer et examiner les questions relatives à la protection des renseignements personnels liées aux programmes, aux initiatives ou aux systèmes qui obtiennent ou gèrent les renseignements personnels.

Le Bureau de l'accès à l'information et de protection des renseignements personnels (AIPRP) d'AAC rend compte de ses activités au moyen des Services de gestion de l'information (SIG) et par l'entremise de la Direction générale des systèmes d'information (DGSI), dirigée par le dirigeant principal de l'information (DPI), et a le mandat de mettre en œuvre et d'administrer la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*.

Dans le cadre de ses responsabilités relatives à la *Loi sur la protection des renseignements personnels*, le Bureau doit notamment s'assurer que les exigences politiques et législatives sont respectées et qu'un cadre de gestion de la protection des renseignements personnels approprié est mis en œuvre pour le ministère. Le Commissariat à la protection de la vie privée du Canada (CPVP) définit le cadre de gestion de la protection des renseignements personnels comme : *« la manière dont chaque institution est organisée, à l'aide de structures, de politiques, de systèmes et de procédures, pour déléguer les responsabilités, coordonner les activités et gérer les risques relatifs à la vie privée, ainsi que pour assurer la conformité à la Loi sur la protection des renseignements personnels. »* Actuellement, il existe sept postes liés à la protection de la vie privée au Bureau de l'AIPRP.

En plus du Bureau de l'AIPRP, le Centre d'excellence des programmes de la DGPFA joue un rôle de surveillance pour tous les programmes de subventions et de contributions non liés à la GRE (gestion des risques de l'entreprise) et donne notamment des conseils sur les dispositions sur la protection des renseignements personnels que les programmes doivent inclure dans les ententes avec des tiers.

En dernier lieu, les membres du personnel d'AAC doivent protéger les renseignements personnels qu'ils gèrent.

Pour réaliser ses programmes, et en raison de la nature de son travail[1], AAC fait face au risque inhérent de contrevenir aux dispositions de la *Loi sur la protection des renseignements personnels* ou aux politiques et directives du SCT. L'importance des activités d'atténuation des risques liés à la protection des renseignements personnels est aussi énoncée dans le profil de risque d'AAC. En raison de ce risque, le sous-ministre a approuvé une vérification de la conformité à la *Loi sur la protection des renseignements personnels* qui doit être intégrée au Plan de vérification axé sur les risques de 2009-2012 d'AAC.

1.2 Objectif de la vérification

La vérification visait à évaluer le caractère adéquat et l'efficacité du cadre de contrôle de la gestion existant pour assurer la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes du Secrétariat du Conseil du Trésor.

1.3 Portée de la vérification

La vérification a évalué le cadre de contrôle de la gestion et la gouvernance du Ministère pour assurer la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes du Conseil du Trésor. La vérification a porté sur tous les renseignements personnels des clients et des membres du personnel d'AAC en format électronique et papier. La vérification a visé toutes les activités d'AAC liées à la conformité à la protection des renseignements personnels du 1er avril 2008 au 31 mars 2010.

En fonction de l'évaluation des risques effectuée pendant l'étape de planification de la vérification, on a décidé que la vérification devait se concentrer non seulement sur le Bureau de l'AIPRP, mais aussi sur la Direction générale des programmes financiers pour l'agriculture (DGPFA) et la Direction générale des ressources humaines (RH). On a choisi ces domaines parce que la plupart des renseignements personnels des clients sont recueillis par la DGPFA, plus précisément par la Direction des programmes du revenu agricole (DPRA) (située à Winnipeg) et par la Direction des programmes d'aide financière et de renouveau (située à Ottawa). En outre, la Direction générale des ressources humaines possède un grand nombre de renseignements personnels potentiellement délicats des membres du personnel.

Bien que le Bureau de l'AIPRP doive aussi assurer la conformité à la *Loi sur l'accès à l'information*, cette vérification ne visait pas la conformité à cette loi.

1.4 Méthode de vérification

La vérification a été effectuée conformément aux *Normes pour la pratique professionnelle de la vérification interne* et à la *Politique sur la vérification interne* du Conseil du Trésor. Ces normes énoncent que la vérification doit être planifiée et menée de manière à obtenir l'assurance raisonnable que les objectifs de la vérification ont été atteints.

[1] Par exemple, AAC travaille fréquemment, dans le cadre du programme des paiements de transfert et des ententes contractuelles, avec des tiers c.-à-d. avec des organisations ou des personnes indépendantes, qui fournissent les programmes ou les services d'AAC aux prestataires ou aux bénéficiaires ultimes.

La vérification a comporté plusieurs contrôles, selon les besoins, pour obtenir une telle assurance. Ces contrôles ont été notamment des entrevues, des observations, des visites, l'examen des documents pertinents et des examens analytiques.

Les critères de vérification utilisés pour évaluer le cadre de contrôle de la gestion ont été élaborés en fonction des exigences législatives et politiques en matière de protection des renseignements personnels d'AAC et plus précisément les exigences énoncées dans :

- La *Loi sur la protection des renseignements personnels* et les règlements connexes;
- La politique sur la protection de la vie privée;
- La directive sur le numéro d'assurance sociale (NAS);
- La politique sur l'évaluation des facteurs relatifs à la vie privée (EFVP).

Il faut souligner que la politique sur l'EFVP du SCT a été remplacée à partir du 1er avril 2010 par une nouvelle directive sur l'EFVP. La nouvelle directive prévoit une approche axée davantage sur les risques liés aux exigences et à la portée des EFVP. En outre, une nouvelle directive sur les pratiques relatives à la protection de la vie privée, qui explique davantage les exigences de la *Loi sur la protection des renseignements personnels* et de la Politique sur la protection de la vie privée, est entrée en vigueur le 1er avril 2010.

La vérification a comporté les phases suivantes :

Planification – de novembre 2009 à février 2010

Réalisation – de février 2010 à avril 2010

Établissement du rapport – mai 2010

1.5 Conclusion

Selon la Direction de la vérification interne d'AAC, le cadre actuel de contrôle de la gestion de la protection des renseignements personnels d'AAC nécessite quelques améliorations pour régler certains problèmes qui exposent AAC au risque accru que la collecte, l'utilisation ou la divulgation des renseignements personnels ne soient pas appropriées et à des risques éventuels de non-conformité aux dispositions de la *Loi sur la protection des renseignements personnels* et aux directives et politiques connexes du Conseil du Trésor.

Il est nécessaire d'améliorer le cadre de contrôle de la gestion dans les domaines suivants :

- gouvernance et contrôle de la protection des renseignements personnels;
- activités de formation et de sensibilisation axées sur la protection des renseignements personnels;
- utilisation du numéro d'assurance sociale (NAS);

- gestion des renseignements personnels par les tiers fournisseurs de services;
- élimination des renseignements personnels électroniques.

Les lacunes dans ces domaines sont précisées à la Section 2.0.

La vérification a déterminé que les contrôles dans d'autres domaines sont satisfaisants et a mis en évidence un certain nombre de pratiques exemplaires, notamment :

- Le Bureau de l'AIPRP a fait beaucoup de progrès au cours de la dernière année pour consolider son rôle au sein du Ministère et pour déterminer les ressources nécessaires pour respecter son mandat, notamment l'élaboration d'un certain nombre de politiques et la préparation et la tenue de séances de formation et de sensibilisation axées sur la protection des renseignements personnels pour le Ministère. Le Bureau de l'AIPRP a aussi centralisé le processus de l'EFVP et s'est assuré qu'il est administré par le Bureau de l'AIPRP de manière à ce que les EFVP soient uniformes et que la gestion des risques communs soit cohérente pour tous les programmes.
- Le Bureau de l'AIPRP respecte ses obligations en vertu de la *Loi sur la protection des renseignements personnels* relativement à la présentation au Conseil du Trésor des fichiers de renseignements personnels qui doivent être inclus dans Info Source et à la préparation du Rapport annuel au Parlement sur la *Loi sur la protection des renseignements personnels*.
- Pour les domaines visés par la vérification, y compris les deux domaines de programmes et la Direction générale des RH, les renseignements personnels sont recueillis par l'autorité compétente d'AAC et à des fins appropriées en harmonie avec l'administration du programme et du domaine fonctionnel.

L'utilisation des deux nouvelles directives sur la protection des renseignements personnels du SCT devrait permettre au Bureau de l'AIPRP d'élaborer et d'adopter une approche axée sur les risques pour gérer la protection des renseignements personnels au sein d'AAC.

1.6 Déclaration de certification

Selon l'avis professionnel du dirigeant principal de la vérification, les procédures de vérification ont été adéquates et suffisantes et des éléments probants ont été recueillis pour assurer l'exactitude de son opinion contenue dans le présent rapport.

Cette opinion se fonde sur une comparaison des conditions existantes au moment de la vérification par rapport aux critères de vérification prédéterminés convenus avec la direction. L'opinion ne porte que sur les processus examinés. Les éléments probants ont été recueillis en conformité avec la politique, les directives et les normes sur la vérification interne du CT et les procédures utilisées sont conformes aux normes professionnelles établies par l'Institut des vérificateurs internes. Les éléments probants recueillis sont suffisants pour fournir à la haute direction la justification de l'opinion fondée sur la vérification interne.

Original signé par :

_____ _____

Dirigeant principal de la vérification Date

1.7 Remerciements

Le Bureau de la vérification et de l'évaluation désire remercier les personnes qui ont participé à ce projet et, plus précisément, les employés du Ministère qui ont été interviewés et qui ont exprimé des points de vue et formulé des commentaires utiles pour cette vérification.

2.0 OBSERVATIONS DÉTAILLÉES, RECOMMANDATIONS ET RÉPONSES DE LA DIRECTION

Cette section présente les observations clés fondées sur les éléments probants et les analyses associés à la vérification et formule des recommandations pour améliorer la situation.

On s'attend à ce que la direction précise les mesures à prendre, notamment :

- un plan d'action pour aborder chaque recommandation;
- une personne chargée de la mise en œuvre du plan d'action;
- une date limite pour terminer la mise en œuvre du plan d'action.

2.1 Gouvernance et contrôle de la protection des renseignements personnels

Un organisme de gouvernance n'a pas reçu le mandat clair d'effectuer des activités de contrôle de la protection des renseignements personnels pour le Ministère et les rôles et les responsabilités liés à la protection des renseignements personnels des membres du personnel à l'extérieur du Bureau de l'AIPRP n'ont pas été clairement définis.

Pour assurer la conformité aux dispositions de la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes du SCT, AAC doit mettre en place des structures, des politiques, des systèmes et des procédures appropriés pour déléguer les responsabilités relatives à la protection des renseignements personnels, pour coordonner le travail sur la protection des renseignements personnels, pour gérer les risques liés à la protection des renseignements personnels et pour assurer la conformité aux exigences en matière de protection des renseignements personnels.

Les rôles et les responsabilités liés à la protection des renseignements personnels au sein d'AAC n'ont pas été officiellement définis et communiqués. AAC prépare actuellement un cadre de gestion de la protection des renseignements personnels visant à préciser les rôles et les responsabilités. Cependant, le cadre de gestion de la protection des renseignements personnels est actuellement aux premiers stades de mise au point et il énonce les rôles et les responsabilités du Bureau de l'AIPRP et des cadres supérieurs, mais n'énonce pas les rôles et les responsabilités des gestionnaires de programme ou d'autres employés qui gèrent les renseignements personnels. Une fois mis au point, le cadre de gestion de la protection des renseignements personnels doit être communiqué de manière appropriée pour permettre à tous les membres du personnel de comprendre leurs rôles et responsabilités relativement à la protection des renseignements personnels.

Le Comité du système d'information des entreprises (CSIE) est un organisme de

gouvernance de fait en matière de protection de la vie privée. Par exemple, dans le cadre des activités annuelles de planification et d'établissement de rapports de la GI-TI, le Bureau de l'AIPRP a présenté au CSIE un rapport sur ses domaines prioritaires et sur la politique sur les atteintes à la vie privée d'AAC. Cependant, on doit souligner que les activités de contrôle et de gouvernance en matière de protection de la vie privée, par exemple, l'examen des questions importantes ou systémiques découlant des EFVP ou des atteintes à la vie privée, n'ont pas été confiées explicitement au CSIE. En raison de cela, les conseils et les directives sur les nouvelles questions relatives à la protection des renseignements personnels liées aux plans et aux priorités du Ministère (par exemple, les questions liées à l'utilisation de tiers fournisseurs de services) sont inadéquats (voir la Section 2.3).

Puisque les rôles et les responsabilités ne sont pas définis de manière adéquate, et en raison de l'absence de directives, chaque domaine de programme doit incorporer ses propres exigences en matière de protection de la vie privée aux procédures et aux processus du programme. Par exemple, la Direction des programmes du revenu agricole (DPRA) a élaboré des directives pour le centre de contact sur les méthodes pour aborder les questions relatives à la protection des renseignements personnels avec les appelants et le Programme de paiements anticipés (PPA) a mis en place un certain nombre d'initiatives concernant la protection des renseignements personnels, notamment une politique de protection de la vie privée, le contrôle des pratiques en matière de protection des renseignements personnels des agents d'exécution et la mise à jour du manuel sur les procédures de bureau des agents de programme, et a élaboré une série de questions sur l'examen des pratiques de protection des renseignements personnels qui doivent être incorporées à la liste de vérification de la conformité.

Recommandation 1 :

Le dirigeant principal de l'information doit :

I. Mettre au point un cadre de gestion de la protection des renseignements personnels pour le Ministère qui énonce les rôles et les responsabilités en matière de protection des renseignements personnels pour tous les membres du personnel du Ministère (surtout pour les employés chargés de la réalisation de programmes), désigne un organisme de gouvernance précis responsable de la protection des renseignements personnels, et précise les directives générales qui doivent être fournies par le Bureau de l'AIPRP;
II. Élaborer une politique de la protection de la vie privée pour AAC qui respecte les exigences politiques et législatives du gouvernement fédéral, mais qui tient compte de la nature des activités d'AAC;
III. Établir un plan officiel pour offrir activement de l'aide aux domaines de programme pour s'assurer que leurs procédures et processus satisfont aux exigences en matière de protection des renseignements personnels, telles qu'énoncées dans le cadre de gestion de la protection des renseignements personnels et dans la politique de la protection de la vie privée, une fois qu'ils seront établis.

Réponses de la direction :

Le dirigeant principal de l'information accepte les trois éléments de la recommandation 1.

Plan d'action :

I. Les cadres supérieurs évaluent actuellement un cadre de gestion de la protection des renseignements personnels aux fins d'approbation,

II. On a élaboré une politique de la protection de la vie privée. La politique sera mise au point une fois que le SCT aura transmis les directives définitives sur sa politique de la protection de la vie privée révisée récemment.

III. Un plan officiel sera mis en place une fois que les documents du cadre de gestion de la protection des renseignements personnels et de la politique de la protection de la vie privée seront finalisés et on continuera d'évaluer les activités existantes.

Personne responsable : dirigeant principal de l'information

Dates limites :

I. Octobre 2010
II. Octobre 2011
III. Octobre 2011

2.2 Activités de formation et de sensibilisation axées sur la protection des renseignements personnels

Bien que le personnel d'AAC soit généralement conscient des exigences en matière de protection des renseignements personnels, les exigences précises liées aux fonctions professionnelles quotidiennes des membres du personnel d'AAC ne sont pas bien comprises.

Le Ministère doit expliquer à ses employés les politiques, les procédures et la responsabilité légale en vertu de la Loi. Bien que le Bureau de l'AIPRP ait fait beaucoup de progrès relativement aux activités de formation et de sensibilisation axées sur la protection des renseignements personnels (par exemple, le Bureau a préparé et donne des cours de formation sur la protection des renseignements personnels chaque mois, y compris une brève présentation pendant les séances d'orientation pour les nouveaux employés d'AAC, et a organisé des séances de formation sur les EFVP et sur les atteintes à la vie privée), au cours des deux derniers exercices financiers, seulement 5 % des employés d'AAC ont suivi les cours de formation sur la protection des renseignements personnels et seulement un nombre minime d'employés d'AAC ont suivi les cours de formation sur les EFVP.

Les cours de formation organisés par le Bureau de l'AIPRP énoncent des principes complexes sur la protection des renseignements personnels, mais n'expliquent pas les exigences de la *Loi sur la protection des renseignements personnels* ou des politiques et des directives du Conseil du Trésor relativement aux méthodes que les membres du personnel d'AAC doivent utiliser pour gérer les renseignements personnels. On n'a pas élaboré une stratégie de formation axée sur la protection des renseignements personnels pour les titulaires des postes au sein d'AAC qui font face à un plus grand nombre de risques inhérents liés à la protection des renseignements personnels en fonction de leurs rôles et responsabilités.

Compte tenu du fait que très peu d'employés d'AAC ont suivi les cours de formation et du fait que les séances de formation ne sont pas obligatoires et sont de haut niveau, il y a un risque accru que les renseignements personnels soient gérés de manière inappropriée.

Recommandation 2 :

Le dirigeant principal de l'information doit :

I. Élaborer une stratégie de formation sur la protection des renseignements personnels fondée sur les besoins et sur les risques;
II. Modifier la section sur la sensibilisation à la protection des renseignements personnels des séances actuelles de formation sur la protection des renseignements personnels de manière à se concentrer sur les directives pratiques et les listes de vérification mettant en évidence comment la *Loi sur la protection des renseignements personnels* et les politiques et les directives

connexes du SCT concernent les fonctions professionnelles quotidiennes des membres du personnel d'AAC.

Réponses de la direction :

Le dirigeant principal de l'information accepte les recommandations visant à élaborer une stratégie de formation sur la protection des renseignements personnels fondée sur les besoins et sur les risques et à modifier les séances de formation sur la sensibilisation à la protection des renseignements personnels.

Plan d'action :

I. Le Bureau de l'AIPRP examinera sa stratégie actuelle de formation sur la protection des renseignements personnels pour déterminer la méthode la plus efficace pour donner la formation en visant les divisions et les directions générales qui nécessitent immédiatement la formation en fonction des besoins et des risques.

II. Le Bureau de l'AIPRP examinera le matériel de formation existant pour s'assurer que les séances de formation sur la sensibilisation à la protection des renseignements personnels sont efficaces et que le contenu est pertinent et pratique pour les différentes fonctions professionnelles quotidiennes du personnel d'AAC. La mise à jour du contenu est un processus permanent pour s'assurer de tenir compte des changements.

Personne responsable : Dirigeant principal de l'information

Dates limites :

I. Octobre 2010
II. Mars 2011

2.3 Tiers fournisseurs de services

Il est nécessaire d'améliorer les contrôles visant à s'assurer que les tiers fournisseurs de services gèrent les renseignements personnels de manière appropriée dans le cadre des ententes de contribution ou des contrats.

Les renseignements personnels recueillis et utilisés par la plupart des tiers sont considérés comme étant sous le contrôle d'AAC même s'ils ne sont pas fournis à AAC lorsque les tiers administrent un programme et, par conséquent, AAC doit s'assurer dans ces cas que les renseignements personnels sont gérés conformément aux

dispositions de la *Loi sur la protection des renseignements personnels*.[2]

Il n'y a pas de directives pour les domaines de programme sur la manière de s'assurer que les tiers fournisseurs de services gèrent de manière appropriée les renseignements personnels recueillis pour le compte d'AAC. Bien que les modèles d'ententes de contribution pour les tiers fournisseurs de services contiennent des clauses portant sur les exigences élevées requises en matière de protection des renseignements personnels, les tiers fournisseurs de services ne reçoivent pas suffisamment de directives de la part des domaines de programmes sur la façon d'appliquer ces exigences aux processus et procédures du programme. Par exemple, souvent, on ne donne pas de directives sur le type d'avis de confidentialité qui doit être utilisé pour les formulaires du programme qui peuvent avoir été élaborés et peuvent être utilisés par les tiers fournisseurs de services (et qui portent le logo d'AAC).

En l'absence de directives ministérielles, les programmes établis tels que le PPA ont élaboré leurs propres processus pour les tiers fournisseurs qui, toutefois, devraient être améliorés.

Chaque année, les agents d'exécution du PPA doivent présenter une nouvelle demande pour agir à titre d'agent d'exécution du PPA. Bien que les candidats retenus soient assujettis à l'Accord de garantie d'avances, qui comporte un appendice énonçant les procédures relatives à la protection des renseignements personnels, le formulaire de demande pour ces agents d'exécution n'explique pas les méthodes de gestion des renseignements personnels et les pratiques relatives à la protection des renseignements personnels des agents d'exécution et les demandeurs ne sont pas tenus de faire part à AAC de leurs pratiques.

Actuellement, les pratiques relatives à la protection des renseignements personnels des tiers ne sont pas contrôlées ou vérifiées, sauf en cas d'accident ou de violation. En 2008, il y a eu une grave atteinte à la vie privée attribuable aux pratiques relatives à la protection des renseignements personnels inappropriées d'un tiers fournisseur de services. Bien que l'Unité de la vérification des bénéficiaires (UVB) du Centre d'excellence des programmes soit actuellement responsable des vérifications de la conformité des bénéficiaires pour le Ministère, le cadre actuel de gestion des risques associés aux bénéficiaires utilisé par l'Unité de la vérification des bénéficiaires ne permet pas de considérer la nature des renseignements personnels recueillis et utilisés ou des pratiques relatives à la protection des renseignements personnels des tiers pour l'évaluation des risques liés aux tiers fournisseurs de services. En outre, l'Annexe (au

[2]. Les lignes directrices du SCT énoncent : « *on considère que des renseignements personnels relèvent d'une institution fédérale lorsque ladite institution est autorisée à accorder ou à refuser l'accès à ces renseignements, à décider de leur utilisation et, sous réserve de l'approbation de l'archiviste fédéral, à en disposer. On présume que les renseignements personnels qui sont en la possession de l'institution ou sous sa garde, qu'il s'agisse de l'administration centrale, des bureaux régionaux, auxiliaires ou autres, au Canada ou à l'étranger, relèvent de cette institution à moins de preuve du contraire*. » AAC a enregistré des fichiers de renseignements personnels et des autorisations de disposition de documents pour ces programmes, ce qui indique qu'AAC a le contrôle de fait des renseignements personnels. En outre, les ententes avec les tiers fournisseurs mettent en évidence qu'AAC a le droit d'accéder aux renseignements.

modèle d'ET pour les vérifications des bénéficiaires) qui énonce les critères de vérification minimaux pour aider le vérificateur à élaborer le programme de vérification de manière à atteindre les objectifs de vérification ne comporte pas de considérations sur la protection des renseignements personnels qui peuvent être appliquées aux vérifications des tiers fournisseurs de services.

Compte tenu du fait qu'il n'y a pas suffisamment de directives pour les domaines de programme et pour les tiers fournisseurs, les tiers peuvent ne pas être au courant de leurs responsabilités relativement à la gestion des renseignements personnels et des méthodes pour appliquer ces exigences en matière de protection des renseignements personnels à l'administration quotidienne de leurs programmes.

Recommandation 3a :

Le dirigeant principal de l'information doit :

Établir des directives claires sur la responsabilité des programmes d'AAC pour s'assurer que les tiers respectent les exigences de la *Loi sur la protection des renseignements personnels*.

Élaborer des directives que les gestionnaires de programmes peuvent fournir aux tiers sur les méthodes pour appliquer les exigences en matière de protection des renseignements personnels énoncées dans les ententes de contribution et les contrats avec AAC aux processus des programmes.

Réponses de la direction :

AAC a fait beaucoup d'efforts pour s'assurer que les contrats conclus avec les tiers fournisseurs de services énoncent les exigences en matière de protection des renseignements personnels appropriées. Toutefois, le dirigeant principal de l'information accepte les deux éléments de la recommandation 3.

Il peut arriver qu'un tiers n'ait pas à se conformer à la Loi sur la protection des renseignements personnels. Il revient à AAC de s'y conformer et de s'assurer que le tiers agit d'une manière conforme aux ententes conclues, de façon à honorer les obligations ministérielles en vertu de la Loi sur la protection des renseignements personnels.

Avant d'établir des directives et des conseils, le Bureau de l'AIPRP doit définir clairement le rôle de la *Loi sur la protection des renseignements personnels* pour les services fournis par les tiers fournisseurs et l'action réciproque entre les dispositions législatives du gouvernement fédéral et les dispositions législatives des provinces et les directives du secteur privé pour les contrats conclus par AAC avec les provinces et les tiers.

Plan d'action **:**

I. Le Bureau de l'AIPRP doit définir l'approche à la protection des renseignements personnels pour les services fournis par les tiers et ensuite établir des directives pour les programmes.
II. Après avoir établi les directives, le Bureau de l'AIPRP doit élaborer des lignes directrices qui peuvent être transmises aux tiers fournisseurs (lorsqu'il y a lieu de le faire). Pour le moment, AAC continuera à formuler des commentaires pour les ententes individuelles par l'entremise du Centre d'excellence des programmes et au moyen du processus de l'équipe « tigre ».

Personne responsable : Dirigeant principal de l'information

Dates limites :

I. Mars 2011
II. Mars 2011

Recommandation 3b :

Le SMA, Direction générale des programmes financiers pour l'agriculture, doit élaborer une approche fondée sur les risques pour vérifier que les tiers fournisseurs de services respectent les exigences en matière de protection des renseignements personnels, notamment intégrer des considérations sur la protection des renseignements personnels dans le cadre axé sur les risques de l'Unité de la vérification des bénéficiaires du Centre d'excellence des programmes pour la sélection des vérifications des bénéficiaires des tiers fournisseurs de services et dans l'énoncé des travaux pour les vérifications des bénéficiaires des tiers fournisseurs de services.

Réponses de la direction :

Le SMA, Direction générale des programmes financiers pour l'agriculture (DGPFA), accepte la recommandation et a pris récemment un certain nombre de mesures permettant de vérifier si les tiers fournisseurs respectent les exigences en matière de protection des renseignements personnels. Un projet sur la protection des renseignements personnels réalisé entre novembre 2008 et le 31 mars 2009 a permis, entre autres choses, d'établir des nouvelles directives pour les agents d'exécution du PPA et de déléguer à la DGPFA la responsabilité de vérifier si les tiers fournisseurs respectent les exigences en matière de protection des renseignements personnels.

Plan d'action :

I. L'Unité de la vérification des bénéficiaires du Centre d'excellence des programmes intégrera les clauses nécessaires, qui ont été examinées par la division de l'AIPRP d'AAC, qui a aussi formulé des commentaires, pour répondre aux préoccupations du bureau de l'AIPRP au sujet de la politique sur les bénéficiaires d'AAC, du processus d'intervention pour divulgation illicite, fraude, atteinte à la vie privée ou appropriation illicite, du processus de recouvrement des paiements excédentaires pour le redressement après vérification, du cadre de gestion des risques associés aux bénéficiaires et de l'énoncé des travaux pour la vérification des bénéficiaires.

Personne responsable : SMA, DGPFA

Date limite : Mars 2011

2.4 Utilisation du numéro d'assurance sociale (NAS)

AAC a fait beaucoup d'efforts au cours des dernières années pour modifier ses processus afin de s'assurer qu'ils sont conformes à la directive sur le numéro d'assurance sociale du SCT. Toutefois, un certain nombre de pratiques ne respectent pas la directive.

Le NAS est considéré comme un renseignement très sensible et, s'il n'est pas protégé, peut donner lieu au vol d'identité ou à d'autres activités illégales. La directive énonce que le NAS doit être obtenu et utilisé uniquement à des fins autorisées; dans le cas d'AAC, le NAS est utilisé uniquement pour les programmes qui comportent des avantages imposables. Le NAS peut être obtenu et utilisé uniquement pour communiquer ces avantages imposables à l'Agence du revenu du Canada (ARC).

Les pratiques actuelles observées au sein d'AAC qui ne respectent pas l'esprit de la directive sur le NAS du SCT sont notamment :

- La DPRA utilise le nom, l'adresse et le NAS des producteurs pour créer un identificateur unique (c.-à-d. le NIP du producteur).
- Le NAS du producteur apparaît sur la page couverture du dossier papier conservé par la DPRA.
- Pour obtenir un code d'activation pour accéder au site Web Mon compte, les producteurs doivent fournir le NAS (en plus du NIP et du code postal).
- Puisque le NIP créé par la DPRA n'est pas utilisé pour tout le Ministère, le NAS est un des renseignements qui sont partagés entre différents programmes pour faire correspondre le nom du producteur aux programmes. Par exemple, la DPRA et la Direction générale des services agroenvironnementaux ont partagé ce renseignement.
- Des programmes d'AAC tels que le Programme de transition pour les exploitations porcines demandent le NAS aux producteurs au moment de la présentation de la demande même si la collecte du NAS pour les personnes qui n'obtiennent pas le financement ne respecte pas la directive du SCT, surtout pour un programme tel que le PTEP dans le cadre duquel un peu moins de la moitié des personnes qui s'inscrivent au programme n'obtiennent pas le financement d'AAC.

Recommandation 4a :

Le dirigeant principal de l'information doit élaborer des directives pour AAC qui satisfont aux exigences de la directive du SCT sur la collecte, l'utilisation et la conservation du NAS.

Réponses de la direction :

Le dirigeant principal de l'information accepte la recommandation.

Plan d'action :

I. Le Bureau de l'AIPRP communiquera les directives du SCT sur le NAS et sur l'utilisation appropriée par AAC-AAFC

Personne responsable : Dirigeant principal de l'information

Date limite : Décembre 2010

Recommandation 4b :

Le SMA, Direction générale des programmes financiers pour l'agriculture, doit s'assurer que le NAS est éliminé en temps opportun des processus, des fichiers et des systèmes de la DGPFA lorsqu'il n'est plus nécessaire (par exemple, les dossiers papier de la DPRA, les producteurs qui n'ont pas obtenu le financement dans le cadre des programmes d'AAC).

Réponses de la direction :

Le SMA, Direction générale des programmes financiers pour l'agriculture, convient qu'il ne faut pas conserver les NAS qui ne sont plus nécessaires.

Plan d'action :

I. Le NAS du producteur n'apparaît plus sur la page couverture du dossier papier conservé dans la salle des dossiers de la DPRA.
II. Pour les dossiers papier qui sont conservés, le NAS figurant sur la page couverture du dossier sera effacé.
III. Pour les nouveaux systèmes Agri-stabilité et Agri-investissement, si les clients ne présentent aucune demande pendant deux ans et n'ont reçu aucun paiement, le NAS sera éliminé.
IV. La DPRA peut archiver les bases de données des programmes qui ont été annulés. La DPRA prévoit restreindre davantage l'accès aux bases de données des programmes qui doivent être annulés.

Personne responsable : SMA, DGPFA

Dates limites :

I. Terminé
II. Mars 2011
III. Mars 2013
IV. Mars 2011

2.5 Programme sur l'excellence du service d'AAC

On a effectué des EFVP pour un grand nombre de différents éléments du programme sur l'excellence du service (programme), mais on n'a pas effectué l'EFVP du programme dans son ensemble.

Les EFVP doivent être effectuées pour les initiatives comportant des renseignements personnels; le fait d'effectuer une EFVP à un stade précoce permet de s'assurer que les exigences en matière de protection des renseignements personnels sont prises en considération de manière appropriée pendant la phase de définition et d'élaboration des exigences.

Dans le cadre du programme sur l'excellence du service d'AAC, qui vise à regrouper et à intégrer les services, AAC continue de travailler à un carrefour pour les producteurs (c.-à-d. une base de données commune pour tous les producteurs) qui doit être utilisé pour tous les programmes du programme sur l'excellence du service. Les données de base sur un demandeur seront disponibles pour tous les programmes participants.

Le regroupement et l'intégration des services dans le cadre du programme sont une activité importante qui soulève des nouvelles questions sur la protection des renseignements personnels, non seulement pour les éléments du programme, mais aussi pour le programme dans son ensemble.

Les risques précis liés à la protection des renseignements personnels pour le programme n'ont pas encore été déterminés, mais les exigences de la *Loi sur la protection des renseignements personnels* qui doivent être prises en considération pendant la phase d'élaboration du programme sont notamment :

- Les renseignements personnels recueillis concernent directement un programme ou une activité (on a précisé l'autorité compétente) et ils sont obtenus directement de la personne concernée (sauf quelques exceptions) et on a donné l'avis approprié.
- Les renseignements personnels sont utilisés et divulgués uniquement aux fins pour lesquelles ils ont été recueillis, sauf si la personne concernée donne son consentement ou si l'utilisation est autorisée en vertu de la *Loi sur la protection des renseignements personnels*.

AAC a élaboré un cadre de protection des renseignements personnels préliminaire pour le programme afin de répondre aux préoccupations et aux questions au sujet de la protection des renseignements personnels qui peuvent découler de la conception et de la mise en œuvre. Le cadre indique que des EFVP ont déjà été effectuées pour un grand nombre de différents éléments du programme et que toute préoccupation mise en évidence doit être intégrée à l'EFVP du programme. Toutefois, il est important, pour s'assurer de déterminer et d'atténuer tous les risques de manière appropriée, que l'EFVP du programme évalue les conséquences potentielles sur la protection des renseignements personnels du programme dans son ensemble et non seulement des

éléments individuels puisque l'interaction de ces éléments soulève d'autres questions liées à la protection des renseignements personnels. Par exemple, si la base de données commune pour tous les producteurs est disponible pour un certain nombre de programmes, l'échange de données peut présenter des risques liés à la protection des renseignements personnels si les renseignements personnels contenus dans la base de données commune pour tous les producteurs ont été recueillis à des fins précises, mais sont ensuite utilisés par d'autres programmes pour d'autres fins qui normalement nécessiteraient le consentement du producteur.

Recommandation 5 :

Le SMA, Direction générale des programmes financiers pour l'agriculture, doit s'assurer d'effectuer une EFVP à un stade précoce pour le programme sur l'excellence du service dans son ensemble qui doit être ensuite mise à jour aux étapes clés de conception et de mise en œuvre du programme.

Réponses de la direction :

Le SMA, Direction générale des programmes financiers pour l'agriculture, accepte la recommandation. On a effectué une analyse des facteurs relatifs à la vie privée pour déterminer la méthode la plus efficace pour préciser et régler les problèmes liés à la protection des renseignements personnels. En fonction du cadre, on a déterminé que la meilleure méthode était d'effectuer deux différentes évaluations des facteurs relatifs à la vie privée (EFVP), une globale et une générique.

Plan d'action :

I. L'EFVP globale a été effectuée, sauf pour le volet du Système de prestation de subventions et de contributions qui sera terminée d'ici mars 2011.
II. L'EFVP générique comprendra tous les programmes de subventions et de contributions non liés à la gestion des risques de l'entreprise (GRE). La DGPFA et le Bureau de l'AIPRP continuent à collaborer et, s'il y a lieu, ils analyseront un plan pour éviter ou atténuer les conséquences négatives qui sera ajouté aux EFVP au fur et à mesure que les éléments du programme pour l'excellence du service seront développés.

.

Personne responsable : SMA, DGPFA

Dates limites :

I. Mars 2011
II. Mars 2011

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

Le Bureau de l'AIPRP a fait beaucoup de progrès pour centraliser le processus de l'EFVP pour s'assurer que toutes les activités liées à l'EFVP sont effectuées par l'entremise du Bureau de l'AIPRP. Cependant, les décisions d'effectuer ou non une EFVP n'ont pas été documentées et, en raison du manque de ressources et d'intérêt pour les EFVP au Bureau de l'AIPRP, les approbations n'ont pas été obtenues en temps opportun et on a négligé d'assurer le suivi pour déterminer si les risques ont été atténués de manière appropriée.

Les EFVP doivent être effectuées pour les initiatives comportant des renseignements personnels et l'examen des EFVP en temps opportun et les mesures d'atténuation des risques déterminés permettent de s'assurer que les domaines de programmes ont mis en place les contrôles appropriés pour protéger les renseignements personnels.

La décision d'effectuer ou non une EFVP n'est pas officiellement documentée, puisque le Bureau de l'AIPRP n'a pas été consulté pour les domaines de programme de la DGPFA pour lesquels on a déterminé qu'une EFVP n'est pas nécessaire.

Dans certains cas, il y a eu des retards importants relativement à l'examen et à l'approbation des EFVP pour les domaines de programme examinés (PPA, DPRA, Agri-stabilité, Agri-investissement) et pour la Direction générale des ressources humaines. Plus précisément, l'EFVP effectuée sur le SMMEA dans le cadre d'une EFVP pour le renouvellement des programmes en 2006 n'a pas encore été examinée ou approuvée par le Bureau de l'AIPRP.

On a élaboré des plans d'action pour les EFVP qui ont été examinés par le Bureau de l'AIPRP. Cependant, le Bureau ou d'autres organismes de surveillance du ministère n'ont pas déterminé la mesure dans laquelle les risques mis en évidence on été atténués par les domaines de programme.

Les lacunes liées à l'achèvement, à l'évaluation et au suivi des EFVP peuvent avoir pour conséquence que les risques liés à la protection des renseignements personnels ne sont pas évalués de manière appropriée, que les exigences de la politique ne sont pas respectées et que des leçons sur les risques et les problèmes communs et sur les mesures d'atténuation les plus efficaces n'ont pas été apprises et échangées.

Le Bureau de l'AIPRP a élaboré une directive sur les EFVP et les procédures connexes qui explique le processus pour les EFVP, y compris les rôles et les responsabilités, qui, toutefois, n'a pas encore été approuvée et qui doit être mise à jour en fonction de la nouvelle directive sur les EFVP du SCT.

Recommandation 6 :

Le dirigeant principal de l'information doit :

I. Finaliser la directive sur les EFVP d'AAC et les procédures connexes pour s'assurer de prendre en compte les exigences de la nouvelle directive sur les EFVP du SCT et de désigner clairement les personnes responsables d'assurer le suivi des EFVP pour déterminer si les risques ont été atténués de manière appropriée.
II. Viser la réduction du nombre d'EFVP qui doivent être examinées et approuvées.

Réponses de la direction :

Le dirigeant principal de l'information accepte les deux éléments de la recommandation 6.

Plan d'action :

I. On élabore une directive sur les EFVP d'AAC qui sera mise à jour lorsque le SCT communiquera les lignes directrices définitives sur la nouvelle directive sur les EFVP.
II. Le Bureau de l'AIPRP a proposé une approche pour réduire le nombre d'EFVP qui doivent être approuvées et continue de la modifier selon les besoins.

Personne responsable : Dirigeant principal de l'information

Dates limites :

I. Mars 2011
II. Mars 2011

2.7 Conservation des renseignements personnels électroniques

Les renseignements électroniques qui peuvent inclure des renseignements personnels ne sont généralement pas éliminés conformément aux calendriers d'autorisation de disposition de documents (ADD).

On doit conserver les renseignements personnels seulement pour le temps nécessaire et conformément aux autorisations de disposition de documents approuvées.

Les bases de données telles que le système du service à la clientèle (SSCC) du Compte de stabilisation du revenu net (CSRN) utilisé par la DPRA et PeopleSoft utilisé pour les ressources humaines conservent des dossiers électroniques après les dates de disposition et des renseignements personnels qui ne sont plus nécessaires sont conservés dans les systèmes partagés par la DPRA, le PPA et le SMMEA au lieu d'être éliminés.

La conservation des renseignements personnels qui ne sont plus nécessaires aux fins pour lesquelles ils ont été recueillis fait augmenter le risque d'utilisation ou de divulgation de renseignements personnels non autorisée et peut porter atteinte à la vie privée.

Le filtrage des renseignements personnels est très difficile pour les systèmes complexes. Cependant, il peut être mis en œuvre plus rapidement pour les données entreposées dans les systèmes partagés. On devrait intégrer aux procédures du programme la disposition régulière des renseignements personnels entreposés dans les systèmes partagés.

Recommandation 7 :

Le dirigeant principal de l'information doit établir un plan officiel pour offrir activement de l'aide aux domaines de programme pour mettre à jour leurs calendriers de disposition et pour s'assurer que les dossiers électroniques sont éliminés conformément à ces calendriers.

Réponses de la direction :

Le dirigeant principal de l'information accepte la recommandation.

Plan d'action :

I. La DGSI doit transmettre aux directions générales le calendrier de conservation et de disposition existant et aider les directions générales pendant le processus de disposition.
II. La DGSI doit organiser des réunions avec toutes les directions générales pour entamer des discussions à l'échelon des cadres supérieurs.
III. Répéter ce processus périodiquement.

Personne responsable : Dirigeant principal de l'information

Dates limites :

I. Octobre 2010
II. Janvier 2011
III. Permanent