Environnement et Changement climatique Canada
Environment and Climate Change Canada

Revue et analyse comparative de la gestion de la protection des renseignements personnels

Direction générale de la vérification et de l'évaluation

Décembre 2015

Canada

Liste des acronymes

AIPRP	Accès à l'information et protection des renseignements personnels
CSPRP	Cadre stratégique pour la protection des renseignements personnels
DA	Dotation accélérée
DPV	Dirigeant principal de la vérification
DGRH	Direction générale des ressources humaines
DGSM	Direction générale des services ministériels
DGVE	Direction générale de la vérification et de l'évaluation
EC	Environnement et Changement climatique Canada
ÉFVP	Évaluation des facteurs relatifs à la vie privée
FRP	Fichier de renseignements personnels
GI	Gestion de l'information
SCT	Secrétariat du Conseil du Trésor
TI	Technologies de l'information

Préparé par l'équipe de la vérification et de l'évaluation

Remerciements

L'équipe de la revue, qui est formée de Sophie Lalonde, chef d'équipe, sous la direction de Stella Line Cousineau, tient à remercier tous ceux et celles qui ont contribué à ce projet et lui ont fait part de leurs commentaires et de leurs observations dans le cadre de cette revue.

Contrôle des versions du document

Nom du fichier :	Revue et analyse comparative de la gestion de la protection des renseignements personnels.docx
Date :	22 décembre 2016

Table des matières

SOMMAIRE

La revue et l'analyse comparative de la gestion de la protection des renseignements personnels sont effectuées dans le cadre du Plan ministérielle de vérification et d'évaluation axé sur le risque de 2013 approuvé par le sous-ministre, d'après la recommandation du Comité consultatif externe de vérification.

En 2012, Environnement et Changement climatique Canada (ECCC) a élaboré et mis en œuvre un cadre stratégique pour la protection des renseignements personnels (CSPRP) doté d'éléments d'appui tel que les directives et de procédures. À la suite d'un cas d'atteinte à la vie privée, la direction a procédé en 2013 à une évaluation de certains processus opérationnels.

En 2013 également, la haute direction a demandé que la Direction générale de la vérification et de l'évaluation (DGVE) effectue une revue du cadre de gestion et des principaux processus de gestion relatifs à la protection des renseignements personnels que détient ECCC et compare ces processus à ceux de ministères fédéraux semblables.

Dans l'ensemble, la revue a confirmé que les politiques et les processus nécessaires pour la gestion de la protection des renseignements personnels sont en place et qu'ils sont essentiellement conformes à tous les éléments de la Politique sur la protection de la vie privée du Secrétariat du Conseil du Trésor (SCT). Le Cadre stratégique de protection des renseignements personnels d'ECCC prévoit les rôles et les responsabilités ainsi que les processus, comme l'évaluation des facteurs relatifs à la vie privée (ÉFVP) et le protocole en cas d'atteinte à la vie privée. La revue a confirmé que les renseignements personnels des activités de dotation et d'approvisionnement ne sont recueillis que pour les besoins de programmes précis.

Depuis l'évaluation de la gestion, de nombreuses séances d'information ont été offertes aux employés s'occupant de dotation et d'approvisionnement, et presque tous les employés (plus de 6 000) ont suivi la séance obligatoire en ligne sur la sensibilisation à la sécurité, qui comprend un module sur la protection des renseignements personnels. Le Ministère a également installé un logiciel de chiffrement de disque sur plus de 1 900 ordinateurs portatifs pour assurer la sécurité de l'information. L'équipe de vérification a toutefois relevé les domaines suivants dans lesquels les pratiques et les processus pourraient être améliorés :

- les pratiques et la méthode de collecte des numéros d'assurance sociale (NAS) dans le contexte du Cadre stratégique de protection des renseignements personnels;
- la surveillance des mesures des évaluations des facteurs relatifs à la vie privée.

Recommandation 1 :
Le directeur général du Secrétariat ministériel devrait revoir le Cadre stratégique de protection des renseignements personnels d'ECCC pour mieux définir les exigences relatives à la collecte, à l'utilisation et à la communication des numéros d'assurance sociale.

Recommandation 2 :
Le directeur général du Secrétariat ministériel devrait améliorer sa méthode de surveillance des évaluations des facteurs relatifs à la vie privée qui sont exigées et effectuées.

Réponse de la direction
La direction accepte ces recommandations. La réponse détaillée de la direction se trouve à la section 3 du présent rapport.

1. INTRODUCTION ET CONTEXTE

La revue et l'analyse comparative de la gestion de la protection des renseignements personnels faisaient partie du Plan intégré de vérification et d'évaluation axé sur le risque de 2013 qui a été approuvé par le sous-ministre, sur recommandation du Comité consultatif externe de vérification (CCEV).

Exigences de gouvernement en matière de protection des renseignements personnels

On entend par renseignements personnels les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable. Le gouvernement du Canada s'est engagé à respecter la vie privée des personnes en ce qui a trait aux renseignements personnels relevant des institutions fédérales.

La *Loi sur la protection des renseignements personnels,* le *Règlement sur la protection des renseignements personnels* et la série de politiques du Secrétariat du Conseil du Trésor (SCT) sur la protection des renseignements personnels appuient l'engagement du gouvernement d'établir des normes claires pour la collecte, l'utilisation, la communication et la conservation des renseignements personnels, ainsi que des pratiques exemplaires ou des mesures de contrôle efficaces pour la promotion de la protection des renseignements personnels et l'application de la législation et de la réglementation qui s'y rattachent.

Gestion de la protection des renseignements personnels à Environnement et Changement climatique Canada

Le **coordonnateur de l'Accès à l'information et de la protection des renseignements personnels (AIPRP)** qui, à ECCC, est le directeur général du Secrétariat ministériel, est chargé :

- de veiller à ce que des mesures et des processus adéquats soient mis en vigueur pour la création, la collecte, la conservation, l'exactitude, l'utilisation, la communication ou la destruction des renseignements personnels;
- d'élaborer un plan en cas d'atteintes à la vie privée;
- d'établir des procédures pour le maintien d'un registre des nouvelles utilisations et communications afin que les fichiers de renseignements personnels (FRP) restent à jour;
- d'informer les employés de leurs responsabilités en matière de gestion des renseignements personnels;
- de déléguer l'autorisation de recueillir et de créer des renseignements personnels.

Il incombe aux **gestionnaires de programme** :

- d'informer la Division de l'AIPRP lorsqu'un programme ou activité est créé ou a subi des modifications importantes;
- de limiter la collecte de renseignements personnels à ce qui est directement lié à des programmes ou à des activités;

- de lancer une nouvelle évaluation des facteurs relatifs à la vie privée (ÉFVP) lorsqu'un programme ou une activité est créé ou a subi des modifications importantes.

Enfin, tous les **employés** ont le devoir de protéger la confidentialité des renseignements personnels qu'ils gèrent.

Tout au long de l'exécution de son programme, ECCC recueille différents types de renseignements personnels[1], comme l'âge, la situation de famille, la race, l'origine nationale ou ethnique, le dossier médical, le casier judiciaire, les antécédents de travail et les numéros d'identification (p. ex. le numéro d'assurance sociale, le code d'identification de dossier personnel).

Conformément aux exigences du gouvernement en matière de protection des renseignements personnels, EC a produit en 2012 un cadre stratégique de protection des renseignements personnels (CSPRP) qui inclut des directives internes sur l'évaluation des facteurs relatifs à la vie privée, les pratiques relatives à la protection de la vie privée et le protocole en cas d'atteinte à la vie privée.

Évaluation de la gestion de la protection des renseignements personnels

En réponse à un cas d'atteinte à la vie privée, la Direction générale des services ministériels (DGSM) d'ECCC, en collaboration avec le Secrétariat ministériel, a en 2013 évalué les pratiques relatives au traitement des renseignements personnels ou de nature délicate. Cette évaluation a porté sur les activités de dotation, financières et d'approvisionnement.

L'évaluation a cerné 124 recommandations qui pourraient être mises en œuvre rapidement, et ont été suivies par plusieurs mesures de gestion. Au moment où s'effectue la présente revue, 90 de ces 124 recommandations ont été mises en œuvre et 34 ont été reportées en attendant la mise en œuvre d'initiatives de plus grande ampleur, comme le système financier SAP et la réorganisation des processus opérationnels des RH. En réponse à l'évaluation, ECCC a mis en place de nombreuses mesures de contrôle qui contribueront à protéger davantage les renseignements personnels, comme l'installation d'un logiciel de chiffrement sur les ordinateurs portatifs.

Les résultats de l'évaluation susmentionnée ont été examinés pendant la planification et l'établissement de la portée de la présente revue.

2. OBJECTIFS ET PORTÉE

Objectifs

Ce projet comprenait deux objectifs :

- procéder à la revue pour déterminer si le cadre stratégique et de gestion nécessaire et les principaux processus de gestion des renseignements personnels d'ECCC sont en place;

[1] Cadre stratégique de protection des renseignements personnels d'EC − 2 novembre 2012.

- procéder à une comparaison des processus de collecte de renseignements personnels d'ECCC et des processus d'autres ministères dont la taille et le mandat sont similaires à ceux d'ECCC.

Les résultats détaillés de l'analyse comparative de la gestion de la protection des renseignements personnels sont présentés dans un rapport distinct à l'annexe 2 (dans laquelle les résultats d'ECCC sont ceux du ministère n^{o} 7). Le rapport de l'analyse comparative présente les résultats des sept ministères participants, mais non une analyse des résultats d'ECCC en particulier, alors que le rapport de la revue est présenté du point de vue d'ECCC.

Portée de la revue

La revue a portée sur les responsabilités du personnel et du coordonnateur de l'AIPRP en ce qui concerne la gestion de la protection des renseignements personnels, ainsi que sur les pratiques des directions générales habilitantes qui traitent le plus de renseignements personnels (c.-à-d. les processus de dotation et d'approvisionnement). Elle n'a pas portée sur :

- les demandes d'accès à l'information et la correction de renseignements personnels (vérification de l'exactitude) puisque les risques à ce sujet ont été considérés comme faibles pendant la phase de planification de la DGEV;
- les renseignements commerciaux sensibles, puisqu'ils ne sont pas couverts par la *Loi sur la protection des renseignements personnels*;
- la validation des assertions de la direction concernant l'état d'avancement de la mise en œuvre des 124 recommandations (de l'évaluation de 2013).

Le travail sur le terrain pour la revue et pour l'analyse comparative n'a été effectué que dans la région de la capitale nationale.

Énoncé de conformité

La présente revue est conforme aux *Normes relatives à la vérification interne au sein du gouvernement du Canada*, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité, appliquée dans le contexte d'une revue.

Selon notre jugement professionnel, tout comme les preuves recueillies, des procédures de vérification suffisantes et appropriées ont été appliquées pour appuyer les conclusions décrites dans le présent rapport. Toutefois, les contrôles n'ont pas été mis à l'essai. Les conclusions reposent sur la comparaison des situations telles qu'elles étaient à la fin du travail sur le terrain (janvier 2015) et des critères de la revue.

3. CONSTATATIONS ET RECOMMANDATIONS

Dans l'ensemble, le cadre stratégique et les principaux processus de gestion de la protection des renseignements personnels nécessaires sont en place. Par exemple, ECCC a un Cadre stratégique de protection des renseignements personnels (CSPRP) en bon état qu'il a fait connaître dans tout le Ministère. Depuis que la direction a procédé à sa propre évaluation en 2013, un certain nombre de mesures de protection et de contrôle connexes ont été mises en œuvre ou améliorées.

De plus, l'analyse de comparaison a établi qu'EC est le seul ministère qui ait pleinement mis en œuvre son CSPRP, qui couvre les principales lignes directrices du SCT. ECCC a également établi la gouvernance nécessaire et communiqué les rôles et les responsabilités aux employés par de la sensibilisation et de la formation.

L'analyse comparative a toutefois également montré qu'il pourrait être bon de procéder à une analyse plus approfondie des renseignements personnels recueillis dans le cadre des processus de dotation et d'approvisionnement, puisqu'il s'est avéré qu'ECCC recueille le plus d'information. La revue a également cerné deux domaines dans lesquels des améliorations sont possibles : les directives sur les processus associés à la collecte des numéros d'assurance sociale (NAS) et la surveillance des évaluations des facteurs relatifs à la vie privée (ÉFVP).

3.1 Cadre stratégique de protection des renseignements personnels

La Politique du SCT sur la protection de la vie privée exige que les responsables des institutions établissent des pratiques de gestion pour assurer une application uniforme de la *Loi sur la protection des renseignements personnels*. Pour s'acquitter de cette obligation, EC a élaboré et mis en œuvre CSPRP, qui présente les processus en détail, y compris les rôles et les responsabilités de tous ceux qui participent à la gestion des renseignements personnels. Le CSPRP a été mis en œuvre en novembre 2012, le dernier document du CSPRP mis en œuvre étant le protocole en cas d'atteinte à la vie privée, en septembre 2013.

L'analyse comparative a montré qu'ECCC est un des six ministères (sur sept) qui ont élaboré un CSPRP, appuyé par l'ensemble suivant de directives internes et d'un protocole :

- directive interne sur les ÉFVP;
- processus interne d'approbation des ÉFVP;
- directive interne sur les pratiques relatives à la protection de la vie privée;
- protocole en cas d'atteinte à la vie privée.

La Politique du SCT sur la protection de la vie privée exige aussi que les ministères respectent les conditions particulières relatives à l'utilisation des NAS ainsi que les restrictions imposées à leur collecte, à leur utilisation et leur communication. Bien qu'EC ait mis en œuvre un CSPRP qui inclut la plupart des exigences de la *Loi sur la protection des renseignements personnels* et des politiques du SCT, les processus de collecte, d'utilisation et de communication des NAS ne sont pas définis.

Une des recommandations de l'évaluation de la gestion était de modifier le processus de collecte et de transmission des renseignements personnels (comme les NAS). En réponse à cette recommandation, la DGRH a modifié ses processus de collecte et de transmission de l'information délicate et demande maintenant ce genre de renseignement au téléphone, ce qui élimine les traces écrites éventuelles. Cependant, il n'est pas question de ce nouveau processus dans le CSPRP; les employés qui ne sont pas au courant peuvent par conséquent procéder de manière inappropriée pour recueillir

des renseignements personnels. Cela peut aussi accroître le risque de diffusion délibérée ou même accidentelle de NAS.

Recommandation 1 :
Le directeur général du Secrétariat ministériel devrait revoir le Cadre stratégique de protection des renseignements personnels d'ECCC pour mieux définir les exigences relatives à la collecte, à l'utilisation et à la communication des numéros d'assurance sociale.

Réponse de la direction
D'accord. Le DG du Secrétariat ministériel procédera à un examen du Cadre stratégique de protection des renseignements personnels d'ECCC, et le mettra à jour. Cet examen visera à améliorer les directives du Ministère en ce qui concerne la collecte, l'utilisation et la communication des NAS.

3.2 Gouvernance, rôles et responsabilités

Selon la *Loi sur la protection des renseignements personnels*, les responsables des institutions peuvent choisir de déléguer leurs pouvoirs, attributions ou fonctions. De plus, s'ils décident de le faire, une ordonnance de délégation de pouvoirs doit être signée et les cadres ou les employés à qui les attributions sont déléguées doivent être d'un niveau hiérarchique approprié à la tâche.

L'analyse comparative a démontré que les sept ministères ont tous une ordonnance de délégation de pouvoirs officielle. À ECCC, cette ordonnance a été approuvé en septembre 2013; il délègue tous les pouvoirs au sous-ministre, au sous-ministre délégué, au directeur général du Secrétariat ministériel, au directeur de l'AIPRP et au gestionnaire de l'AIPRP pour toutes les responsabilités pouvant être attribuées en matière de protection des renseignements personnels. Il existe aussi une structure organisationnelle plus précise pour le groupe de l'AIPRP et une équipe distincte se consacre maintenant aux atteintes à la vie privée.

Le SCT a de plus affecté une série de responsabilités aux cadres de direction et aux cadres supérieurs qui gèrent des programmes ou des activités exigeant la création et le traitement de renseignements personnels. Ces responsabilités sont énoncées à la fois dans la Politique du CT sur la protection de la vie privée et dans la Directive sur les pratiques relatives à la protection de la vie privée.

Bien qu'ECCC n'ait pas établi d'organisme de supervision particulier, comme le recommandent l'orientation et les critères connexes du Cadre de responsabilisation de gestion (CRG), dans l'ensemble, le Ministère a établi les principaux éléments de la gouvernance qui définissent les rôles et les responsabilités, ainsi que des directives et des processus plus détaillés. Ceux-ci se trouvent dans le Cadre stratégique de protection des renseignements personnels et sont communiqués par différentes méthodes, comme les séances de formation et de sensibilisation, le site intranet de l'AIPRP, ECollab et Nouvelles@ECCC.

3.3 Collecte de renseignements personnels et information à fournir

Conformément à l'article 4 de la *Loi sur la protection* des *renseignements personnels*, une institution ne peut recueillir de renseignements personnels que s'ils sont directement liés à une activité ou à un programme. De plus, lorsque l'information est recueillie en vertu du paragraphe 5(2) de la *Loi*, la personne qu'elle concerne doit aussi être informée des fins auxquelles elle est destinée. La Politique du CT sur la protection de la vie privée prévoit en outre que les ministères doivent veiller à ce que des dispositions appropriées pour la protection des renseignements personnels soient incluses dans les contrats ou les ententes pouvant donner lieu à la circulation intergouvernementale ou transfrontalière de renseignements personnels.

La revue a confirmé que les renseignements personnels recueillis pour les activités de dotation et d'approvisionnement ne le sont que pour les besoins de programmes opérationnels. De plus, ECCC a adopté pour les activités de dotation et d'approvisionnement un avis de non-responsabilité qui informe aussi les gestionnaires de leurs obligations en matière de protection des renseignements personnels.

À la suite de l'évaluation de la gestion, les mesures de contrôle supplémentaires suivantes ont été mises en œuvre pour la collecte et la transmission de renseignements personnels pour les besoins de la dotation et de l'approvisionnement :

- plutôt que de recueillir des copies des données d'identification personnelle, ECCC exige que les gestionnaires d'embauche signent une lettre attestant qu'ils ont vu ces données (fait surtout pour la dotation accélérée [DA]);
- les employés de la DA et de l'approvisionnement utilisent l'impression sécurisée lorsqu'ils traitent des renseignements personnels;
- les employés fournissent le NAS par téléphone (seulement pendant le processus de DA);
- les renseignements personnels inutiles ont été enlevés du système de DA et des communications de l'approvisionnement;
- l'accès des employés de la DA et de l'approvisionnement aux renseignements personnels est limité à ceux qui en ont besoin pour s'acquitter de leurs tâches.

Les résultats de l'analyse comparative montrent que la plupart des ministères informent les gens que leurs renseignements personnels seront protégés au moyen d'une clause de protection des renseignements personnels incluse dans les formulaires et contrats utilisés. Bien qu'ECCC informe habituellement les gens par téléphone ou par courriel pour les activités de dotation et les activités d'approvisionnement, cette pratique est conforme aux exigences de la Politique et de la *Loi sur la protection des renseignements personnels*.

3.4 Évaluations des facteurs relatifs à la vie privée

Selon la Directive du SCT sur l'évaluation des facteurs relatifs à la vie privée (ÉFVP), les responsables des institutions doivent établir un processus d'ÉFVP et d'approbation :

- qui correspond au niveau de risque d'atteinte à la vie privée des programmes ou activités de l'institution;

- grâce auquel l'ÉFVP est effectuée par le haut fonctionnaire ou le cadre responsable dans l'institution des nouveaux programmes, des nouvelles activités, ou des programmes ou activités qui ont subi des modifications importantes.

Les ÉFVP aident les gestionnaires de programme à s'acquitter de leurs responsabilités en matière de gestion des renseignements personnels. Les ÉFVP sont essentiellement un outil de gestion des risques permettant d'évaluer si les exigences de la *Loi sur la protection des renseignements personnels* sont respectées. Les ÉFVP aident aussi les décideurs à éviter les risques d'atteinte à la vie privée et leur apportent l'information dont ils ont besoin pour prendre des décisions éclairées. En veillant à ce que les ÉFVP soient effectuées, ECCC peut prévoir la réaction du public aux incidences sur la protection de la vie privée et donc éviter des refontes coûteuses de programmes, de services ou de processus.

En 2012, ECCC a élaboré une directive interne sur les ÉFVP ainsi que le processus interne d'approbation des ÉFVP. Ces documents ont été communiqués aux employés par le truchement d'ECollab et du site Web interne d'ECCC. Cette directive exige qu'il y ait un processus par lequel les ÉFVP sont :

- lancées ou mises à jour par les chefs des directions générales;
- approuvées à la fois par le coordonnateur de l'AIPRP et les chefs des directions générales;
- suivies par le gestionnaire de l'AIPRP.

La directive exige aussi que l'information suivante soit tenue à jour :

- le nombre d'ÉFVP entreprises;
- le nombre d'ÉFVP modifiées;
- le nombre d'ÉFVP présentées pour approbation au SCT;
- le nombre d'ÉFVP présentées pour approbation au Commissariat à la protection de la vie privée;
- le nombre d'ÉFVP approuvées par le SCT;
- le nombre d'ÉFVP approuvées par le Commissariat à la protection de la vie privée.

Bien que les processus et les pratiques aient été mis par écrit et communiqués aux employés, la DGEV n'a pu établir si l'information ci-dessus est suivie. Il est par conséquent difficile de déterminer si toutes les ÉFVP nécessaires sont dûment entreprises et terminées.

Recommandation 2 :
Le directeur général du Secrétariat ministériel devrait améliorer sa méthode de surveillance des évaluations des facteurs relatifs à la vie privée qui sont effectuées et exigées.

Réponse de la direction
D'accord. Le DG du Secrétariat ministériel concevra un système de surveillance amélioré pour les évaluations des facteurs relatifs à la vie privée qui sont exigées et effectuées au Ministère.

3.5 Sensibilisation et formation

Conformément aux politiques et aux directives du Conseil du Trésor, tous les employés qui traitent des renseignements personnels ou participent à la conception et à la mise en œuvre de systèmes qui traitent des renseignements personnels doivent être pleinement conscients de leurs obligations.

L'analyse comparative a montré que les sept ministères tiennent des séances de formation et de sensibilisation. Dans certains ministères, cette formation est obligatoire pour tous les nouveaux employés et fait partie de leur orientation. Voici certaines des pratiques exemplaires d'autres ministères en ce qui concerne la formation des employés :

- Fait partie du programme intensif pour les nouveaux inspecteurs (école préparatoire).
- Sur demande et adaptée (division).
- Séances de sensibilisation aux tables de gouvernance et de direction.
- Parallèlement à la formation sur la sensibilisation à la GI.
- Réunions mensuelles avec des agents de liaison de l'AIPRP qui répondent aux questions.
- Tutoriel fourni avec la déclaration et affichage sur la page Web interne.

Quatre ministères, dont ECCC, envoient des rappels aux employés à propos des atteintes à la vie privée. À EC, tous les nouveaux employés doivent suivre la séance d'information obligatoire en ligne sur la sécurité, qui explique les responsabilités des employés, entre autres les contrôles de l'accès et le traitement de l'information. Plus de 90 % des employés d'EC ont suivi cette formation obligatoire.

Des séances de formation ciblées ont de plus été tenues avec les employés des Ressources humaines, des Finances (y compris ceux de l'Approvisionnement) et de la Sécurité de la GI/TI. D'autres séances de formation ciblées sont également données à divers employés du Ministère qui doivent traiter des renseignements personnels. Différents documents de communication permettent aussi aux employés de prendre davantage conscience des questions de sécurité et de protection de la vie privée.

3.6 Fonds de renseignements

Conformément à la Directive du SCT sur les pratiques relatives à la protection de la vie privée, les ministères doivent limiter l'accès aux renseignements personnels et l'utilisation de ces renseignements par des moyens administratifs, techniques et matériels visant à protéger les renseignements personnels et la vie privée. Les politiques du SCT et d'ECCC exigent aussi que les ministères produisent chaque année de l'information détaillée sur l'organisation, les programmes, les fonctions et les fonds de renseignements du Ministère.

L'analyse comparative a montré qu'ECCC suit de nombreuses pratiques exemplaires, comme le chiffrement du disque sur les ordinateurs portatifs et les lecteurs portables et clés USB pour atténuer le risque de compromission de renseignements personnels, cela en réponse aux recommandations découlant de l'évaluation de la gestion dont il a déjà

été question. Jusqu'à maintenant, le chiffrement de tout le disque de plus de 3 900 ordinateurs portatifs a été configuré, et d'autres sont prévus.

Comme ils y sont tenus, tous les ministères, y compris ECCC, identifient et décrivent chaque année les renseignements personnels contenus dans les fichiers de renseignements personnels (FRP).

4. CONCLUSION

Dans l'ensemble, la revue a confirmé que les politiques et les processus requis pour la gestion de la protection des renseignements personnels sont en place et essentiellement conformes à tous les éléments de la Politique du Secrétariat du Conseil du Trésor (SCT) sur la protection de la vie privée. Le Cadre stratégique de protection des renseignements personnels d'EC consigne les rôles et les responsabilités et des lignes directrices, comme celles qui ont trait aux processus des évaluations des facteurs relatifs à la vie privée (ÉFVP) et du protocole en cas d'atteinte à la vie privée. La revue a confirmé que les renseignements personnels pour les activités de dotation et d'approvisionnement ne sont recueillis que pour les besoins de programmes précis.

La revue a tout de même cerné deux domaines où des améliorations sont possibles : les lignes directrices sur les processus relatifs à la collecte des numéros d'assurance sociale (NAS) et la surveillance des évaluations des facteurs relatifs à la vie privée (EFVP).

Annexe 1 Méthodologie et critères

Méthodologie

Une évaluation des risques a permis de confirmer, pendant la phase de planification de cette revue, l'objectif de la vérification et les domaines qui méritaient d'être examinés davantage. Les critères utilisés dans le contexte de cette revue ont été élaborés à partir d'une combinaison de normes et de modèles, comme le Global Technology Audit Guide − Practice Guide on Managing and Auditing Privacy Risks, la *Loi sur la protection des renseignements personnels* et les directives internes et politiques connexes du SCT et d'EC. Un mélange d'entrevues et d'une revue de la documentation a été utilisé.

L'évaluation de la gestion qui a été faite en 2013 par le personnel de l'AIPRP et de la Sécurité de la GI/TI, et l'analyse comparative menée par la DGEV ont également été examinées, et leurs résultats ont été pris en compte.

Critères

Critère de la revue **1. Le cadre de gestion et les principaux processus de gestion des renseignements personnels d'EC sont en place.**		**Respecté/ pas respecté**
1.1	**Cadre stratégique de protection des renseignements personnels** (CSPRP) – Le CSPRP a été élaboré et mis en œuvre pour appuyer la gestion et la surveillance des pratiques relatives à la protection de la vie privée.	En partie respecté
1.2	**Gouvernance et supervision –** Il existe des structures officielles de gouvernance qui aident à surveiller les pratiques relatives à la protection de la vie privée.	Respecté
1.3	**Rôles et responsabilités** – Les rôles et les responsabilités sont clairement définis et communiqués à tous les employés d'EC.	Respecté
1.4	**Collecte de renseignements personnels et information à fournir** – Les renseignements personnels qui sont recueillis sont directement liés à une activité ou à un programme. La personne qu'ils concernent est de plus avisée, au moment de la collecte, de la raison de celle-ci.	Respecté
1.5	**Évaluations des facteurs relatifs à la vie privée (ÉFVP)** – Des ÉFVP sont effectuées pour les programmes et les activités qui ont subi des modifications importantes et pour lesquels des renseignements personnels sont recueillis.	En partie respecté
1.6	**Sensibilisation et formation** – Des séances de formation et de sensibilisation qui transmettent aux employés l'information dont ils ont besoin pour s'acquitter de leurs rôles et de leurs responsabilités sont tenues.	Respecté
1.7	**Fonds de renseignements** – Chaque année, les renseignements personnels relevant d'EC sont identifiés et décrits dans des catégories de fichiers de renseignements personnels (FRP).	Respecté

Dates importantes

Première rencontre (note de lancement)	novembre 2013
Plan de la revue envoyé à la direction	avril 2014
Rapport de l'analyse comparative envoyé au Comité consultatif externe de vérification à titre d'information	mars 2015
Recommandation du Comité consultatif externe de vérification	juin 2015
Approbation du sous-ministre	décembre 2015

Annexe 2
Rapport final de l'analyse comparative

Analyse comparative de la gestion de la protection des renseignements personnels

Direction générale de la vérification et de l'évaluation

Mars 2015

Canada

ANNEXE 2

Liste des acronymes

AIPRP	Accès à l'information et protection des renseignements personnels
AM	Autres ministères
CCEV	Comité consultatif externe de vérification
CPVP	Commissariat à la protection de la vie privée
CSPRP	Cadre stratégique de protection des renseignements personnels
DGF	Direction générale des finances
DGRH	Direction des ressources humaines
DGSM	Direction générale des services ministériels
EC	Environnement et Changement climatique Canada
ÉFVP	Évaluation des facteurs relatifs à la vie privée
FRP	Fichier de renseignements personnels
SCT	Secrétariat du Conseil du Trésor
SM	Secrétariat ministériel
SM	Sous-ministre

Préparé par l'équipe de la vérification et de l'évaluation

Remerciements

L'équipe de la revue, formée de Sophie Lalonde, chef d'équipe, de Sara Halford et de John Galarneau, sous la direction de Stella Line Cousineau, tient à remercier ceux et celles qui, à EC et dans les six ministères participants, ont contribué à ce projet. Elle aimerait remercier tout particulièrement les coordonnateurs de l'AIPRP, les employés de la dotation et ceux de l'approvisionnement, ainsi que de nombreuses autres personnes qui nous ont fait part de leurs observations et de leurs commentaires.

Contrôle des versions du document

Nom du fichier : Benchmarking FINAL Report

Date : 12 mai 2015

Table des matières

1. Introduction

En 2013, la Direction générale des services ministériels (DGSM) d'Environnement et Changement climatique Canada (EC), en collaboration avec le Secrétariat ministériel, a procédé à une évaluation des pratiques relatives au traitement des renseignements personnels et de nature délicate. Cette évaluation a mené à des recommandations qui pouvaient être mises en œuvre rapidement, et ont été suivies par plusieurs mesures de gestion. La haute direction a également demandé à la Direction générale de la vérification et de l'évaluation (DGVE) d'effectuer une analyse comparative des processus de dotation et d'approvisionnement d'EC et de ceux d'autres ministères dont la taille et le mandat sont similaires à ceux d'EC. Ce projet a donc été inclus dans le Plan de vérification axé sur le risque de 2013 qui a été approuvé par le sous-ministre, sur recommandation du Comité consultatif externe de vérification.

Les résultats de cette étude feront partie de la revue globale de la gestion de la protection des renseignements personnels effectuée par la DGEV.

Le présent rapport a trait aux conclusions de l'analyse comparative.

2. Contexte

2.1 Législation et politiques applicables

La *Loi sur la protection des renseignements personnels*, la réglementation et les politiques et directives connexes appuient l'engagement du gouvernement, qui est déterminé à protéger les renseignements personnels dont il fait la collecte et à faire en sorte que ceux-ci soient utilisés et conservés de manière cohérente et appropriée. On entend par renseignements personnels les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable. En vertu de la *Loi*, les renseignements personnels qu'une institution fédérale peut recueillir sont ceux qui ont un lien direct avec ses programmes ou ses activités[2].

Aux termes de la *Loi* également, il incombe au responsable d'un ministère ou d'une institution, ou à ses délégués :

- de préparer et de déposer un rapport annuel sur l'administration de la *Loi* devant chacune des chambres du Parlement;
- de préparer de nouvelles descriptions, ou de modifier les descriptions des fichiers de renseignements personnels (FRP);
- de transmettre au SCT :
    - un exemplaire du rapport annuel;
    - une mise à jour du chapitre d'*Info Source* concernant les FRP dont la création ou la modification est proposée;
    - un rapport statistique sur l'application de la *Loi* dans l'institution[3].

[2] *Loi sur la protection des renseignements personnels,* art. 4.

[3] Politique sur la protection de la vie privée du SCT, art. 6.3.2.

De plus, tout programme, service ou système qui recueille et détiennent des renseignements personnels doit effectuer des évaluations des facteurs relatifs à la vie privée (ÉFVP) pour cerner, évaluer et atténuer les risques d'atteinte à la vie privée.

En plus de la *Loi sur la protection des renseignements personnels* et du *Règlement sur la protection des renseignements personnels*, plusieurs directives et politiques du CT ont une incidence directe sur la gestion de la protection de la vie privée et des renseignements personnels. Ce sont, entre autres, mais non exclusivement :

- la *Politique sur la protection de la vie privée,*
- la *Politique du gouvernement sur la sécurité;*
- la *Politique sur la gestion de l'information;*
- la *Directive sur les pratiques relatives à la protection de la vie privée,*
- la *Directive sur l'évaluation des facteurs relatifs à la vie privée,*
- les *Lignes directrices sur les atteintes à la vie privée.*

La Politique du CT sur la protection de la vie privée, de 2008, a subi des révisions mineures et a été mise à jour en août 2014. Cette politique précise un certain nombre d'obligations des institutions fédérales en ce qui concerne les saines pratiques de gestion pour le traitement et la protection des renseignements personnels, dont les principales exigences suivantes :

- Faire connaître les politiques et les procédures ainsi que leurs responsabilités aux termes de la *Loi* aux employés de l'institution fédérale.
- Satisfaire aux exigences de la *Loi sur la protection des renseignements personnels* lors de la conclusion de contrats avec des organismes du secteur privé ou l'établissement d'accords ou d'ententes avec des organisations du secteur public.
- Veiller à ce que des dispositions appropriées en matière de protection des renseignements personnels soient incluses dans les contrats ou les ententes pouvant donner lieu à la circulation intergouvernementale ou transfrontalière de renseignements personnels.
- Veiller à ce que les conditions particulières ayant trait à l'utilisation des numéros d'assurance sociale (NAS) soient respectées, ainsi que les restrictions relatives à leur collecte, à leur utilisation et à leur communication.
- Veiller, le cas échéant, à la réalisation, à la mise à jour et à la diffusion des évaluations des facteurs relatifs à la vie privée (ÉFVP) et des ÉFVP multi-institutionnelles.
- Mettre les fichiers de renseignements personnels (FRP) à jour chaque année. Ces fichiers renferment la description des renseignements personnels organisés et extractibles par nom de personne ou numéro d'identification, symbole ou autre indication particulière qui n'est attribuée qu'à cette personne[4].
- Consulter le SCT au sujet de toutes les propositions d'établissement ou de révocation d'un fichier inconsultable et présenter une demande particulière au président du Conseil du Trésor en ce qui concerne la proposition.

3. Objectif, portée et méthodologie

L'analyse comparative visait à comparer les principaux processus d'EC en matière de protection des renseignements personnels à ceux d'autres ministères (AM) comparables afin de mettre des pratiques exemplaires en œuvre s'il y a lieu. L'annexe 1 présente les principaux sujets de l'étude et les questions concernant :

- le cadre stratégique de protection des renseignements personnels (CSPRP);
- la gouvernance et la surveillance;
- les rôles et responsabilités;
- la collecte des renseignements personnels et l'information à fournir;
- les ÉFVP;
- la sensibilisation et la formation;
- les fonds de renseignements.

Ces sujets ont été choisis en fonction des prescriptions de la *Loi sur la protection des renseignements personnels* et des politiques du CT relatives à la protection des renseignements personnels. L'étude a également porté sur le traitement des renseignements personnels particuliers aux processus de la dotation et de l'approvisionnement.

La gestion de la protection des renseignements personnels de sept ministères a été analysée et comparée à l'aide d'un sondage en ligne complété par des entrevues et un examen de la documentation. Les ministères ont été choisis en fonction de la similitude de leur taille et de la nature de leurs activités. Les ministères suivants ont participé à l'étude :

- Environnement et Changement climatique Canada;
- Agriculture et Agroalimentaire Canada;
- Agence canadienne d'inspection des aliments;
- Pêches et Océans Canada;
- Conseil national de recherches Canada;
- Ressources naturelles Canada;
- Transports Canada.

Les processus suivants ont permis de recueillir de l'information et de faire état des résultats :

- un sondage initial a été envoyé aux coordonnateurs de l'AIPRP d'AM, une copie étant transmise à leurs dirigeants principaux de la vérification (DVP);
- au besoin, ce sondage a été suivi d'entrevues avec les ministères pour éclaircir certains renseignements ou obtenir de l'information complémentaire;
- les réponses et les données recueillies ont été analysées et comparées;
- les pratiques exemplaires ont été consignées;
- comme les ministères en avaient convenu dès le départ, les résultats de l'analyse ont été communiqués de manière semi-confidentielle (les participants sont identifiés, mais les résultats ne sont pas liés à des participants en particulier);

- les observations et les commentaires obtenus dans le cadre du processus de validation avec les ministères ont été regroupés et intégrés au présent rapport final, pour lequel le même principe de confidentialité a été respecté.

Cette étude n'a pas porté sur les demandes d'accès à l'information, la correction de renseignements personnels (vérification de l'exactitude) ou l'infrastructure et les mesures de protection de la TI.

4. Observations

Dans l'ensemble, les pratiques de gestion des renseignements personnels des ministères participants étaient similaires à celles des autres ministères.

- Tous les ministères ont élaboré un cadre stratégique de protection des renseignements personnels (CSPRP) comme l'exige la *Loi sur la protection des renseignements personnels* et la *Politique sur la protection de la vie privée* du CT.
- Bien que la plupart des ministères aient répondu que la mise en œuvre était très avancée, jusqu'à maintenant, un seul a entièrement mis en œuvre son CSPRP.
- Pour tous les ministères, la surveillance s'effectue par le truchement des structures générales de gouvernance et les liens hiérarchiques.
- Il y a des similitudes entre les ministères pour ce qui est des outils dont ils se servent pour le traitement des renseignements personnels, mais les types de renseignements personnels qu'ils recueillent varient beaucoup. Tous les ministères ont pris des mesures pour limiter la collecte de renseignements personnels.
- Tous les ministères offrent aux employés de la formation sur les questions de respect de la vie privée et la plupart leur rappellent leurs obligations à intervalles réguliers.

4.1 Cadre stratégique de protection des renseignements personnels

Selon la *Politique sur la protection de la vie privée*, il incombe aux responsables des institutions fédérales d'appliquer efficacement, de manière coordonnée et proactive, la *Loi sur la protection des renseignements personnels* dans leur institution respective. Le protocole et les directives aident les responsables à assurer la coordination et à gérer de manière proactive un programme de protection de la vie privée efficace. Le CSPRP doit énoncer clairement les responsabilités des institutions gouvernementales en matière de prise de décisions et de gestion de la mise en œuvre de la *Loi sur la protection des renseignements personnels* et du *Règlement sur la protection des renseignements personnels*.

Bien que les sept ministères aient tous élaboré un CSPRP, un seul l'a entièrement mis en œuvre. Le cadre des six autres était mis en œuvre à 50 % ou plus. Un ministère prévoyait que ce serait fait en mars 2015.

Les sections des cadres de la majorité des ministères étaient similaires. La plupart des ministères ont suivi les lignes directrices du SCT et ont inclus des instructions sur les

pratiques relatives à la protection de la vie privée, les évaluations des facteurs relatifs à la vie privée (ÉFVP), les atteintes à la vie privée ainsi que le consentement et la notification et la communication. Tous les ministères ont des lignes directrices sur les atteintes à la vie privée, qui font l'objet des dernières lignes directrices du CT sur les atteintes à la vie privée. Ces lignes directrices s'ajoutent aux politiques et aux lignes directrices générales du CT, comme la Directive sur le numéro d'assurance sociale (NAS) de 2008, qu'elles complètent.

Le CSPRP d'un des ministères illustre des pratiques exemplaires et inclut plusieurs documents de lignes directrices. Les rôles, les responsabilités et les exigences sont décrits en détail. Par exemple, la politique de ce ministère régissant la gestion des renseignements personnels énonce les différences entre le pouvoir délégué et les responsabilités prévues par la loi. Ce même document décrit les exigences relatives à la conservation et à la destruction ainsi que le protocole ayant trait à la protection des renseignements personnels à des fins non administratives.

Comme pratique exemplaire, un CSPRP efficace exigerait qu'une analyse de l'écart soit effectuée à intervalles réguliers pour vérifier que les politiques pertinentes ont correctement été mises en œuvre. Sur les six ministères qui ont mis un cadre stratégique en œuvre, trois ont procédé à une analyse de l'écart entre ce qu'ils ont fait et les politiques et directives du CT. Un ministère a répondu qu'il a élaboré des lignes directrices sur l'atteinte à la vie privée à la suite de cette analyse de l'écart.

Le tableau ci-après présente les principaux sujets que les ministères abordent dans leur CSPRP.

Figure 1 – Principaux sujets faisant l'objet de lignes directrices dans le CSPRP

Sujets du CSPRP	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Pratiques, protocole, rôles et responsabilités en matière de protection de la vie privée	Oui	Oui	Oui	Non	Oui	Oui	Oui
Évaluations des facteurs relatifs à la vie privée, des risques	Oui	Oui	Oui	Non	Oui	Oui	Oui
Atteintes à la vie privée	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Numéro d'assurance sociale (NAS)	Non	Non	Oui	Non	Non	Non	Non
Lignes directrices sur le consentement et la notification/ communication	Non	Non	Non	Oui	Oui	Oui	Oui

4.2 Gouvernance et surveillance

Conformément à la *Politique sur la protection de la vie privée* du CT, les responsables des institutions fédérales[5] :

- décident s'ils délèguent certains des pouvoirs ou certaines des attributions ou des fonctions que leur confère la *Loi*;
- lorsque la décision de déléguer est prise, signent un arrêté de délégation autorisant des cadres ou des employés de l'institution qui occupent un poste de niveau approprié à exercer les pouvoirs, les attributions ou les fonctions mentionnés dans l'arrêté. Une fois l'arrêté signé, les pouvoirs, attributions ou fonctions qui ont été délégués ne peuvent être exercés que par le responsable de l'institution ou son délégué. Les délégués sont responsables des décisions qu'ils prennent. C'est cependant toujours le responsable de l'institution fédérale qui est en fin de compte responsable.

Il incombe aux responsables des institutions fédérales de décider si les pouvoirs, les attributions ou les fonctions prévus par l'article 73 de la *Loi sur l'accès à l'information* seront délégués en vertu de cette loi. Les sept ministères suivent des pratiques exemplaires et ont une délégation de pouvoirs officielle. Le niveau de la délégation de

[5] Article 6.1 de la Politique sur la protection de la vie privée du SCT.

pouvoirs diffère d'un ministère à l'autre (voir la figure 2), mais dans tous les cas le groupe de l'AIPRP y participe.

Figure 2. Délégation de pouvoirs pour la gestion de la protection des renseignements personnels

Niveaux de pouvoir	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Sous-ministre adjoint/responsable de la protection de la vie privée	Oui	Oui	Oui	Non	Oui	Oui	Non
Directeur général responsable de l'AIPRP	Non	Oui	Oui	Non	Oui	Oui	Oui
Directeur de l'AIPRP	Oui	Oui	Oui	Oui	Oui	Non	Oui
Directeur adjoint / gestionnaire de l'AIPRP	Non	Oui	Oui	Oui	Oui	Non	Non

Selon les lignes directrices du Cadre de responsabilisation de gestion (CRG) du SCT, les ministères doivent avoir un organisme de surveillance pour la gouvernance de leur gestion, qui inclut la gestion des responsabilités en matière de protection des renseignements personnels.

Lorsqu'ils ont été interrogés à propos de cette ligne directrice, aucun des ministères n'a dit avoir d'organisme de surveillance. Les ministères ont répondu en faisant référence à leur délégation officielle de pouvoirs et aux liens hiérarchiques. La surveillance s'effectue par le truchement des structures de gouvernance générales et des liens hiérarchiques.

Pour que des CSPRP efficaces soient mis en œuvre et qu'une surveillance adéquate des pratiques relatives à la protection de la vie privée s'exerce, la *Politique sur la protection de la vie privée* du CT charge les responsables des institutions gouvernementales, ou leurs délégués, de veiller à ce que la gestion soit conforme à la Politique en ce qu'elle a trait à l'administration de la *Loi sur la protection des renseignements personnels.* Cette surveillance peut prendre la forme d'une revue ou d'une vérification.

Un seul ministère a effectué une vérification de la protection des renseignements personnels en 2010 et un autre ministère a procédé à une évaluation en 2013.

4.3 Rôles et responsabilités

Conformément à la *Politique sur la protection de la vie privée* du CT, les responsables des institutions gouvernementales doivent veiller à ce que les responsabilités en matière de prise de décisions et de gestion de l'application de la *Loi sur la protection des renseignements personnels* et du *Règlement sur la protection des renseignements personnels* soient claires. Ils doivent également faire en sorte que les employés de l'institution fédérale connaissent les politiques, les procédures ainsi que leurs responsabilités aux termes de la *Loi*.

Bien que six ministères communiquent leurs rôles et leurs responsabilités aux employés par l'entremise de leur groupe d'AIPRP, un n'a pu confirmer que cela avait été fait.

Nous avons remarqué la pratique exemplaire consistant à donner de la documentation écrite sur les rôles et responsabilités sous forme de cadre ou de manuel, et d'offrir des séances de formation aux employés.

4.4 Collecte et communication de renseignements personnels

La présente section porte sur la collecte, le traitement et la communication des renseignements personnels particuliers aux processus d'approvisionnement et de dotation.

Collecte

Selon la *Loi sur la protection des renseignements personnels*, les renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités. Bien que l'objectif de cet exercice n'ait pas été d'évaluer si l'information recueillie avait un lien avec un programme, la DGEV souhaitait savoir quels types de renseignements sont recueillis dans le cadre des processus d'approvisionnement et de dotation, ce qui pourrait, le cas échéant, permettre la mise en œuvre de pratiques exemplaires.

Le tableau suivant (figure 3) présente les résultats du sondage particulier aux activités d'approvisionnement et de passation de marchés. Globalement, deux ministères recueillent toute l'information mentionnée ci-après et tous les ministères participants recueillent le nom, l'adresse (antérieure et actuelle) et l'adresse électronique. Le tableau montre aussi que les autres types de renseignements personnels qui sont recueillis varient considérablement.

Figure 3 − Renseignements personnels recueillis pour les activités d'approvisionnement

Information recueillie	(1)	(2)	(3)	(4)	(5)	(6)	(7)	% des ministères qui recueillent cette information
Nom	x	x	x	x	x	x	x	100 %
Adresse (antérieure et actuelle)	x	x	x	x	x	x	x	100 %
Adresse électronique	x	x	x	x	x	x	x	100 %
Numéro de téléphone		x	x	x	x	x	x	86 %
Taux de facturation ou salaire exact	x	x	x		x	x	x	86 %
Date de naissance	x			x	x	x	x	71 %
Confirmation de l'autorisation			x	x	x	x	x	71 %

de sécurité								
Emploi antérieur				x	x	x	x	57 %
Date de début et de fin des travaux			x	x	x	x	x	57 %
Lieu de travail			x		x	x	x	57 %
Scolarité					x	x	x	43 %
Numéro d'assurance sociale				x	x		x	43 %
Heures de travail (empl. temp.)					x	x	x	43 %
Autres	x	x					x	43 %

Dans le cas du processus de dotation, nous avons remarqué, comme pratique exemplaire, qu'un ministère, plutôt que de recueillir des copies des données d'identification personnelle pour les opérations de dotation, exige que les gestionnaires d'embauche signent une lettre attestant qu'ils ont vu ces données. Il s'agit d'une mesure de protection supplémentaire contre l'accès non autorisé aux renseignements personnels.

Le tableau ci-dessous présente les types de renseignements personnels recueillis dans le contexte du processus de dotation. Il est important de remarquer qu'un des ministères (le n^{o} 6) n'a pas répondu à cette section du sondage.

De nouveau, le tableau montre qu'une grande variété de renseignements sont recueillis, dont l'information suivante recueillie par tous les ministères : le nom, l'adresse, le numéro de téléphone, l'adresse électronique et le curriculum vitæ. Dans la catégorie des « Autres types de renseignement », un ministère a noté qu'il recueille un formulaire de consentement signé autorisant la transmission des renseignements personnels au Système de gestion de l'information sur les priorités (SIGP).

Figure 4 − Renseignements personnels recueillis pour les activités de dotation

Dotation	(1)	(2)	(3)	(4)	(5)	(7)	% des ministères qui recueillent cette information
Nom	x	x	x	x	x	x	100 %
Adresse (antérieure et actuelle)	x	x	x	x	x	x	100 %
Numéro de téléphone	x	x	x	x	x	x	100 %
Adresse électronique	x	x	x	x	x	x	100 %
Curriculum vitæ	x	x	x	x	x	x	100 %
Scolarisation		x	x	x	x	x	83 %
Confirmation de l'autorisation de sécurité		x	x	x	x	x	83 %
Numéro d'assurance sociale		x	x	x	x	x	83 %
Évaluation psychologique		x	x	x	x	x	83 %
Date de début et de fin		x	x	x	x	x	83 %
Date de naissance			x	x	x	x	67 %
Attestation d'établissements d'enseignement		x	x		x	x	67 %

Formulaire personnel d'information sur la sécurité		x	x		x	x	67 %
Code d'identification de dossier personnel (CIDP)		x	x		x	x	67 %
Balayage de la carte de citoyenneté		x	x		x	x	67 %
Preuve de l'attestation de citoyenneté canadienne		x	x		x	x	67 %
Heures de travail		x	x	x		x	67 %
Lieu de travail		x	x		x	x	67 %
Nom et poste du superviseur		x	x		x	x	67 %
Emploi antérieur		x	x		x	x	67 %
Balayage du permis de conduire		x	x			x	50 %
Balayage du certificat de naissance		x	x			x	50 %
Balayage du passeport		x	x			x	50 %
Salaire exact		x	x			x	50 %
Code de classification du poste		x	x			x	50 %
Autres (veuillez préciser)	x	x			x		50 %

La *Loi sur la protection des renseignements personnels* exige que, lorsque des renseignements personnels sont recueillis, la personne qu'ils concernent soit informée de la raison pour laquelle ils le sont. Elle porte également ceci : « Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article. » La *Politique sur la protection de la vie privée* du CT dit explicitement que les ministères doivent veiller à ce que des dispositions en matière de protection des renseignements personnels soient incluses dans les contrats et les ententes pouvant donner lieu à la circulation intergouvernementale ou transfrontalière de renseignements personnels.

Une pratique exemplaire consisterait à consigner sous une forme ou une autre la manière dont quelqu'un est informé de l'objet de la collecte. La plupart des ministères informent les gens que leurs renseignements personnels seront protégés au moyen d'une clause sur la protection des renseignements personnels qui est incluse dans les formulaires et les contrats qui recueillent des renseignements personnels. Un ministère informe les gens soit par téléphone ou par courriel.

La *Loi* et la *Politique sur la protection de la vie privée* du CT ne décrivent pas les méthodes de collecte pouvant être utilisées. Selon le type de renseignements et leur caractère plus ou moins délicat, les ministères sondés utilisent diverses méthodes de collecte.

Pour la passation de marchés, sur les six ministères ayant participé à l'étude :

- six recueillent des renseignements personnels par courriel et par des formulaires;
- cinq obtiennent l'information par téléphone ou télécopieur;
- quatre obtiennent des renseignements personnels au moyen de copies numérisées;
- trois obtiennent l'information soit sur papier ou par d'autres moyens, comme les propositions de prix présentées par le vendeur.

Pour la dotation, les six ministères qui ont répondu aux questions du sondage ont dit recueillir des renseignements personnels pour les opérations de dotation par l'une au moins des méthodes suivantes :

- six utilisent le courriel;
- un utilise soit le télécopieur ou le téléphone;
- six utilisent soit les formulaires papier ou électroniques.

D'après notre analyse de l'information reçue, le courriel et les formulaires électroniques sont considérés comme de meilleures façons de recueillir des renseignements personnels en raison de la capacité de chiffrement.

Traitement

Lorsque les renseignements personnels ont été recueillis, les ministères ont besoin de processus robustes pour que leurs fonds de renseignements personnels soient en sécurité et soient exacts pour la production de rapports annuels. L'utilisation d'imprimantes ou de numériseurs exige un protocole pour que l'information ne reste pas stockée dans l'appareil, et les documents imprimés doivent circuler et être entreposés conformément aux exigences en matière de classement.

Pour la passation de marchés, sur les sept ministères qui ont répondu aux questions du sondage :

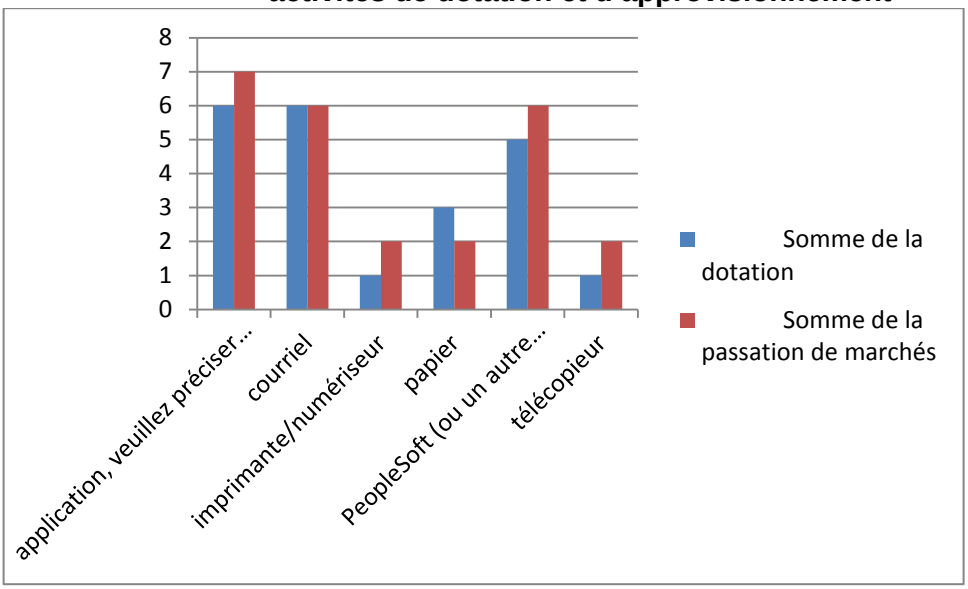
- tous les sept traitent les renseignements personnels par courriel;
- six utilisent le logiciel d'exploitation ou une application pour la collecte de renseignements personnels;
- deux traitent aussi l'information en se servant du télécopieur, de papier, d'une imprimante ou d'un numériseur. (Voir la figure 5.)

Pour la dotation, sur les six ministères ayant répondu aux questions du sondage :

- tous les six traitent les renseignements personnels par courriel et par le logiciel d'exploitation ou une application (p. ex. PeopleSoft);
- trois incluent aussi des formulaires papier et des dossiers dans leur processus. (Voir la figure 5.)

Comme nous l'avons dit à la section précédente, le courriel et les formulaires électroniques sont considérés comme de meilleures façons de traiter les renseignements personnels en raison de la capacité de chiffrement.

Figure 5 – Méthode de traitement des renseignements personnels pour les activités de dotation et d'approvisionnement



Description de la figure 5

Le diagramme en barres ci-dessus illustre les résultats du sondage sur les méthodes utilisées pour le traitement des renseignements personnels pour les activités de dotation et de passation de marchés.

Pour la dotation, sur les six ministères ayant répondu aux questions du sondage, tous traitent les renseignements personnels par courriel et par le logiciel d'exploitation ou une application (p. ex. PeopleSoft) et trois incluent aussi des formulaires papier et des dossiers dans leurs processus.

Pour la passation de marchés, sur les sept ministères qui ont répondu aux questions du sondage, six utilisent le logiciel d'exploitation ou une application pour la collecte de renseignements personnels, tous traitent les renseignements personnels par courriel, et deux traitent aussi l'information en se servant du télécopieur, de papier, d'une imprimante ou d'un numériseur.

Communication de renseignements personnels

Pour respecter l'intention de la *Loi* et de la Politique du CT, les ministères doivent limiter l'accès aux renseignements personnels aux employés qui ont besoin de cette information pour exécuter leur programme et à d'autres personnes, selon les motifs admissibles de communication à une institution publique ou privée conformément à l'article 13 de la *Loi*.

Tous les ministères ayant répondu au sondage ont dit qu'ils ne donnent officiellement accès aux renseignements personnels qu'aux employés du ministère ayant des responsabilités soit en dotation ou en approvisionnement, comme les agents d'administration ou les chefs d'équipe chargés de l'administration d'un contrat, les

employés des RH et les gestionnaires responsables des opérations de dotation. Les ministères sondés ont également dit que les renseignements personnels sont communiqués aussi à d'autres ministères (AM) fédéraux ou provinciaux ou à des organisations privées dans le cadre d'activités de dotation ou d'approvisionnement.

L'échange de renseignements dépend du mandat de chacun des ministères. Certains ministères travaillent en étroite collaboration et doivent donc échanger des renseignements personnels. Selon le sondage, tous les ministères respectent les objectifs énoncés à l'article 13 de la *Loi.*

La présentation au public de rapports cohérents sur l'administration de la *Loi*, sous forme de rapports annuels au Parlement, de rapports statistiques et de la publication annuelle d'Info Source, est un des résultats escomptés de la Politique sur la protection de la vie privée. Les sept ministères ont dit produire un rapport statistique et une description de leurs FRP. À l'exception d'un seul ministère, tous revoient aussi leur description tous les ans.

4.5 Évaluation des facteurs relatifs à la vie privée

La *Politique du gouvernement sur la sécurité* et la Directive sur l'évaluation des facteurs relatifs à la vie privée du CT exigent que des ÉFVP soient effectuées pour les programmes et les activités qui ont subi des modifications importantes et pour lesquels des renseignements personnels sont recueillis.

Six ministères suivent la pratique exemplaire qui consiste à mettre par écrit leur processus d'ÉFVP. Bien qu'un ministère ait officialisé son processus, il effectue toujours les ÉFVP de façon ponctuelle. Les résultats montrent aussi que d'autres ministères utilisent diverses méthodes pour s'acquitter en partie de cette responsabilité : dans un ministère, le groupe de l'AIPRP collabore étroitement avec le groupe de la TI et est par conséquent informé lorsque des systèmes d'information sont mis en œuvre ou subissent des modifications importantes; un autre ministère transmet un questionnaire d'ÉFVP à tous les gestionnaires de programme.

4.6 Sensibilisation et formation des employés

Conformément aux politiques et aux directives du Conseil du Trésor, tous les employés qui traitent des renseignements personnels ou participent à la conception et à la mise en œuvre de systèmes qui traitent des renseignements personnels doivent être pleinement conscients de leurs obligations.

Tous les ministères donnent des séances de formation et de sensibilisation. Dans certains ministères, cette formation est obligatoire pour tous les nouveaux employés et fait partie de leur orientation. Voici les types de pratiques exemplaires des différents ministères en ce qui concerne la formation des employés :

- Fait partie du programme intensif pour les nouveaux inspecteurs (école préparatoire).
- Sur demande et adaptée (division).
- Séances de sensibilisation aux tables de gouvernance et de direction.
- Parallèlement à la formation sur la sensibilisation à la GI.

- Réunions mensuelles avec des agents de liaison de l'AIPRP qui répondent aux questions.
- Tutoriel fourni avec la déclaration et affichage sur la page Web interne.

Quatre ministères ont suivi la pratique exemplaire et ont envoyé des rappels aux employés à propos des atteintes à la vie privée. Une atteinte à la vie privée est un incident ou un événement qui contrevient à la *Loi sur la protection des renseignements personnels;* il y a atteinte à la vie privée en cas de collecte, d'utilisation, de communication, de conservation ou de destruction inappropriée ou non autorisée de renseignements personnels.

4.7 Fonds de renseignements

La *Politique sur la protection de la vie privée* du CT exige que les ministères « [a]ssure[nt] la protection et la gestion efficace des renseignements personnels en cernant, en évaluant, en surveillant et en atténuant les risques d'entrave à la vie privée dans les programmes et activités du gouvernement dans le cadre desquels des renseignements personnels sont recueillis, conservés, utilisés, divulgués ou détruits ».

Les résultats de notre analyse indiquent que six ministères utilisent le chiffrement des données, les signatures numériques et les certificats d'authenticité pour atténuer le risque d'atteinte à la vie privée. Un ministère ne savait pas si ce genre d'instrument était utilisé chez lui au moment du sondage.

Quatre ministères utilisent des ordinateurs portatifs et des lecteurs portables ou des clés USB pour recueillir des renseignements personnels. Parmi ceux-ci, trois ont des procédures de protection convenables qui exigent que la clé USB soit commandée par l'entremise des groupes TI et chiffrée.

Annexe 1 – Sujets de l'analyse comparative et questions du sondage

Sujets de l'analyse comparative	
1.1	**Cadre stratégique de protection des renseignements personnels (CSPRP)** – Un CSPRP efficace a été élaboré et mis en œuvre pour appuyer la gestion et la surveillance des pratiques relatives à la protection de la vie privée. Un CSPRP a-t-il été élaboré et à quel point est-il mis en œuvre? Sur quels éléments votre CSPRP porte-t-il? Avez-vous procédé à une analyse de l'écart par rapport à la Politique sur la protection des renseignements personnels?
1.2	**Gouvernance et surveillance** – Il existe des structures de gouvernance officielles qui aident à surveiller les pratiques relatives à la protection de la vie privée. Avez-vous un arrêté de délégation officiel pour les responsabilités relatives à la protection des renseignements personnels? Quel type de structures de gouvernance avez-vous en ce qui concerne la gestion des renseignements personnels? Une revue ou une vérification de la protection des renseignements personnels a-t-il eu lieu dans votre ministère? Si oui, en quelle année?
1.3	**Rôles et responsabilités** – Les rôles et responsabilités sont clairement définis et communiqués à tous les employés d'EC. Les rôles et les responsabilités en matière de gestion de la protection des renseignements personnels sont-ils bien communiqués aux agents de dotation et de passation de marchés?
1.4	**Collecte de renseignements personnels et information à fournir** – Les renseignements personnels qui sont recueillis sont directement liés à une activité ou à un programme. Au moment de la collecte, la personne que ces renseignements concernent est aussi informée de la raison pour laquelle ils sont recueillis. Quels types de renseignements personnels recueillez-vous pour les activités d'**approvisionnement et de passation de marchés**? Quels types de renseignements personnels recueillez**-**vous pour les opérations de **dotation**? Lorsque vous recueillez des renseignements personnels pour des activités **de passation de marchés ou de dotation**, de quelle façon informez-vous les personnes concernées de la raison pour laquelle cette information est recueillie? Vos formulaires et contrats comportent-ils une clause sur la protection des renseignements personnels? (Formulaires utilisés pour recueillir les renseignements

	personnels pour **les marchés et la dotation.**) De quelle façon recueillez-vous les renseignements personnels pour les activités **de passation de marchés et de dotation**? De quelle façon traitez-vous les renseignements personnels après les avoir recueillis (pour la passation de marchés **ou les processus de dotation**). Comment l'accès aux renseignements personnels est-il déterminé pour la passation de marchés et la **dotation**? Transmettez-vous des renseignements personnels à d'autres organisations? Si oui, à qui?
1.5	**Évaluations des facteurs relatifs à la vie privée (ÉFVP)** – Des ÉFVP sont effectuées pour les programmes et activités qui ont subi des modifications importantes et pour lesquels des renseignements personnels sont recueillis. La bonne gestion et les principales décisions reposent sur les résultats des ÉFVP. Le processus des évaluations des facteurs relatifs à la vie privée (ÉFVP) est-il consigné? Comment faites-vous en sorte que des ÉFVP soient réalisées pour tous les nouveaux programmes et toutes les nouvelles activités, et tous les programmes et activités qui ont subi des modifications importantes et pour lesquels des renseignements personnels sont recueillis?
	Sensibilisation et formation – Des séances de formation et de sensibilisation qui donnent aux employés l'information sur la protection des renseignements personnels dont ils ont besoin pour remplir leur rôle et s'acquitter de leurs responsabilités sont offertes. Votre ministère ou organisme offre-t-il des séances de sensibilisation et de formation? Si oui, à quel type de séances les employés ont-ils accès? Envoyez-vous des rappels aux employés à propos d'atteintes éventuelles à la vie privée? Veillez-vous à ce que tous les renseignements personnels qui relèvent de votre organisation soient identifiés et décrits?
1.7	**Fonds de renseignements personnels** – Chaque année, les renseignements personnels qui relèvent d'EC sont identifiés et décrits en catégories de fichiers de renseignements personnels (FRP). Utilisez-vous le chiffrement pour protéger les renseignements personnels? Quel type de chiffrement utilisez-vous? Quels appareils portatifs et mobiles utilisez-vous pour la collecte de renseignements personnels?