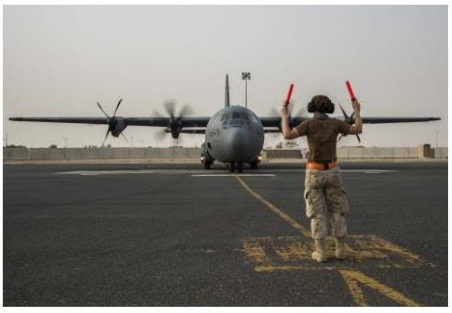
National Defence / Défense nationale

SOUS-MINISTRE ADJOINT (SERVICES D'EXAMEN)

Revu par le SMA(Svcs Ex) conformément à la Loi sur l'accès à l'information.
Information SANS CLASSIFICATION.

Audit de la protection de la vie privée et des renseignements personnels





1259-5-020 (SMA[Svcs Ex])
978-0-660-45523-5
D2-639/2022F-PDF
Septembre 2022

Canada

Table des matières

Sigles et abréviations

AIPRP	Accès à l'information et protection des renseignements personnels
BAC	Bibliothèque et Archives Canada
BC	Bureau consultatif
BM	Bien-être et maintien du moral
BNP	Biens non publics
BPR	Bureau de première responsabilité
CE	Chef de l'exploitation
CPVP	Commissariat à la protection de la vie privée
CT	Conseil du Trésor
DPI	Dirigeant principal de l'information
DPRH	Dirigeant principal des ressources humaines
EFVP	Évaluation des facteurs relatifs à la vie privée
FAC	Forces armées canadiennes
FNP	Fonds non publics
FRP	Fichier de renseignements personnels
GI	Gestion de l'information
GN AIPRP	Gestionnaire national, Accès à l'information et protection des renseignements personnels
GRC	Gendarmerie royale du Canada
MDN	Ministère de la Défense nationale
PON	Procédure opérationnelle normalisée
RARM	Régime d'assurance-revenu militaire
SBMFC	Services de bien-être et de maintien du moral des Forces canadiennes
SCT	Secrétariat du Conseil du Trésor
SGC	Secrétaire général en chef
SI	Sécurité de l'information
SMA(Svcs Ex)	Sous-ministre adjoint (Services d'examen)
TI	Technologie de l'information

Sommaire des résultats

La *Loi sur la protection des renseignements personnels* régit les pratiques des organisations fédérales concernant le traitement des renseignements personnels. Cette loi, qui est entrée en vigueur le 1er juillet 1983, encadre la collecte, l'utilisation, l'échange, la divulgation et l'élimination des renseignements personnels des personnes. Au sens de la *Loi*, les renseignements personnels sont des renseignements, quels que soient leur forme et leur support, qui concernent une personne identifiable et qui peuvent être utilisés seuls ou en combinaison avec d'autres renseignements afin d'identifier une personne.

La Politique sur la protection de la vie privée et la Directive sur les pratiques relatives à la protection de la vie privée du Conseil du Trésor (CT) obligent les organisations fédérales à protéger les renseignements personnels qu'elles recueillent.

Depuis sa création en avril 2017, le programme sur l'accès à l'information et la protection des renseignements personnels (AIPRP) des Services de bien-être et de maintien du moral des Forces canadiennes (SBMFC) a déployé des efforts considérables pour établir un cadre solide de gestion de la protection de la vie privée. Dans plusieurs domaines, nous avons relevé des pratiques positives en matière de protection de la vie privée. Nous avons également identifié des domaines nécessitant des améliorations.

Nous avons examiné la gestion des pratiques en matière de protection de la vie privée au sein des SBMFC. L'ensemble du personnel est responsable des pratiques en matière de protection de la vie privée, mais le gestionnaire national de l'AIPRP (GN AIPRP), qui fait partie de la Division des services généraux des SBMFC, dirige les efforts globaux en matière de protection de la vie privée pour les SBMFC. Les principales responsabilités du programme d'AIPRP comprennent les suivantes : élaborer des politiques, des procédures et des pratiques en matière de protection de la vie privée; offrir au personnel des programmes de formation et de sensibilisation à la protection de la vie; évaluer et signaler les atteintes à la vie privée; coordonner et évaluer la contribution des SBMFC à *InfoSource*; ainsi qu'effectuer des analyses et formuler des conseils en matière de protection de la vie privée à l'aide d'un certain nombre d'outils, comme les évaluations des facteurs relatifs à la vie privée (EFVP).

Principales constatations et recommandations

Les SBMFC ont conscience que la protection des renseignements personnels est une composante centrale de la mise en œuvre de programmes et d'activités organisationnelles. Les SBMFC ont élaboré un cadre de gestion de la protection de la vie privée qui fixe les responsabilités et les politiques relatives au traitement des renseignements personnels conformément à la *Loi sur la protection des renseignements personnels* et aux politiques et directives pertinentes du CT.

Conclusion générale

- Les SBMFC disposent d'un cadre de gestion de la protection de la vie privée bien défini.
- Des mesures de contrôle clés sont en place pour protéger les renseignements personnels.

Bien que les pouvoirs délégués au GN AIPRP en tant que responsable fonctionnel soient clairs en vertu de la *Loi*, des responsabilités plus précises sont nécessaires; en effet, il faut s'assurer que les divisions évaluent les risques d'atteinte à la vie privée dans le cadre de leurs programmes et qu'elles adoptent des mesures de contrôle telles que la formation du personnel et la surveillance des tiers afin de protéger les renseignements personnels d'une manière proportionnelle à leur sensibilité.

Il est possible d'améliorer la sécurité des renseignements personnels conservés dans les bases de données opérationnelles des SBMFC en renforçant les activités de surveillance et de conformité associées aux diverses bases de données et en éliminant les renseignements personnels des bases de données lorsqu'ils n'ont plus d'utilité.

Nota : Se reporter à l'annexe A – Plan d'action de la direction pour obtenir de plus amples renseignements sur la réponse de la direction aux recommandations du SMA(Svcs Ex).

1.0 Introduction

1.1 Contexte

Les SBMFC sont responsables de l'administration des biens non publics (BNP) au nom du chef d'état-major de la défense ainsi que de la prestation de certains services et certaines activités en matière de bien-être et de moral (BM) à l'intention des militaires admissibles et leurs familles. Les programmes de BM appartiennent à l'une des deux catégories suivantes :

a) Programmes publics : programmes de BM qui sont (à quelques exceptions près) remboursés à 100 % par le public et qui constituent une responsabilité publique;

b) Programmes de BM des BNP : programmes de BM qui peuvent avoir une composante publique, mais dont certains éléments de coût peuvent bénéficier d'un niveau de soutien public inférieur à 100 %. Ces programmes relèvent des BNP.

Puisqu'ils recueillent, utilisent et divulguent des informations personnelles, les SBMFC sont assujettis aux exigences de la *Loi sur la protection des renseignements personnels*. Ils sont également assujettis aux politiques et directives émises par le CT qui appuient l'administration de la *Loi*; principalement, la Politique sur la protection de la vie privée, la Directive sur les pratiques relatives à la protection de la vie privée et la Directive sur l'évaluation des facteurs relatifs à la vie privée.

La *Loi* fournit le cadre juridique de la collecte, de l'utilisation, de la divulgation et de l'élimination de renseignements personnels par les organisations fédérales. Elle repose sur le principe selon lequel les personnes ont le droit de savoir quels renseignements sont recueillis à leur sujet et comment ceux-ci seront utilisés dans l'administration de services et programmes du gouvernement.

La *Loi* énonce les règles régissant la gestion des renseignements personnels détenus par les organisations du gouvernement fédéral. Les articles 4 à 8 restreignent la collecte de renseignements personnels et limitent la façon dont ces renseignements, une fois recueillis, peuvent être utilisés et divulgués.

La *Loi* concerne également la conservation et l'élimination des renseignements personnels. Elle établit un équilibre entre les besoins légitimes de collecte et d'utilisation essentiels aux programmes gouvernementaux et le droit d'une personne à une attente raisonnable en matière de protection de la vie privée.

La Politique sur la protection de la vie privée et la Directive sur les pratiques relatives à la protection de la vie privée du CT obligent les organisations fédérales à protéger les renseignements personnels qu'elles recueillent. La politique du CT établit des exigences de base en matière de sécurité pour protéger les fonds de renseignements, y compris les renseignements personnels. Toutefois, les organisations sont chargées de mener leurs propres évaluations pour déterminer si des mesures de protection supérieures au niveau de base sont nécessaires.

Avant l'année financière 2017-2018, les activités d'AIPRP liées aux BNP et au Personnel des fonds non publics (FNP), Forces canadiennes étaient gérées par le bureau de l'AIPRP du ministère de la Défense nationale (MDN).

À la suite de l'approbation ministérielle du décret de désignation de l'AIPRP BNP en février 2017, et puisque le Personnel des FNP, Forces canadiennes est un organisme distinct, les SBMFC ont établi leur propre bureau d'AIPRP, lequel a lancé ses activités en avril 2017.

Le GN AIPRP administre les dispositions de la *Loi sur la protection des renseignements personnels* au sein des SBMFC pour les BNP et le Personnel des FNP, Forces canadiennes.

Il rend compte au directeur – Services généraux qui, à son tour, rend compte au vice-président, Services généraux (secrétaire général en chef [SGC]).

De plus, il est responsable de la gestion de toutes les activités liées au programme d'AIPRP des SBMFC, conformément au décret de désignation de l'AIPRP BNP et aux dispositions de la *Loi sur la protection des renseignements personnels*, ainsi qu'aux règlements, directives, politiques et lignes directrices applicables.

Bien que l'AIPRP joue un rôle de premier plan dans l'élaboration et le soutien de pratiques en matière de protection de la vie privée dans l'ensemble des SBMFC, la responsabilité de la protection et du traitement des renseignements personnels au sein des SBMFC est partagée entre l'AIPRP et les divisions. Bien que les pouvoirs délégués en vertu de la *Loi sur la protection des renseignements personnels* sont confiés au GN AIPRP, les divisions doivent appuyer le responsable fonctionnel en s'assurant que les renseignements personnels sous leur contrôle sont gérés conformément à la *Loi sur la protection des renseignements personnels*. Cela comprend, entre autres, l'évaluation des risques d'atteinte à la vie privée dans le cadre de leur programme, la protection des renseignements personnels d'une manière proportionnelle à leur sensibilité, la réalisation d'une EFVP au besoin, l'atténuation des risques d'atteinte à la vie privée au moyen de la formation, ainsi que la surveillance et la notification immédiate de l'AIPRP en cas de violation.

1.2 Justification

Les personnes sont de plus en plus préoccupées par la protection et la sécurité de leurs renseignements personnels. Cette préoccupation accroît la pression exercée sur les organisations pour qu'elles s'attaquent aux problèmes de protection de la vie privée et des données. La nécessité de protéger les données contre la perte, le vol ou l'utilisation abusive a fait naître un tout nouveau domaine de risque pour les organisations. Les nouvelles technologies axées sur les données ont soulevé de nouvelles préoccupations en matière de protection des données et de la vie privée.

Les SBMFC recueillent des renseignements personnels dans le cadre de l'administration de certains avantages sociaux payés par l'employeur pour les membres des Forces armées canadiennes (FAC) et le Personnel des FPN, ainsi que de la prestation de services directement aux membres des FAC, aux vétérans et à leurs familles, et au personnel d'autres organisations fédérales comme la Gendarmerie royale du Canada (GRC) et la Garde côtière canadienne.

À ce titre, les SBMFC possèdent et utilisent les renseignements personnels de leurs membres/clients, et la protection de ces renseignements est cruciale. Les atteintes à la vie privée pourraient nuire aux personnes ainsi qu'à la réputation des SBMFC. Le présent audit a permis d'examiner le cadre général de gestion de la protection de la vie privée en place pour régir les fonds de données et de renseignements personnels des SBMFC, et de formuler certaines recommandations sur la façon de mieux protéger les renseignements personnels dont ils ont la charge et le contrôle.

1.3 Objectif

Le présent audit a pour but d'évaluer le cadre de gestion de la protection de la vie privée des SBMFC et de déterminer si les politiques, procédures et pratiques de gestion des renseignements personnels sont conformes à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes du CT.

2.0 Constatations et recommandations

2.1 Cadre de gestion de la protection de la vie privée

Les éléments clés d'un programme complet de gestion de la protection de la vie privée sont en place.

En vertu de la Politique sur la protection de la vie privée, les responsables d'organisations sont tenus d'établir des pratiques de gestion pour appliquer la *Loi sur la protection des renseignements personnels.* En général, ces pratiques de gestion sont régies par un cadre ministériel ou organisationnel de gestion de la protection de la vie privée. Dans un tel cadre, on retrouve les structures, politiques, procédures et processus en place pour s'assurer qu'une organisation gouvernementale respecte ses obligations en vertu de la *Loi sur la protection des renseignements personnels*. Parmi les éléments de base, citons une gouvernance efficace, des responsabilités claires, un protocole en cas d'atteinte à la vie privée, un processus d'identification et de gestion des risques d'atteinte à la vie privée et une formation de sensibilisation.

Pratiques notables

- Les SBMFC disposent d'un cadre général de gestion de la protection de la vie privée pour orienter les activités dans ce domaine.
- La responsabilité en matière de respect de la vie privée est définie dans les politiques internes.
- Des normes et pratiques communes pour le traitement des renseignements personnels ont été établies.

Un cadre de gestion de la protection de la vie privée peut servir de fondement pour établir et mettre en œuvre un programme complet de protection des renseignements personnels qui répond aux obligations et aux risques en matière de protection de la vie privée tout en facilitant les occasions d'affaires actuelles et futures.

L'équipe d'audit a effectué une évaluation des politiques, procédures et pratiques des SBMFC en matière de protection de la vie privée en fonction des exigences du CT contenues dans sa Politique sur la protection de la vie privée, sa Directive sur l'évaluation des facteurs relatifs à la vie privée et sa Directive sur les pratiques relatives à la protection de la vie privée. Dans l'ensemble, les politiques ont été jugées conformes aux exigences de la *Loi sur la protection des renseignements personnels* et des politiques et directives connexes.

L'audit a permis de constater que la Direction de l'AIPRP a mis en place plusieurs politiques et procédures devant servir à faciliter la gestion et la protection des renseignements personnels dont les SBMFC ont la charge et le contrôle. En règle générale, ces politiques et procédures étaient concises et faciles à comprendre. De plus, elles sont accessibles à tout le personnel à partir du site intranet de l'organisation. En avril 2021, la Politique en matière de cybersécurité des SBMFC et les directives connexes sont entrées en vigueur. Ces documents définissent les exigences relatives à la protection des informations détenues sous forme électronique tout au long de leur cycle de vie.

2.2 Rôles et responsabilités

En vertu de la *Loi sur la protection des renseignements personnels*, les responsables d'organisations gouvernementales peuvent déléguer certains pouvoirs ou fonctions prévus par la *Loi* à un ou plusieurs dirigeants ou employés. Une fois qu'une ordonnance de délégation de pouvoirs a été signée, les fonctions et les pouvoirs délégués ne peuvent être exercés ou exécutés que par l'administrateur général ou ses représentants désignés. La Politique sur la protection de la vie privée et la Directive sur les pratiques relatives à la protection de la vie privée du CT établissent clairement les responsabilités en matière de prise de décision sur les questions relevant de la *Loi* et la responsabilité de la gestion des renseignements personnels au sein d'une organisation.

Par le biais d'une ordonnance de délégation de pouvoirs, l'autorité pour certaines exigences légales et réglementaires a été confiée au GN AIPRP. Ce dernier rend compte au directeur – Services généraux qui, à son tour, rend compte au vice-président, Services généraux (au sein de l'organisation du SGC). La Section de l'AIPRP, composée d'une seule personne, est responsable de la gestion de toutes les activités liées au programme d'AIPRP des SBMFC, conformément au décret de désignation de l'AIPRP BNP et aux dispositions de la *Loi sur la protection des renseignements personnels*, ainsi qu'aux règlements, directives, politiques et lignes directrices applicables. En outre, les divisions des SBMFC facilitent l'administration de la *Loi*. En effet, chaque division dispose d'un point de contact d'AIPRP qui coordonne la collecte de renseignements. Les agents de liaison fournissent de l'aide au GN AIPRP en recherchant et en rassemblant les documents relatifs aux demandes de renseignements personnels dans leurs divisions respectives.

Bien que l'AIPRP joue un rôle de premier plan dans l'élaboration et le soutien de pratiques en matière de protection de la vie privée dans l'ensemble des SBMFC, la responsabilité de la protection et du traitement des renseignements personnels au sein des SBMFC est partagée entre l'AIPRP et les divisions. De plus, bien que les pouvoirs délégués en vertu de la *Loi sur la protection des renseignements personnels* sont confiés au GN AIPRP, les divisions doivent appuyer le responsable fonctionnel en s'assurant que les renseignements personnels sous contrôle des divisions sont gérés conformément à la *Loi sur la protection des renseignements personnels*. Cela comprend, entre autres, la protection des renseignements personnels d'une manière proportionnelle à leur sensibilité, la réalisation d'une EFVP au besoin ainsi que la notification immédiate de l'AIPRP en cas d'atteinte à la vie privée.

Les responsabilités en matière de protection de la vie privée au sein des SBMFC sont décrites dans plusieurs documents mis à disposition à l'interne, notamment les suivants : la Politique sur le Programme d'accès à l'information et de protection des renseignements personnels et la Politique sur les pratiques relatives à la protection de la vie privée des SBMFC. Toutefois, les responsabilités justifiées des responsables de programme et du personnel des SBMFC en matière de protection de la vie privée ne tiennent pas compte du type et de la sensibilité des renseignements traités par ces derniers.

De plus, la responsabilité des responsables de programme d'évaluer les risques d'atteinte à la vie privée de leurs propres programmes et d'intégrer des mesures de protection de la vie privée dans les systèmes, les procédures et la formation liés aux programmes n'est pas explicitement définie.

Recommandation du SMA(Svcs Ex)

1. Les SBMFC devraient établir des responsabilités en matière de protection de la vie privée pour le personnel de division et de programme afin d'assurer une responsabilisation claire dans ce domaine.

BPR : SGC
BC : Toutes les divisions

2.3 Évaluation des facteurs relatifs à la vie privée

Les SBMFC ont mis en place un processus d'EFVP, lequel comprend une politique visant à informer le personnel et les parties prenantes de la directive sur l'EFVP et de ses exigences.

En vertu de la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor du Canada (SCT) (entrée en vigueur le 1er avril 2010), les organisations fédérales sont tenues d'instaurer un processus officiel pour déterminer et atténuer les risques d'atteinte à la vie privée lors de la mise en place de toute activité ou de tout programme, nouveau ou considérablement modifié, qui fait appel à des renseignements personnels. La Directive sur l'évaluation des facteurs relatifs à la vie privée établit les éléments de base de la conduite des EFVP, qui se concentrent sur les obligations légales liées à la protection de la vie privée. Les organisations fédérales doivent présenter leurs rapports d'EFVP définitifs au Commissariat à la protection de la vie privée (CPVP) avant de mettre en œuvre les programmes ou services.

Le processus d'EFVP aide à garantir que toutes les préoccupations concernant la protection de la vie privée ont été correctement cernées, évaluées et réglées avant la mise en œuvre d'une activité ou d'un programme nouveau ou considérablement modifié faisant appel à des renseignements personnels. L'EFVP est la composante des activités ministérielles de gestion du risque qui se concentre sur l'élaboration de mesures de protection de la vie privée appropriées dans le cadre de nouveaux programmes ou de nouvelles activités.

Les SBMFC ont mis en œuvre un processus officialisé pour se conformer à la Directive sur l'évaluation des facteurs relatifs à la vie privée du SCT, y compris les rôles et les responsabilités, ainsi que les étapes à suivre pour déterminer la nécessité d'une EFVP et pour effectuer l'évaluation.

Les SBMFC ont établi des procédures pour s'assurer que lors de l'élaboration de chaque nouvelle initiative de programme, on se penche sur la nécessité d'effectuer des EFVP. Le

GN AIPRP travaille en étroite collaboration avec les responsables de la gestion de l'information (GI) et de la technologie de l'information (TI) pour cerner et atténuer les risques en matière de sécurité liés à la mise en place de nouveaux systèmes de TI. Déterminer si une EFVP est nécessaire est l'une des étapes du cycle de vie normal d'un projet de TI.

Les gestionnaires de programme sont responsables de prévoir des EFVP pour tous les nouveaux programmes et services sous leur contrôle, tandis que l'unique responsable de la Section de l'AIPRP est chargé de faciliter le processus d'EFVP au sein des SBMFC, de fournir des outils de protection de la vie privée et d'approuver les EFVP avant l'examen par le CPVP. À ce jour, une seule EFVP officielle a été réalisée par les SBMFC.

Les opérations en cours présentent également des risques d'atteinte à la vie privée. Plusieurs bases de données des SBMFC ont été créées avant que l'EFVP ne devienne une exigence. Par conséquent, il est difficile de savoir si toutes les répercussions sur la protection de la vie privée ont été cernées et traitées. À l'heure actuelle, le GN AIPRP travaille avec les divers secteurs de programme pour aider à cerner et à traiter les risques liés à la protection de la vie privée dans les opérations en cours.

Recommandation du SMA(Svcs Ex)

2. Les SBMFC devraient examiner régulièrement les opérations en cours dans le but de cerner les risques liés à la protection de la vie privée qui en découlent et s'assurer que des mesures de contrôle sont en place pour atténuer ces risques.

BPR : SGC
BC : CE

2.4 Formation et sensibilisation

La Politique sur la protection de la vie privée du CT prévoit que l'administrateur général ou ses représentants désignés soient responsables de sensibiliser le personnel aux politiques, procédures et obligations légales découlant de la *Loi sur la protection des renseignements personnels*. Il est essentiel que le personnel des SBMFC comprenne comment protéger adéquatement les renseignements personnels, car un manque de sensibilisation pourrait entraîner un incident majeur lié à la protection de la vie privée et nuire à la réputation des SBMFC. Par conséquent, il est crucial de mettre en œuvre un programme de formation sur la sensibilisation à la protection de la vie privée afin de permettre à tout le personnel de protéger les renseignements personnels de façon proactive. Une formation sur la protection de la vie privée aidera le personnel à cerner et à atténuer les risques en la matière.

Il est important de former et de sensibiliser tout le personnel à la protection de la vie privée, en particulier les personnes qui sont amenées à traiter régulièrement des renseignements personnels. On pourrait notamment inclure un aperçu des notions relatives à la protection de la vie privée dans le programme d'orientation des nouveaux membres du personnel. Les objectifs d'apprentissage devraient inclure de comprendre leurs responsabilités en tant qu'intendants

des données pour identifier et protéger les renseignements personnels, et savoir quand et comment signaler un incident en matière de protection de la vie privée.

Le programme de formation et de sensibilisation des SBMFC comprend la tenue de séances d'information informelles à l'intention des chefs de division et des équipes de gestion, ainsi qu'une présentation réalisée au cours de l'année financière 2017-2018 à l'intention du Conseil de gestion. Des conseils sont également offerts aux gestionnaires et au personnel à tous les niveaux, selon les besoins. L'audit a relevé un certain nombre de cas où des gestionnaires de programmes ont demandé des conseils à l'AIPRP sur l'application de la *Loi sur la protection des renseignements personnels* et des politiques et directives connexes. Quelques membres du personnel ont suivi le cours gratuit en ligne intitulé Cours de base sur l'accès à l'information et la protection des renseignements personnels, offert sur GCcampus.

Bien que les SBMFC aient mis en place une formation obligatoire sur la sensibilisation à la sécurité, celle-ci est axée sur le traitement confidentiel des renseignements personnels et non sur les responsabilités plus vastes prévues par la *Loi sur la protection des renseignements personnels*. La sécurité et la protection de la vie privée sont deux concepts différents. En l'absence d'une formation sur la sensibilisation à la protection de la vie privée adaptée aux particularités des SBMFC, la probabilité que les membres du personnel ne soient pas conscients de leurs responsabilités et de ce qu'ils doivent faire en cas d'atteinte à la vie privée augmente.

À l'avenir, les SBMFC ont l'intention de rendre le Cours de base sur l'accès à l'information et la protection des renseignements personnels obligatoire pour tout son personnel. Étant donné que la formation sur l'AIPRP n'est plus offerte à l'ensemble du personnel des SBMFC sur GCcampus, ceux-ci élaboreront leur propre cours de formation sur les principes fondamentaux de l'AIPRP pour tous les employés. Bien que cette initiative soit importante et louable, le programme de sensibilisation à l'AIPRP des SBMFC, tel qu'il est conçu actuellement, ne procure pas aux membres du personnel une connaissance générale des principes fondamentaux de la protection de la vie privée qui leur permet de tenir pleinement compte des répercussions sur la vie privée lorsqu'ils offrent des services. Les SBMFC bénéficieraient d'une stratégie complète de sensibilisation à la protection de la vie privée conçue spécifiquement pour le personnel qui manipule des renseignements personnels au quotidien.

Il est également important de fournir des conseils sur la façon d'appliquer les principes de protection de la vie privée dans les activités quotidiennes du programme. Par ailleurs, l'audit a permis de constater que des procédures opérationnelles normalisées (PON) existent pour certains programmes des SBMFC. Ces PON régissent la collecte et l'utilisation des renseignements personnels et offrent des directives au personnel de première ligne sur la meilleure façon d'exercer ses obligations en vertu de la *Loi sur la protection des renseignements personnels*. Toutefois, des efforts supplémentaires sont nécessaires pour s'assurer que des PON sont en place pour tous les fonds de données de renseignements personnels des SBMFC.

Recommandation du SMA(Svcs Ex)

3. Les SBMFC devraient élargir leur programme actuel de sensibilisation et de formation à la protection de la vie privée en y ajoutant des exigences de formation pour le personnel qui participe le plus activement au traitement des renseignements personnels. Ils devraient également s'assurer de mettre en place des PON pour tous leurs fonds de données de renseignements personnels.

BPR : SGC
BC : DPRH

2.5 Avis/fins de la collecte de renseignements

Les SBMFC respectent les dispositions relatives aux avis prévues dans la *Loi sur la protection des renseignements personnels*.

Conformément au paragraphe 5(2) de la *Loi sur la protection des renseignements personnels*, une organisation fédérale est tenue d'aviser les personnes auprès desquelles elle recueille des renseignements personnels les concernant des fins de cette collecte. Au moment de la collecte, la personne qui fournit les renseignements personnels doit être avisée de la raison pour laquelle ces renseignements sont recueillis, à moins que cela n'entraîne la collecte de renseignements inexacts ou ne compromette la finalité ou l'utilisation pour laquelle les renseignements sont recueillis.

Pratiques notables

- Les pratiques de collecte ne dépassent pas les limites du mandat législatif.
- Les SBMFC limitent leur collecte et leur utilisation de renseignements personnels aux renseignements qui sont directement liés à leurs activités opérationnelles.

En vertu de l'alinéa 6.2.9 de la Directive sur les pratiques relatives à la protection de la vie privée, les organisations doivent aviser directement la personne dont les renseignements sont recueillis des éléments suivants :

1. les fins de la collecte et en vertu de quelle autorité elle est faite;
2. tout usage ou divulgation conforme à la fin originale;
3. tout usage ou divulgation qui n'est pas lié à la fin originale;
4. toute conséquence administrative ou légale découlant d'un refus de fournir les renseignements personnels;
5. les droits d'accès, de correction et de protection des renseignements personnels en vertu de la *Loi*;

L'avis de confidentialité et les formulaires d'inscription/d'adhésion des SBMFC, qui se trouvent sur Internet, résument leurs pratiques en matière de protection de la vie privée. Ils indiquent notamment que les SBMFC recueillent des renseignements personnels en vertu de la *Loi sur la défense nationale* et précisent les fins auxquelles ces renseignements sont recueillis. L'avis de

confidentialité comprend également des références à la façon dont les renseignements peuvent être utilisés et à la façon dont on peut retirer son consentement.

Lors de la création d'un formulaire qui nécessite la collecte de renseignements personnels, la Politique sur les pratiques relatives à la protection de la vie privée des SBMFC exige que les gestionnaires consultent le GN AIPRP pour un examen de la conformité et pour l'ajout de la déclaration de consentement et de l'avis de confidentialité appropriés. Des entrevues avec la haute direction et un examen de la correspondance entre les divisions et le GN AIPRP montrent que ce dernier a été consulté lors de l'élaboration de nouveaux formulaires. Le GN AIPRP a également pris l'initiative d'examiner les formulaires actuels et de remettre en question la collecte de certains renseignements.

2.6 Limitation de la collecte et de l'utilisation

Un bon cadre de gestion de la protection de la vie privée doit garantir qu'une organisation ne recueille que les renseignements dont elle a besoin dans l'immédiat et qu'elle est autorisée à recueillir. Le pouvoir des SBMFC de recueillir des renseignements personnels relève de la *Loi sur la défense nationale*.

Conformément au paragraphe 4 de la *Loi sur la protection des renseignements personnels*, les seuls renseignements personnels que peut recueillir une organisation fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités. L'organisation doit avoir l'autorisation légale pour le programme ou l'activité en question et pouvoir démontrer son besoin de recueillir chaque élément de renseignements personnels qu'elle recueille. Les renseignements personnels ne peuvent être utilisés qu'aux fins pour lesquelles ils ont été obtenus ou pour un usage compatible avec ces fins.

Les SBMFC recueillent les renseignements personnels nécessaires à l'administration de divers programmes et services. En plus des données biographiques (p. ex., noms, adresses, dates de naissance, état matrimonial, numéros matricules), des renseignements financiers, médicaux et militaires sont recueillis.

Les SBMFC reconnaissent l'importance de vérifier que les fonds de données de l'organisation ne contiennent que des renseignements qu'ils sont autorisés à recueillir en vertu de la loi. De plus, ils ont adopté un certain nombre de mesures concrètes au cours des dernières années pour limiter la collecte de renseignements personnels à ce qui est nécessaire pour la mise en œuvre de ses programmes. Les renseignements personnels sont généralement recueillis auprès de la personne à laquelle ils se rapportent, à quelques exceptions près qui sont actuellement à l'étude.

Les fichiers de renseignements personnels (FRP) sont des descriptions de renseignements personnels relevant d'une organisation fédérale qui sont organisés et qui peuvent être récupérés au moyen du nom d'une personne ou par un numéro, un symbole ou d'autres éléments qui identifient cette personne. En vertu de la *Loi sur la protection des renseignements*

personnels, les responsables d'organisations gouvernementales sont tenus d'identifier et de décrire leurs FRP, ainsi que de les rendre publics. Les FRP sont les voies par lesquelles une organisation gouvernementale informe le public des renseignements personnels qu'elle recueille. Grâce à ces descriptions, les personnes peuvent également apprendre comment leurs renseignements personnels sont utilisés et pendant combien de temps ils sont conservés.

L'équipe d'audit a examiné un échantillon de formulaires d'inscription/d'adhésion utilisés pour recueillir des renseignements personnels ainsi que les renseignements énumérés dans les FRP propres à l'organisation correspondants des SBMFC, afin de confirmer que les renseignements personnels recueillis au moyen des formulaires étaient conformes aux renseignements indiqués dans les FRP.

Pour les deux programmes examinés, l'audit a révélé que des FRP avaient été établis pour définir et approuver la collecte de renseignements conformes au programme, et que les formulaires d'inscription/d'adhésion recueillaient des renseignements conformes aux FRP.

2.7 Limitation de la divulgation

Conformément au paragraphe 8(1) de la *Loi sur la protection des renseignements personnels*, les renseignements personnels qui relèvent d'une organisation gouvernementale ne peuvent être communiqués par celle-ci sans le consentement de la personne concernée, obtenu au moment de la collecte initiale des renseignements.

Le paragraphe 8(2) de cette même loi énumère 13 motifs autorisés de divulgation sans consentement.

L'avis de confidentialité général des SBMFC, les FRP propres à un programme et l'avis sur les formulaires propres à un programme décrivent la façon dont les renseignements personnels recueillis peuvent être communiqués.

L'équipe d'audit a examiné un échantillon de formulaires d'inscription/d'adhésion utilisés par les SBMFC et a constaté que les avis de divulgation de renseignements figurant sur les formulaires utilisés par les personnes pour fournir leurs renseignements et pour donner leur consentement à la divulgation de ces renseignements correspondaient aux FRP et à l'avis de confidentialité des SBMFC. Par conséquent, les personnes qui ont donné leur consentement étaient bien informées des circonstances possibles dans lesquelles leurs renseignements personnels pouvaient être divulgués.

2.8 Entente sur l'échange de renseignements avec des tiers fournisseurs de services

La Directive sur les pratiques relatives à la protection de la vie privée du CT exige que les contrats établis avec des entités du secteur privé prévoient des mesures et des dispositions concernant ce qui suit :

- contrôle des renseignements personnels;
- restrictions régissant la collecte et le traitement des renseignements personnels, ainsi que toute interdiction relative aux renseignements aux fins du contrat;
- retrait des renseignements personnels, s'il y a lieu;
- mesures de protection administratives, techniques et physiques;
- obligations des autres parties agissant au nom de l'organisation fédérale.

Les organisations assujetties à la *Loi sur la protection des renseignements personnels* sont responsables des renseignements personnels qui sont sous leur contrôle. La sous-traitance d'un programme ou d'un service ne libère pas une organisation de ses obligations en matière de protection de la vie privée. Des faiblesses dans la conception, le fonctionnement ou l'efficacité des mesures de contrôle des tiers, ou l'absence de telles mesures, pourraient entraîner des atteintes à la vie privée. Par conséquent, les contrats avec des tiers devraient contenir des dispositions appropriées concernant les mesures de contrôle relatives à la protection des renseignements personnels et de la vie privée. Ils devraient également prévoir des exigences en matière de surveillance ou d'audit afin de garantir que les renseignements recueillis ou transférés à des tiers sont sécurisés tout au long de leur cycle de vie.

Les SBMFC ont conclu des contrats avec des tiers dans divers secteurs, y compris le secteur bancaire et celui des assurances, ainsi qu'avec des entreprises commerciales, afin de faciliter l'offre de programmes et de services. Compte tenu de la sensibilité et du volume des données divulguées par les SBMFC à des tiers, et des conséquences associées à d'éventuelles atteintes à la protection des données, des ententes appropriées sur l'échange de renseignements constituent un moyen important d'atténuer certains des risques associés aux transferts de données.

Un examen de plusieurs instruments de politique internes a révélé que les politiques et les directives en place pour la passation de marchés avec des tiers sont assez prescriptives. Nous avons examiné les conditions générales des SBMFC en ce qui a trait à la passation de marchés avec des tiers fournisseurs de services. Elles stipulent que l'entrepreneur doit protéger le caractère privé et confidentiel de tout renseignement personnel recueilli, créé ou traité par l'entrepreneur dans le cadre de l'exécution de tout contrat, et ne doit pas utiliser, copier, divulguer, éliminer ou détruire ces renseignements autrement qu'en conformité avec les dispositions du contrat. Nous avons également examiné la directive sur la cybersécurité et les personnes (Directive on Cybersecurity and People) des SBMFC, laquelle exige que les ententes sur l'échange de renseignements avec les fournisseurs externes définissent les exigences en matière de protection des renseignements confidentiels. La directive des SBMFC est conforme

aux exigences de la *Loi sur la protection des renseignements personnels* et aux orientations du SCT sur les clauses de protection de protection de la vie privée dans les contrats.

La directive des SBMFC, qui exige des clauses spécifiques sur la protection de la vie privée dans les contrats officiels avec des tiers, est louable. L'audit a également permis de constater que le GN AIPRP consulte régulièrement les gestionnaires de programmes sur les aspects de la protection de la vie privée qui devraient être inclus dans les ententes avec les tiers. Toutefois, nous n'avons pas été en mesure de confirmer le nombre d'ententes sur l'échange de renseignements en vigueur au moment de l'audit. Sans un inventaire à jour des tiers et des raisons du transfert de renseignements personnels, il n'est pas possible de confirmer que des clauses appropriées ont été incluses aux contrats officiels.

Comme ils l'ont reconnu lors des entrevues, les SBMFC n'ont pas mis en place un processus officiel pour surveiller la conformité des tiers aux clauses de protection de la vie privée contenues dans les ententes. Les programmes des SBMFC s'appuient plutôt sur la vigilance et la réglementation accrues imposées dans les secteurs des services financiers et des assurances. Il se peut que cette pratique ne soit pas suffisante pour garantir que les pratiques de traitement des données sont conformes aux conditions des ententes et qu'elles assurent efficacement la protection des renseignements personnels.

Recommandation du SMA(Svcs Ex)

4. Les SBMFC devraient tenir à jour un inventaire des ententes commerciales dans le cadre desquelles des renseignements personnels sont transférés à un tiers, et obtenir l'assurance que les pratiques de traitement des données de leurs partenaires sont conformes aux modalités de leurs ententes sur l'échange de renseignements.

BPR : CE, SGC
BC : DPI, chefs de division

2.9 Limitation de la conservation

En vertu du paragraphe 6(1) de la *Loi sur la protection des renseignements personnels*, les organisations doivent conserver les renseignements personnels utilisés à des fins administratives afin de s'assurer que la personne concernée a une possibilité raisonnable d'accéder à ces renseignements si elle le désire. De plus, le paragraphe 6(3) précise que l'élimination définitive des renseignements personnels qui relèvent d'une organisation doit être effectuée de manière sécuritaire et conforme aux autorisations en matière d'élimination des documents de Bibliothèque et Archives Canada (BAC).

Les organisations fédérales doivent élaborer des calendriers de conservation et d'élimination pour gérer leurs documents. Ces calendriers établissent la durée de conservation des documents avant leur élimination ou leur transfert à BAC. À cette fin, le bibliothécaire et archiviste du Canada émet des autorisations de disposition de documents.

Un calendrier de conservation et d'élimination des documents est important du point de vue de la protection de la vie privée, car la conservation des documents au-delà de la période où ils sont utilisés dans le cadre du programme expose les renseignements à un risque d'utilisation abusive sans aucun avantage pour le programme.

Les SBMFC ont documenté les périodes de conservation pour la plupart de leurs fonds de données, comme l'indique *InfoSource*. Bien que ces périodes de conservation aient été fixées en collaboration avec BAC, les SBMFC attendent toujours que BAC leur fournisse des numéros d'autorisation de disposition de documents pour certains de ces fonds de données.

2.10 Élimination

Il peut arriver que certains renseignements soient conservés plus longtemps que la période de conservation requise, car les systèmes de TI ne disposent pas de mécanismes pour éliminer les renseignements personnels qui ne sont plus nécessaires.

Les SBMFC ont l'obligation de protéger les renseignements personnels qu'ils recueillent à partir du moment où ces renseignements sont obtenus jusqu'à ce qu'ils soient éliminés conformément à une méthode approuvée. L'élimination appropriée des renseignements personnels est conséquente avec le fait de ne conserver que les renseignements nécessaires. Les documents doivent être éliminés de manière à ne pas présenter de risque pour la protection de la vie privée.

Nous avons examiné les pratiques d'élimination des SBMFC et avons constaté qu'ils ont élaboré des politiques et des PON pour l'élimination des supports papier et électroniques, comme les CD et les clés USB. Le matériel classifié, désigné ou de nature délicate doit être détruit à l'aide de sacs à brûler ou d'une déchiqueteuse approuvée. Cette opération est effectuée par les services administratifs des SBMFC et est enregistrée. Les documents classifiés ou désignés « Sécurité de l'information » en attente d'être détruits sont entreposés dans un conteneur sécurisé jusqu'à ce qu'ils soient éliminés de façon appropriée.

Bien que nous ayons constaté que les SBMFC disposent de calendriers établissant la durée de conservation des renseignements personnels avant leur destruction, nous avons remarqué que certains des principaux dépôts électroniques pour les renseignements des clients n'ont pas la capacité technique d'éliminer les documents. Ces derniers sont plutôt séparés des dossiers actifs et placés dans un dépôt à accès très restreint. Par conséquent, les renseignements personnels ne sont pas éliminés à la fin de la période de conservation.

Recommandation du SMA(Svcs Ex)

5. Les SBMFC devraient éliminer les données dont ils n'ont plus besoin de leurs bases de données afin de se conformer aux pratiques exemplaires énoncées dans la *Loi sur la protection des renseignements personnels*.

BPR fonctionnel : CE
BPR technique : DPI
BPR des bases de données : RARM et UneFC

2.11 Protection des renseignements personnels

Les SBMFC ont mis en place des mesures de protection administratives, physiques et techniques pour protéger ses fonds de renseignements personnels.

De saines pratiques de sécurité sont essentielles pour répondre aux exigences de protection établies en vertu de la *Loi sur la protection des renseignements personnels.* Des mesures et des mécanismes de contrôle appropriés doivent être en place pour garantir que les renseignements personnels ne font pas l'objet d'un accès, d'une utilisation, d'une divulgation, d'une altération ou d'une élimination non autorisés.

Les dispositions régissant la protection des renseignements personnels sont énoncées dans la Directive sur les pratiques relatives à la protection de la vie privée du SCT. La politique du CT établit des exigences de base en matière de sécurité pour protéger les fonds de renseignements, y compris les renseignements personnels. Toutefois, les organisations sont chargées de mener leurs propres évaluations pour déterminer si des mesures de protection supérieures au niveau de base sont nécessaires.

Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol, ainsi que la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. L'accès aux renseignements ne doit être accordé que sur la base du besoin de connaître et seulement lorsque le personnel a obtenu la cote de sécurité appropriée.

Un examen des Ordonnances de sécurité et politiques en matière de cybersécurité des SBMFC et des directives qui les accompagnent, datant du 1er avril 2021, a révélé que des politiques et des procédures étaient en place pour régir la protection des renseignements personnels tout au long de leur cycle de vie. Ces documents énoncent les pratiques et les procédures de sécurité internes et la responsabilité de chaque membre des SBMFC de se conformer à tous les règlements de sécurité et de maintenir des pratiques de sécurité appropriées.

Bien que les protocoles de sécurité entourant les renseignements personnels varient en fonction du degré de sensibilité de l'information recueillie, les renseignements personnels sous la responsabilité et le contrôle des SBMFC sont généralement protégés par des mesures physiques (p. ex., accès restreint aux zones d'opérations et d'entreposage des documents,

postes de travail verrouillés lorsqu'ils ne sont pas occupés); des mesures organisationnelles (p. ex., cotes de sécurité); et des mesures technologiques (p. ex., contrôles d'accès, systèmes de détection d'intrusion, mots de passe et chiffrement).

2.12 Contrôles d'accès

Les SBMFC disposent d'un processus formel de qualification des utilisateurs pour gérer l'accès (c.-à-d. l'accorder, le modifier ou le retirer) de tous les types d'utilisateurs à tous les systèmes et services.

Lorsque des renseignements personnels ou des données sur les clients sont recueillis, entreposés ou conservés par voie électronique, ils doivent être protégés au moyen de contrôles d'accès appropriés. Le terme « contrôle d'accès » est utilisé pour décrire les solutions physiques et techniques servant à ne permettre l'accès qu'aux personnes autorisées et de restreindre les fonctions qu'elles peuvent exécuter. En règle générale, il convient d'appliquer le principe de droit d'accès minimal, c'est-à-dire de limiter l'accès de chaque utilisateur autorisé aux seules informations et ressources nécessaires à l'exécution de ses tâches et fonctions légitimes.

L'accès automatisé en fonction du rôle dans un système facilite la gestion continue des droits d'accès. Il accorde des autorisations d'accès à certains rôles et assigne des membres du personnel à ces rôles. Les changements apportés au niveau d'accès d'un rôle sont automatiquement appliqués à tous les membres du personnel ayant ce rôle. Les contrôles d'accès doivent être gérés de manière à déterminer quels sont les personnes ou les groupes autorisés, et quels sont leurs rôles et privilèges. On doit également mettre en place des processus pour supprimer les droits d'accès lorsque les personnes n'en ont plus besoin.

Nous avons examiné la façon dont les SBMFC déterminent qui doit avoir accès à ses diverses bases de données et à quels renseignements ces personnes doivent avoir accès dans ces systèmes. Nous avons également examiné les processus et procédures administratifs en place pour la gestion continue de cet accès.

L'audit a permis de constater que les SBMFC disposent de processus et de procédures pour accorder, retirer et gérer l'accès à leurs systèmes, et que les principes du besoin de connaître et du droit d'accès minimal sont observés. Conformément aux Ordonnances de sécurité des systèmes d'information des SBMFC, il est prévu qu'une personne pourra uniquement avoir accès aux renseignements pour lesquels une ou plusieurs autorisations d'accès appropriées et un besoin de connaître établi ont été approuvés. L'accès doit être accordé seulement aux ressources nécessaires à l'exécution des tâches attribuées. L'accès est habituellement contrôlé par une combinaison de méthodes techniques, physiques ou procédurales. Les membres du personnel se voient accorder un accès en fonction de leur poste. S'ils changent de poste, le niveau d'accès est modifié pour refléter les exigences du nouveau poste ou l'accès est retiré en cas de départ ou de congé prolongé.

L'équipe d'audit a été informée que les gestionnaires déterminent les contrôles d'accès, les règles, les droits d'accès et les restrictions appropriés pour chaque rôle d'utilisateur et effectuent des examens périodiques de tous les droits d'accès pour confirmer que ces droits sont toujours appropriés. La portée de cet audit ne comprenait pas le test de l'examen et de l'approbation des droits d'accès par les gestionnaires.

2.13 Surveillance

L'article 6.2.21 de la Directive sur les pratiques relatives à la protection de la vie privée du SCT exige que les organisations gouvernementales adoptent des mesures appropriées pour s'assurer que l'accès, l'utilisation et la divulgation des renseignements personnels sont surveillés et documentés, de sorte que toute activité inappropriée ou non autorisée à cet égard puisse être repérée et rectifiée en temps opportun.

Il est essentiel de consigner et de surveiller l'activité des utilisateurs pour déterminer si les droits d'accès ont été exercés de manière appropriée. Si l'on ne consigne pas de façon exhaustive les accès ainsi que les modifications apportées aux données contenues dans les différentes bases de données des SBMFC, les renseignements personnels peuvent être consultés, utilisés ou divulgués de manière inappropriée sans aucun moyen de détection.

En règle générale, les SBMFC ont mis en place des contrôles pour protéger les renseignements personnels dont ils ont la charge contre une utilisation et une divulgation non autorisées par des forces externes. Les responsables de la TI surveillent le réseau 24 heures sur 24, 7 jours sur 7 pour détecter tout accès non autorisé aux systèmes de TI. Les événements et incidents de cybersécurité sont repérés et traités rapidement afin d'en atténuer les répercussions, et des mesures correctives sont mises en œuvre pour réduire la probabilité et la gravité d'événements et d'incidents similaires.

L'activité des utilisateurs sur les systèmes des SBMFC est consignée. Un enregistrement est créé et consigné lorsque les utilisateurs se connectent, et lorsqu'ils créent, modifient ou suppriment des fichiers sur l'un des réseaux. Toutefois, tous les journaux ne font pas l'objet d'une surveillance active qui permettrait de repérer rapidement un accès inapproprié ou non autorisé à des renseignements personnels dont disposent les utilisateurs internes, ou la divulgation inappropriée ou non autorisée de tels renseignements. Les SBMFC auraient avantage à surveiller régulièrement les journaux et les enregistrements d'audit interne afin de repérer toute trace d'accès, d'utilisation ou de divulgation inappropriés et toute tentative de contourner les protocoles de sécurité.

Recommandation du SMA(Svcs Ex)

6. Les SBMFC devraient mettre en place un outil d'examen du journal d'audit afin de faciliter les enquêtes sur les accès, les utilisations ou les divulgations non autorisés par des utilisateurs internes.

BPR fonctionnel : SGC
BPR technique : DPI
BPR de l'exécution : Toutes les divisions

2.14 Protocole en cas d'atteinte à la vie privée

Le SCT a publié des Lignes directrices sur les atteintes à la vie privée afin d'aider les organisations à éviter les cas d'accès inapproprié ou non autorisé à des renseignements personnels et les cas de divulgation inappropriée ou non autorisée de tels renseignements, ainsi qu'à atténuer les conséquences d'une atteinte à la vie privée, le cas échéant.

Une approche globale du signalement des cas d'atteinte à la vie privée peut aider les organisations à mieux gérer les risques en la matière et leur permettre d'adapter leurs activités commerciales en fonction des leçons retenues. Les Lignes directrices sur les atteintes à la vie privée publiées par le SCT exigent que les organisations établissent des plans et des procédures pour traiter les atteintes à la vie privée.

Les Lignes directrices sur les atteintes à la vie privée des SBMFC décrivent le processus à suivre pour répondre aux atteintes à la vie privée. Ce document contient des mesures pour guider le personnel dans ses responsabilités ainsi que des actions à prendre en cas d'atteinte à la vie privée. La Section de l'AIPRP est chargée d'enquêter sur le cycle de vie d'une atteinte à la vie privée, de gérer ce cycle et d'aviser le SCT et le CPVP au besoin.

L'équipe d'audit a examiné la documentation du GN AIPRP sur sa réponse à plusieurs atteintes à la vie privée survenues au cours des dernières années. L'audit a permis de constater que le GN AIPRP a suivi les Lignes directrices sur les atteintes à la vie privée des SBMFC et du SCT en documentant la nature des atteintes et en les signalant au SCT et au CPVP lorsque nécessaire.

3.0 Conclusion générale

Une atteinte à la vie privée, qu'elle soit intentionnelle ou accidentelle, peut être dévastatrice pour un organisme et les personnes qui en sont victimes. Les risques que court une personne en cas d'atteinte à sa vie privée sont notamment un préjudice à sa réputation, un préjudice financier et, dans certains cas, un préjudice personnel ou des poursuites judiciaires. Pour un organisme, une atteinte à la vie privée peut entraîner de l'embarras, une perte de crédibilité et une plus grande méfiance du public.

L'audit a permis de constater que les SBMFC ont conscience que la protection des renseignements personnels est une composante centrale de la mise en œuvre de programmes et d'activités organisationnelles. Depuis sa création en avril 2017, le programme d'AIPRP des SBMFC a permis de mettre en place un cadre de gestion de la protection de la vie privée qui fixe les responsabilités et les politiques relatives au traitement des renseignements personnels conformément à la *Loi sur la protection des renseignements personnels* et aux politiques et directives pertinentes du CT.

L'audit a permis de relever un certain nombre d'exemples de pratiques positives en matière de protection des renseignements personnels. Parmi ceux-ci, on compte notamment un programme complet de gestion de la protection de la vie privée, des normes et pratiques établies pour le traitement des renseignements personnels, des procédures d'intervention en cas d'incident pour traiter les atteintes à la vie privée, et un processus visant à garantir qu'une EFVP est menée pour tout programme nouveau ou considérablement modifié faisant appel à la collecte et à la conservation de renseignements personnels. Les responsabilités et les obligations du personnel de l'AIPRP et de la sécurité sont coordonnées et appellent à la collaboration. Les SBMFC ont élaboré des mesures de protection administratives, physiques et techniques pour limiter l'accès inapproprié aux renseignements personnels.

Toutefois, il reste du travail à faire pour s'assurer que les divisions ont évalué les risques d'atteinte à la vie privée dans le cadre de leurs programmes afin de garantir que les renseignements personnels sont protégés selon leur degré de sensibilité. L'amélioration des contrôles, des procédures et des pratiques, comme la formation sur la sensibilisation à la protection de la vie privée, l'élaboration de PON, la surveillance lorsque des renseignements personnels sont transférés à des tiers, le contrôle de l'accès interne aux bases de données des SBMFC pour détecter les activités inappropriées et s'assurer de l'élimination des renseignements qui ne sont plus nécessaires permettrait d'améliorer la sécurité des renseignements personnels relevant des SBMFC.

Annexe A – Plan d'action de la direction

Rôles et responsabilités

Recommandation du SMA(Svcs Ex)

1. Le SBMFC devraient établir des responsabilités en matière de protection de la vie privée pour les divisions et le personnel du programme afin d'assurer une responsabilisation claire dans ce domaine.

Mesures de la direction

Mesure 1.1 : Le SBMFC élaboreront des responsabilités et des obligations en matière de protection de la vie privée pour les divisions et le personnel du programme.

BPR : SGC

BC : Toutes les divisions

Date cible : avril 2023

Mesure 1.2 : La Section de l'AIPRP est composée d'une seule personne. En raison de l'augmentation des risques d'atteinte à la vie privée et du grand nombre d'initiatives et de programmes menés par les SBMFC, la demande de services de protection de la vie privée a dépassé la capacité d'une seule personne. Les SBMFC demanderont un financement public pour des ressources supplémentaires en matière d'AIPRP selon les besoins.

BPR : SGC

Date cible : avril 2023

Évaluation des risques

Recommandation du SMA(Svcs Ex)

2. Les SBMFC devraient examiner régulièrement les opérations en cours dans le but de cerner les risques liés à la protection de la vie privée qui en découlent et s'assurer que des mesures de contrôle sont en place pour les atténuer.

Mesures de la direction

Mesure 2.1 : Les SBMFC établiront des procédures pour que les secteurs d'activité examinent les opérations en cours afin d'identifier les risques d'atteinte à la vie privée.

BPR : SGC

BC : CE

Date cible : s/o – processus continu

Mesure 2.2 : Les SBMFC mettront en œuvre des examens des risques d'atteinte à la vie privée dans le cadre des opérations courantes ainsi que des mesures de contrôle pour l'atténuation des risques, au besoin.

BPR : SGC

BC : CE, toutes les divisions

Date cible : s/o – processus continu

Formation et sensibilisation

Recommandation du SMA(Svcs Ex)

3. Les SBMFC devraient élargir leur programme actuel de sensibilisation et de formation à la protection de la vie privée en y ajoutant des exigences de formation pour le personnel qui participe le plus activement au traitement des renseignements personnels. Ils devraient également s'assurer de mettre en place des PON pour tous leurs fonds de données de renseignements personnels.

Mesure 3.1 : Les SBMFC entreprendront l'élaboration d'un cours de formation spécifique aux SBMFC/BNP à l'intention du personnel qui participe le plus activement au traitement des renseignements personnels, et donnera des directives à toutes les unités pour s'assurer qu'elles élaborent de façon autonome des PON pour tous les fonds de données de renseignements personnels des SBMFC. Un financement public sur plusieurs exercices sera probablement nécessaire pour l'élaboration du cours.

BPR : SGC

BC : DPRH, toutes les divisions

Date cible : avril 2024

Entente sur l'échange de renseignements avec des tiers fournisseurs de services

Recommandation du SMA(Svcs Ex)

4. Les SBMFC devraient tenir à jour un inventaire des ententes commerciales dans le cadre desquelles des renseignements personnels sont transférés à un tiers, et obtenir l'assurance que les pratiques de traitement des données de leurs partenaires sont conformes aux modalités de leurs ententes sur l'échange de renseignements.

Mesure 4.1 : Les SBMFC créeront et tiendront à jour un inventaire des ententes commerciales dans le cadre desquelles des renseignements personnels sont transférés à un tiers.

BPR : CE, SGC

BC : DPI, chefs de division

Date cible : octobre 2023

Mesure 4.2 : Le personnel des SBMFC examineront les méthodes permettant d'obtenir des garanties dans les futurs contrats portant sur les pratiques de traitement des données par des tiers, et mettront en œuvre celles qui sont les plus raisonnables et les plus appropriées.

BPR : SGC

Date cible : avril 2024

Limitation de l'élimination

Recommandation du SMA(Svcs Ex)

5. Les SBMFC devraient éliminer les données dont ils n'ont plus besoin de leurs bases de données afin de se conformer aux pratiques exemplaires énoncées dans la *Loi sur la protection des renseignements personnels*.

Mesure 5.1 : Les SBMFC examineront et modifieront les systèmes de TI afin d'y ajouter la capacité d'éliminer de leurs bases de données les renseignements personnels qui ne sont plus nécessaires.

BPR fonctionnel : CE

BPR technique : DPI

BPR des bases de données : RARM et UneFC

Date cible : avril 2023

Mesure 5.2 : Les SBMFC élaboreront et mettront en œuvre des procédures servant à éliminer périodiquement de leurs bases de données les renseignements personnels qui ne sont plus nécessaires.

BPR fonctionnel : CE

BPR technique : DPI

BPR des bases de données : RARM et UneFC

Date cible : avril 2023

Surveillance

Recommandation du SMA(Svcs Ex)

6. Les SBMFC devraient mettre en place un outil d'examen du journal d'audit afin de faciliter les enquêtes sur les accès, les utilisations ou les divulgations non autorisés par des utilisateurs internes.

Mesure 6.1 : Les SBMFC étudieront les différents outils d'examen du journal d'audit et en mettront un en œuvre en fonction du coût et de l'efficacité.

BPR fonctionnel : SGC

BPR technique : DPI

BPR de l'exécution : toutes les divisions qui en feront usage

Date cible : octobre 2023

Mesure 6.2 : Les SBMFC élaboreront et mettront en œuvre des procédures d'examen régulier des journaux d'accès.

BPR fonctionnel : SGC

BPR technique : DPI

BPR de l'exécution : toutes les divisions qui en feront usage

Date cible : octobre 2023

Annexe B – À propos de l'audit

Objectif

Le présent audit a pour objectif d'évaluer le cadre de gestion de la protection de la vie privée des SBMFC et de déterminer si les politiques, procédures et pratiques de gestion des renseignements personnels sont conformes à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes du CT.

Critères d'audit[1]

Gouvernance : Fournir une assurance raisonnable que des politiques, pratiques et procédures sont en place pour gérer et protéger efficacement les renseignements personnels conformément aux exigences de la *Loi sur la protection des renseignements personnels* et des politiques et directives connexes, et que les rôles en matière de protection de la vie privée sont clairement définis, approuvés officiellement et communiqués.

Gestion des risques : Fournir une assurance raisonnable que les SBMFC repèrent et analysent les risques d'atteinte à la vie privée afin de trouver une façon de gérer ces risques pour assurer la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes, et fournir une assurance raisonnable qu'ils offrent un solide programme de formation et de sensibilisation.

Contrôles : Fournir une assurance raisonnable que les SBMFC ont mis en œuvre des activités de contrôle pour aider à assurer la conformité à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes.

Portée

La portée du présent audit comprenait les responsabilités en matière de gestion de la protection de la vie privée de la Division des services généraux ou du GN AIPRP ainsi que les pratiques de protection de la vie privée en place pour régir la collecte des renseignements personnels dans le cadre du programme d'adhésion à UneFC et du Régime d'assurance-revenu militaire (RARM).

L'audit a permis d'examiner la conception des pratiques de gestion de la protection de la vie privée des SBMFC par rapport aux exigences de la *Loi sur la protection des renseignements personnels* ainsi que des politiques et directives connexes. L'accent a été mis sur les politiques, procédures et normes documentées en place pour la collecte, l'utilisation, la divulgation, la conservation et l'élimination des renseignements personnels. Nous nous sommes également penchés sur la façon dont les renseignements sont protégés.

---

[1]**Sources des critères** : *Loi sur la protection des renseignements personnels,* Politique du CT sur la protection de la vie privée, Directive du CT sur les pratiques relatives à la protection de la vie privée, Directive du CT sur l'évaluation des facteurs relatifs à la vie privée, Politique sur la sécurité du gouvernement.

L'audit concernait les activités réalisées entre le 1er avril 2017 et le 31 décembre 2021, mais portait principalement sur les pratiques actuelles.

Les travaux en lien avec l'audit ont été réalisés entre octobre 2020 et janvier 2022.

La portée n'incluait pas une évaluation de l'exactitude et de l'exhaustivité des renseignements recueillis, ni la conception et l'efficacité des domaines de contrôle clés de l'environnement de sécurité de la TI existant, car cela a été examiné dans le cadre de l'Audit de la sécurité des TI d'avril 2019.

En raison des restrictions imposées par la pandémie, l'équipe d'audit n'a pas été en mesure d'examiner les opérations quotidiennes du personnel le plus activement engagé dans le traitement des renseignements personnels, ni de procéder à des inspections physiques.

Méthodologie

La méthodologie employée dans le cadre de l'audit incluait un examen des lois et des politiques applicables, un examen des principaux documents à l'appui et des documents de référence pertinents et des entrevues avec des membres clés du personnel des SBMFC à Ottawa.

Énoncé de conformité

Les constatations et conclusions figurant dans le présent rapport sont étayées par des preuves d'audit suffisantes et appropriées regroupées conformément à des procédures qui respectent les exigences énoncées dans le document *Normes internationales pour la pratique professionnelle de l'audit interne* du Institute of Internal Auditors. Par conséquent, l'audit interne est conforme aux *Normes internationales pour la pratique professionnelle d'audit interne* du Institute of Internal Auditors, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité. Les opinions exprimées dans le présent rapport sont fondées sur les conditions qui avaient cours au moment de l'audit et ne s'appliquent qu'à l'entité examinée.

Annexe C – RARM et programme d'adhésion à UneFC

RARM

Le RARM a été créé en 1969 pour gérer le Régime d'assurance-revenu militaire qui offrait aux membres des FAC et du MDN une couverture payée par le gouvernement en vertu de polices d'assurance-vie et d'assurance-invalidité collectives.

Au fil du temps, le RARM a élargi sa gamme de services et de produits offerts par l'entremise de vingt-quatre bureaux répartis dans tout le pays afin de répondre aux besoins financiers des membres des FAC, des réservistes, des retraités et de leurs familles. Dans le but de garantir que « [c]haque membre de la collectivité des FAC et leur famille jouissent d'une santé et d'une sécurité financière », l'offre bonifiée donne accès à ce qui suit :

- des polices d'assurance-vie collective et d'assurance-invalidité collective payées par le gouvernement et les participants;
- une assurance habitation, automobile, voyage et contre les maladies graves;
- des services bancaires aux particuliers et aux entreprises;
- des placements détenus dans des REER, des CELI, des REEE, des comptes non enregistrés, des régimes d'épargne des FAC et des régimes enregistrés d'épargne-invalidité.

Les services incluent les suivants :

- conseils financiers;
- consultation en matière de finances et de dettes.

Adhésion à UneFC

L'adhésion à UneFC donne accès à une variété de programmes et de services administrés par les SBMFC. La carte confirme de façon simple et claire l'appartenance à la collectivité militaire canadienne.

De plus, l'adhésion à UneFC donne accès au programme de récompenses et de fidélisation de CANEX, aux tarifs réservés aux membres de CANEX, au Programme de reconnaissance des FC et aux programmes financiers affinitaires, dont les services bancaires de la Défense de BMO et La Personnelle, compagnie d'assurances. Les programmes ciblés pour les militaires comprennent le programme Vacances pour les anciens combattants, le programme de camp d'été Appuyons nos troupes et le programme de bourses d'études Appuyons nos troupes.

La carte de membre UneFC est utilisée pour valider l'admissibilité à divers programmes tels que le RARM, les services de loisirs des PSP, les mess et l'accès des familles militaires aux soins virtuels Maple.

Les membres des FAC (Force régulière et Force de réserve), de la GRC et de la garde côtière, les vétérans, les retraités de ces organisations et les militaires étrangers qui servent actuellement au sein des FAC ainsi que leurs familles peuvent adhérer à UneFC. Le personnel du MDN et le personnel de nombreuses organisations affiliées au MDN ainsi que leurs familles sont également admissibles à l'adhésion.