

## **POLICY ON PRIVACY PRACTICES**

**DATE OF ISSUE : September 2017**  
**REVISION DATE : N/A**

### **APPLICATION**

1. This is an order that applies to members of the Canadian Armed Forces and a directive that applies to employees of the Department of National Defence (DND) and to the Staff of the Non-Public Funds (NPF), Canadian Forces (CF) involved in the administration and delivery of Non-Public Property (NPP) activities, services and programs.

2. For greater certainty, this includes all non-public property vested in the commanders of units and other elements, and in the Chief of the Defence Staff (CDS) established under sections 38 to 41 of the *National Defence Act*; all activities of the Staff of the NPF, CF; and all non-public property services, programs and operations including the public Alternative Service Delivery functions assigned to be executed under the NPP accountability framework.

### **APPROVAL AUTHORITY**

3. This policy is issued under the authority of the Director General Morale Welfare Services (DGMWS), in his capacity as the Managing Director NPP and Chief Executive Officer (CEO), Staff of the NPF, CF.

## **POLITIQUE SUR LES PRATIQUES RELATIVES À LA VIE PRIVÉE**

**DATE DE PUBLICATION : Septembre 2017**  
**DATE DE RÉVISION : S.O.**

### **APPLICATION**

1. Le présent document est une ordonnance qui s'applique aux membres des Forces armées canadiennes et une directive qui s'applique aux employés du ministère de la Défense nationale (MDN) ainsi qu'au Personnel des fonds non publics (FNP), Forces canadiennes (FC) qui sont responsables de l'administration et de la prestation des activités, services et programmes des Biens non publics (BNP).

2. Il est entendu que ces derniers comprennent tous les BNP dévolus aux commandants d'unités, à d'autres éléments et au chef d'état-major de la défense (CEMD) en vertu des articles 38 à 41 de la *Loi sur la défense nationale*; toutes les activités du personnel des FNP, FC; et l'ensemble des services et programmes des BNP, y compris les fonctions de diversification des modes de prestation de services qu'ils sont tenus d'exécuter et d'administrer dans le cadre de responsabilisation des BNP.

### **AUTORITÉ APPROBATRICE**

3. Cette politique est publiée avec l'autorisation du directeur général – Services de bien-être et moral (DGSBM) en sa qualité de directeur général des BNP et chef de la direction (CDir) du Personnel des FNP, FC.

## ENQUIRIES

4. Enquiries should be directed to the Canadian Forces Morale and Welfare Services (CFMWS) National Manager Access to Information and Privacy Program (NM ATIP).

## DEFINITIONS

5. See Annex A: Definitions.

## POLICY OBJECTIVE

6. The objective of this policy is to establish consistent practices and procedures to ensure that personal information is protected and effectively managed by identifying and mitigating privacy risks in accordance with the requirements of the *Privacy Act* (the Act), Regulations, and related Treasury Board Secretariat (TBS) policies, directives, standard and guidelines.

7. Non-compliance with the Act may result in complaints and investigations by the Office of the Privacy Commissioner of Canada as well as reviews by the Federal Court. A privacy breach may cause injury or harm to affected individuals and also affect the achievement of the organization's objectives.

## DEMANDES DE RENSEIGNEMENTS

4. Les demandes de renseignements doivent être adressées au gestionnaire national du Programme de l'accès à l'information et la protection des renseignements personnels (GN AIPRP) des Services de bien-être et moral des Forces canadiennes (SBMFC).

## DÉFINITIONS

5. Voir l'annexe A : Définitions.

## OBJECTIF DE LA POLITIQUE

6. La présente a pour objectif d'établir des pratiques et des procédures uniformes pour s'assurer que les renseignements personnels sont protégés et gérés efficacement en cernant et en atténuant et les risques d'entrave à la vie privée conformément aux exigences de la *Loi sur la protection des renseignements personnels* (la Loi), au règlement et aux politiques, directives, norme et lignes directrices connexes du Secrétariat du Conseil du Trésor (SCT).

7. La non-conformité à la *Loi* peut engendrer des plaintes et des enquêtes du commissariat à la protection de la vie privée du Canada ainsi que des révisions par la Cour fédérale. Une atteinte à la vie privée peut causer un dommage ou un préjudice aux personnes touchées et aussi nuire à l'atteinte des objectifs de l'organisation.

## AUTHORITIES, ROLES AND RESPONSIBILITIES

8. Pursuant to section 73 of the Act, the Minister of National Defence, as the head of the government institution, has designated the following positions within the CFMWS to exercise all his powers, duties and functions under the Act concerning NPP services, programs and operations:

- a. Managing Director NPP/  
CEO of the Staff of the NPF, CF;
- b. Chief of Staff/Vice-President  
Corporate Services (COS/  
VP CorpSvcs); and
- c. NM ATIP.

9. **CFMWS VP CorpSvcs** oversees the administration of the CFMWS ATIP Program and reports on the state of privacy management within NPP entities at the Executive Management Board (ExMB) on an annual basis.

10. **CFMWS NM ATIP** is responsible for:

- a. providing privacy advice and guidance as well as training and awareness to the managers and staff involved in NPP programs and services;
- b. determining the need and conducting a privacy impact assessment (PIA) when warranted, and creating or modifying a personal information bank (PIB), in collaboration with program managers;

## AUTORITÉS, RÔLES ET RESPONSABILITÉS

8. Conformément à l'article 73 de la *Loi*, le ministre de la Défense nationale, à titre de responsable de l'institution fédérale, a désigné les postes suivants au sein des SBMFC pour exercer tous ses pouvoirs, attributions et fonctions en vertu de la *Loi* concernant les services, programmes et activités des BNP :

- a. Directeur général des BNP/  
Cdir du Personnel des FNP, FC
- b. Chef d'état-major et vice-président  
des Services généraux (CEM/ VP SG);  
et
- c. GN AIPRP.

9. Le **VP SG SBMFC** surveille l'administration du programme d'AIPRP des SBMFC et fait rapport au conseil de la haute direction sur l'état de la gestion des renseignements personnels au sein des organismes des BNP sur une base annuelle.

10. Le **GN AIPRP SBMFC** est chargé de:

- a. donner des conseils et une orientation ainsi que des séances de formation et de sensibilisation sur la protection de la vie privée aux gestionnaires et au personnel responsable de l'administration et de la prestation des programmes et services des BNP;
- b. déterminer la nécessité d'effectuer une évaluation des facteurs relatifs à la vie privée (ÉFVP) et exécuter celle-ci lorsque les circonstances le justifient, et créer un fichier de renseignements personnels (FPR) ou le modifier en collaboration avec les gestionnaires de programme;

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>c. ensuring stakeholders review of the PIA in a timely manner, and endorsing and co-signing the completed PIA, as the delegate responsible for section 10 of the Act;</li> <li>d. submitting to TBS for registration and approval any new or revised PIB, along with the approved PIA that has been sent to the Office of the Privacy Commissioner (OPC), at least 60 days before the implementation of the new or substantially modified NPP program or activity;</li> <li>e. ensuring that sections I and II of completed PIAs are published on the CFMWS Web site, within three months following the approval of the PIA;</li> <li>f. working in close collaboration with the offices of primary interest (OPIs), and the CFMWS Unit Security Supervisor as required, in the management and resolution of privacy breaches in accordance with the CFMWS Privacy breach protocol;</li> <li>g. monitoring the implementation of the action plans developed by CFMWS divisions to address the privacy issues and risks identified in PIAs, or as a result of a privacy breach;</li> </ul> | <ul style="list-style-type: none"> <li>c. assurer que les intervenants passent en revue l'ÉFVP en temps opportun, et approuver et cosigner l'ÉFVP dûment remplie à titre de délégué responsable pour l'article 10 de la <i>Loi</i>;</li> <li>d. présenter aux fins d'enregistrement et d'approbation par le SCT tout FPR nouveau ou modifié, accompagné de l'ÉFVP approuvée qui a été envoyée au Commissariat à la protection de la vie privée (CPVP) au moins 60 jours avant le lancement ou la modification importante d'une activité ou d'un programme des BNP;</li> <li>e. veiller à ce que les sections I et II des ÉFVP dûment effectuées soient publiées sur le site Web des SBMFC dans les trois mois suivant l'approbation de l'ÉFVP;</li> <li>f. travailler en étroite collaboration avec les bureaux de première responsabilité (BRP), et le superviseur de la sécurité de l'unité des SBMFC le cas échéant, en vue de gérer et de résoudre les atteintes à la vie privée conformément aux Protocole sur les atteintes à la vie privée des SBMFC;</li> <li>g. surveiller la mise en application des plans d'action élaborés par les divisions des SBMFC pour régler les problèmes et les risques liés à la protection de la vie privée cernés dans les ÉFVP ou découlant d'une atteinte à la vie privée;</li> </ul> |
|--|--|

- h. making decisions regarding the disclosure of personal information pursuant to subsection 8(2)(e), (j) and (m) of the Act. See Annex B: Guidelines for the disclosure of personal information pursuant to subsection 8(2) of the *Privacy Act*;
- i. notifying the OPC in a timely manner of any planned initiative or issue that may relate to the Act or any of its provisions or that may have an impact on the privacy of Canadians (e.g. “material” privacy breaches, completed PIAs, new consistent uses of personal information, and disclosure in the public interest); and
- j. maintaining an up-to-date inventory of all current NPP personal information sharing agreements.

11. **CFMWS Division Heads**, in their capacity as NPP functional authorities, are responsible for:

- a. ensuring that privacy practices within their areas of responsibilities are consistent with and respect the provisions of the Act, Regulations and other applicable legislation;

- h. prendre les décisions concernant la communication de renseignements personnels en vertu des alinéas 8(2)e), j) and m) de la *Loi*. Voir l'annexe B : Lignes directrices sur la divulgation de renseignements personnels en vertu du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*;
- i. aviser le CPVP en temps opportun de toute nouvelle initiative ou question pouvant avoir rapport avec la *Loi* ou l'une de ses dispositions, ou pouvant avoir une incidence sur la vie privée des Canadiens (par exemple, les atteintes « substantielles » à la vie privée, les ÉFVP remplies, les nouveaux usages compatibles et les communications dans l'intérêt du public); et
- j. tenir à jour un inventaire de toutes les ententes d'échange de renseignements personnels des BNP en vigueur.

11. Les **chefs de divisions des SBMFC**, en leur qualité d'autorités fonctionnelles liées aux BNP, doivent :

- a. s'assurer que les pratiques de protection de la vie privée au sein de leurs secteurs de responsabilité sont conformes à la *Loi*, au *Règlement* et à toute autre loi applicable;

- b. Approving and co-signing the PIA completed for their division and ensuring that the PIA is provided to the OPC by the NM ATIP, along with any additional documentation that may be required by that office, at least 60 days before the implementation of a new or substantially modified NPP program or activity involving personal information;
  - c. ensuring that an action plan is developed and implemented in a timely manner to address privacy risks identified in the PIA, or as a result of a privacy breach; and
  - d. informing employees of the legal and administrative consequences of any inappropriate or unauthorized access to, or use, disclosure, modification, retention and disposal of, personal information related to a particular NPP program or activity.
- b. approuver et cosigner l'ÉFVP dûment achevée pour leur division, et veiller à ce que l'ÉFVP approuvée soit transmise au CPVP par l'entremise du GN AIPRP, accompagnée des autres documents requis au moins dans les 60 jours avant le lancement ou la modification important d'une activité ou d'un programme des BNP faisant appel à des renseignements personnels;
  - c. veuillez à la création et à la mise en œuvre en temps utile d'un plan d'action visant à régler les risques d'atteinte à la vie privée relevés dans l'ÉFVP ou découlant d'une atteinte à la vie privée; et
  - d. informer les employés des conséquences juridiques et administratives que peut entraîner un accès inapproprié ou non autorisé à des renseignements personnels liés à un programme ou à une activité des BNP en particulier, ou à l'utilisation, à la divulgation, à la modification, à la conservation et à l'élimination de ces renseignements personnels.

12. **Managers** and, where applicable, **staff** involved in the management or delivery of programs, activities and services under the NPP accountability framework are responsible for:

- a. complying with the requirements set out in sections 4 to 8 of the *Privacy Act*, the Regulations, and section 6.2 of the TBS Directive on Privacy Practices regarding the creation, collection, notification and consent, accuracy, use and disclosure, safeguards, retention and disposal of personal information, as well as the TBS Directive on Social Insurance Number (SIN) regarding the restrictions limiting the collection and use of this identifying number;
- b. prior to disclosing personal information in response to a request from a NPP client, ensuring that the individual has adequately identified himself or herself as the individual to whom the information pertains, or as the person authorized in writing by the individual or authorized by law to administer the affairs of the individual;

12. Les **gestionnaires** et, selon le cas, le **personnel** participant à la gestion ou à l'exécution des programmes, à la réalisation des activités et à la prestation des services dans le cadre de responsabilisation des BNP doivent :

- a. respecter les exigences des articles 4 à 8 de la *Loi sur la protection des renseignements personnels*, du règlement et de la section 6.2 de la Directive sur les pratiques relatives à la protection de la vie privée du SCT concernant la création, la collecte, la notification et le consentement, l'exactitude, l'utilisation et la communication, la protection, la conservation et l'élimination des renseignements personnels, ainsi que la Directive sur le numéro d'assurance social (NAS) du SCT qui porte sur les restrictions limitant la collecte et l'utilisation de ce numéro d'identification;
- b. avant de divulguer des renseignements personnels en réponse à une demande d'un client des BNP, s'assurer que la personne s'est identifiée correctement comme la personne à laquelle les renseignements appartiennent ou celle ayant obtenu une autorisation écrite de la personne visée, ou encore comme la personne autorisée par la *Loi* à administrer les affaires de la personne visée;

**Note:** *Where a rigorous verification of identity is necessary, the individual may be required to be present when the information is disclosed. If there is any doubt concerning the identity of the person seeking access, disclosure must not take place;*

- c. safeguarding and not disclosing personal information without the consent of the individual to whom it relates, except in accordance with section 8 of the Act and Annex B: Guidelines for the disclosure of personal information pursuant to subsection 8(2) of the *Privacy Act*;
- d. promptly reporting and managing any suspected or actual breach of privacy, in accordance with the CFMWS Privacy breach protocol;
- e. consulting the CFMWS NM ATIP in the following circumstances:
  - i. in the early stages of the planning of any new or substantially modified NPP program or activity involving personal information to determine whether a PIA is warranted;

**Nota :** *Si une vérification rigoureuse de l'identité est nécessaire, la personne visée peut être tenue d'être présente lors de la communication des renseignements. En cas de doute concernant l'identité de la personne demandant l'accès à des renseignements personnels, les renseignements ne doivent pas être divulgués;*

- c. protéger et ne pas communiquer des renseignements personnels sans consentement de l'individu qu'ils concernent, sauf en conformité avec l'article 8 de la *Loi* et l'annexe B : Lignes directrices concernant la communication de renseignements personnels en vertu du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*;
- d. signaler et gérer rapidement toute cas présumé ou réel d'atteinte à la vie privée conformément au Protocole sur les atteintes à la vie privée des SBMFC;
- e. consulter le GN AIPRP SBMFC dans les circonstances suivantes :
  - i. au tout début de la planification du lancement ou de la modification importante d'une activité ou un programme des BNP faisant appel à des renseignements personnels pour déterminer si une ÉFVP est nécessaire;



- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>ii. when creating or revising a form requiring the collection of personal information, for a compliance review and the inclusion of the appropriate privacy notice and consent statement, as required;</li> </ul>  | <ul style="list-style-type: none"> <li>ii. lors de la création ou de la révision d'un formulaire nécessitant la collecte de renseignements personnels dans le but d'en faire l'examen de conformité ou d'y inclure un avis de confidentialité et une déclaration de consentement, au besoin;</li> </ul>   |
| <ul style="list-style-type: none"> <li>iii. prior to any new use or disclosure consistent with the purpose for which the personal information was originally obtained or compiled, but is not currently described in a PIB, or for a purpose that was not originally intended;</li> </ul>   | <ul style="list-style-type: none"> <li>iii. avant toute nouvelle utilisation ou communication conforme aux fins auxquelles les renseignements personnels ont été initialement obtenus et compilés, mais qui n'est pas actuellement décrite dans un FPR, ou à des fins qui n'étaient pas prévues initialement;</li> </ul>  |
| <ul style="list-style-type: none"> <li>iv. when preparing information sharing agreements involving personal information with public sector organizations, to ensure that appropriate privacy protection provisions are included therein, in accordance with the requirements of the Act and the TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information;</li> </ul> | <ul style="list-style-type: none"> <li>iv. lors de la préparation d'ententes d'échange de renseignements personnels avec les organisations du secteur public pour veillez à ce que les dispositions relatives à la protection des renseignements personnels soient incluses conformément aux exigences de la <i>Loi</i> et le Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels du SCT;</li> </ul> |
| <ul style="list-style-type: none"> <li>f. collaborating with the CFMWS NM ATIP in the development of a PIA and the creation or modification of a PIB, and providing in a timely manner necessary documentation and evidence;</li> </ul>   | <ul style="list-style-type: none"> <li>f. collaborer avec le GN AIPRP SBMFC à l'élaboration d'une ÉFVP et à la création ou la modification d'un FPR, et fournir rapidement les documents et les preuves nécessaires;</li> </ul>   |

- g. developing and implementing an action plan to address any privacy risks identified in the PIA, or as a result of a privacy breach, and providing a status update to the CFMWS NM ATIP, as required; and
- h. depositing a copy of all current personal information sharing agreements with the CFMWS NM ATIP.

- g. élaborer et mettre en application un plan d'action pour régler les risques d'atteinte à la vie privée cernés dans l'ÉFVP ou découlant d'une atteinte à la vie privée et faire rapport sur l'état d'avancement au GN AIPRP SBMFC, au besoin; et
- h. déposer un exemplaire de toutes les ententes d'échange de renseignements personnels auprès du GN AIPRP SBMFC.

**13. CFMWS Chief Information Officer** ensures that:

- a. as part of any security assessment of IM/IT solutions involving personal information, that the CFMWS NM ATIP has been consulted to determine whether a PIA is warranted. If a PIA is required, and has not been completed prior to granting an Authority to Operate, the corresponding Letter of Authorization must contain a mandatory condition requiring the submission of a completed PIA within acceptable timelines; and
- b. the NPPNet is compliant with the requirements of the *Privacy Act* and the related TBS policies and directives, including the *Standard on Privacy and Web Analytics* and also the terms and conditions for privacy notices in Appendix C of the *Standard on Web Usability*.

**13. Le chef des services de l'information des SBMFC** doit veiller à ce que :

- a. le GN AIPRP SBMFC soit consulté dans le cadre d'une évaluation de sécurité concernant des solutions de GI/TI faisant appel à des renseignements personnels pour déterminer si les conséquences justifient une ÉFVP. Si une ÉFVP est jugée nécessaire et qu'elle n'a pas été effectuée avant l'octroi d'une autorisation d'exploitation, la lettre d'autorisation correspondante doit renfermer une condition obligatoire exigeant la présentation d'une ÉFVP dans les délais acceptables; et
- b. le réseau des BNP respecte les exigences de la *Loi* et des politiques et directives connexes du SCT, y compris la Norme sur la protection de la vie privée et le Web analytique et les modalités de l'annexe C de la Norme sur la facilité d'emploi des sites Web relative aux avis de confidentialité.

14. **CFMWS Unit Security Supervisor** works in close collaboration with the CFMWS NM ATIP to ensure the timely reporting of, intervention in, and investigation into suspected or actual breaches of privacy related to NPP activities, in accordance with the CFMWS Privacy breach protocol.

15. **NPP Contracting authorities** must consult the CFMWS NM ATIP when a proposed NPP procurement involves personal information, to ensure that appropriate privacy protection clauses are included in contracting documents, in accordance with the requirements of the Act and the TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions.

## MONITORING AND CONSEQUENCES

16. The CFMWS NM ATIP monitors compliance with the Treasury Board Secretariat (TBS) policies, directives, standard and guidelines related to the administration of the *Privacy Act* within NPP organizations.

17. Privacy breaches caused by the culmination of inappropriate information-management practices may result in disciplinary action, up to and including termination of employment.

## REFERENCES

Acts and regulations:

- a. *Access to Information Act*
- b. *Privacy Act*
- c. *Access to Information Regulations*

14. Le **superviseur de la sécurité de l'unité des SBMFC** travaille en étroite collaboration avec le GN AIPRP SBMFC pour veiller à ce que les cas présumés ou réels d'atteintes à la vie privée liées aux activités des BNP soient signalés et fassent l'objet d'une intervention et d'une enquête, conformément au Protocole sur les atteintes à la vie privée des SBMFC.

15. Les **autorités contractantes des BNP** doivent consulter le GN AIPRP SBMFC lorsqu'un projet d'approvisionnement des BNP **est lié à** des renseignements personnels afin de s'assurer que les documents contractuels renferment les clauses de protection de la vie privée pertinentes conformément aux exigences de la *Loi* et du Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché du SCT.

## SURVEILLANCE ET CONSÉQUENCES

16. Le GN AIPRP SBMFC surveille la conformité aux politiques, directives, norme et lignes directrices du Secrétariat du Conseil du Trésor (SCT) liées à l'administration de la *Loi sur la protection des renseignements personnels* au sein des organisation des BNP.

17. Les atteintes à la vie privée résultant de pratiques de gestion de l'information inadéquates entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement.

## RÉFÉRENCES

Lois et règlements :

- a. *Loi sur l'accès à l'information*
- b. *Loi sur la protection des renseignements personnels*
- c. *Règlement sur l'accès à l'information*

d. *Privacy Regulations*

d. *Règlement sur la protection des renseignements personnels*

Treasury Board publications:

Publications du Conseil du Trésor :

- a. Policy on Privacy Protection
- b. Directive on Privacy Impact Assessment
- c. Directive on Privacy Practices
- d. Directive on Social Insurance Number
- e. Guidance Document: Taking Privacy into Account Before Making Contracting Decisions
- f. Guidance on Preparing Information Sharing Agreements Involving Personal Information
- g. Guidelines for Privacy Breaches
- h. *Info Source*
- i. Standard on Privacy and Web Analytics

- a. Politique sur la protection de la vie privée
- b. Directive sur l'évaluation des facteurs relatifs à la vie privée
- c. Directive sur les pratiques relatives à la vie privée
- d. Directive sur le numéro d'assurance social
- e. Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché
- f. Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels
- h. Lignes directrices sur les atteintes à la vie privée
- i. *Info Source*
- i. Norme sur la protection de la vie privée et le Web analytique

CFMWS policies:

Politiques des SBMFC :

- a. Policy on the Access to Information and Privacy (ATIP) Program
- b. Privacy Breach Protocol

- a. Politique sur le programme d'accès à l'information et de protection des renseignements personnels (
- b. Protocole sur les atteintes à la vie privée

- c. Protocol for non-administrative uses of personal information (*under development*)
- d. CFMWS Non-Public Property Functional Authority Policy
- e. Non-Public Property (NPP) Network (NPP Net) Privacy Policy

- c. Protocole sur les usages non administratifs de renseignements personnels (*en cours d'élaboration*)
- d. Politique sur les autorités fonctionnelles des SBMFC liées aux Biens non-publics
- e. Politique sur la protection des renseignements personnels sur le réseau des Biens non publics (Rés BNP)

## **ANNEXES**

Annex A: Definitions

Annex B: Guidelines for the disclosure of personal information pursuant to subsection 8(2) of the *Privacy Act*

## **ANNEXES**

Annexe A : Définitions

Annexe B : Lignes directrices relatives à la communication de renseignements personnels en vertu du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*.

## ANNEX A: DEFINITIONS

**Administrative purpose:** Use of personal information about an individual in a decision-making process that directly affects that individual. This includes all uses of personal information for confirming identity (i.e., authentication and verification purposes) and for determining eligibility of individuals for government programs.

**Consistent use:** Use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

**Data matching:** An activity that involves comparing personal data obtained from a different source within the same government institution, for administrative or non-administrative purposes. The data-matching activity that is established can be systematic or recurring. The data-matching activity can also be conducted on a periodic basis when deemed necessary. Under the TBS Policy on Privacy Protection, data matching includes the disclosure or sharing of personal information with another organization for data-matching purposes.

**Delegate:** An officer or employee of a government institution who has been delegated to exercise or perform the powers, duties and functions of the head of the institution under the Act.

## ANNEXE A : DÉFINITIONS

**Fins administratives :** Utilisation de renseignements personnels concernant un particulier « dans le cadre d'une décision le touchant directement » (l'article 3). Cela comprend toute utilisation de renseignements personnels afin de confirmer l'identité d'une personne (c.-à-d. à des fins d'authentification et de vérification) ainsi que de déterminer si celle-ci est admissible aux programmes gouvernementaux.

**Usage compatible :** Usage se rapportant de façon raisonnable et directe à l'objectif premier pour lequel les renseignements ont été obtenus ou recueillis. Cela signifie que les fins premières et les fins qui ont été proposées sont si intimement liées que la personne s'attendrait à ce que les renseignements soient utilisés pour les fins conformes, même si elles n'ont pas été expressément mentionnées.

**Couplage de données :** Une activité qui consiste à comparer des renseignements personnels provenant de diverses sources, y compris de sources d'une même institution, à des fins administratives ou non administratives. Le couplage des données peut être systématique, récurrent ou peut être effectué périodiquement lorsqu'il est jugé nécessaire. En vertu de la Politique sur la protection de la vie privée du SCT, le couplage des données comprend la communication de renseignements personnels à une autre organisation à des fins de couplage de données.

**Délégué :** Un cadre ou employé d'une institution fédérale délégué pour exercer les pouvoirs, attributions et fonctions du responsable de l'institution en vertu de la *Loi*.

**Disclosure:** Release of personal information by any method (e.g., transmission, provision of a copy, examination of a record) to any body or person.

**Government institution:** For the purposes of the *Access to Information Act* and the *Privacy Act*, any department, ministry of state, body, or office listed in Schedule I of the Acts as well as any parent Crown corporation and wholly-owned subsidiary of a Crown corporation within the meaning of section 83 of the *Financial Administration Act*. These institutions must respect and fulfill all responsibilities provided for in the Acts.

**Head of government institution:** For the purpose of the *Access to Information Act* and the *Privacy Act*, in the case of a department or ministry of state, the head of the government institution is the minister. In other cases, the head of the institution is the person designated by an Order in Council or, if no such person is designated, the chief executive officer of the institution, whatever their specific title. The head, or their delegate(s), is responsible for exercising all powers, duties and functions related to the application of the *Access to Information Act* and the *Privacy Act* within their institution. For NPP entities, the Minister of National Defence is the head of the institution.

**Divulgateion :** Communication de renseignements personnels par une méthode quelconque (c'est-à-dire la transmission, la présentation d'une copie ou l'examen d'un document) à toute entité ou personne.

**Institution fédérale :** Aux fins de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, tout ministère, département d'État, organisme ou bureau figurant à l'annexe I des lois, et toute société d'État mère ou filiale en propriété exclusive d'une société d'État, au sens de l'article 83 de la *Loi sur la gestion des finances publiques*. Ces institutions doivent se conformer et s'acquitter aux responsabilités prévues dans les lois.

**Responsable d'une institution fédérale :** Aux fins de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, le responsable d'une institution fédérale est le ministre dans le cas d'un ministère ou d'un département d'État. Dans tout autre cas, la personne désignée par décret et, si aucune personne n'est désignée, le premier dirigeant de l'institution, quel que soit son titre. Le responsable ou son délégué est responsable d'exercer l'ensemble des pouvoirs, des tâches et des fonctions liés à l'application de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* dans son institution. Pour les entités des BNP, le ministre de la Défense nationale est le responsable de l'institution fédérale.

**Info Source:** A series of annual TBS publications aimed at the public that contain clear and detailed information on government institutions, their program responsibilities and their information holdings, for the purpose of assisting members of the public in exercising their right of access under the Act. *Info Source* publications also provide contact information for government institutions as well as summaries of court cases and statistics on access to information and privacy requests.

**Need-to-know:** The restriction of access to protected or classified information to individuals who need to access and know the information in order to perform their duties.

**New consistent use:** Consistent use that was not originally identified in the appropriate personal information bank (PIB) described in the *Info Source*.

**Non-administrative purpose:** Use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistic analysis, audit, and evaluation purposes.

**Non-Public Property:** NPP is defined in section 2 of the *National Defence Act* (NDA) and includes all money and property received for or administered by or through NPP organizations, and all money and property contributed to or by CAF members for their collective benefit and welfare.

**Info Source :** Une série de publications annuelles du SCT à l'intention du public qui contiennent des renseignements clairs et détaillés sur les institutions fédérales, leurs responsabilités en matière de programmes et leurs fonds de renseignements, pour permettre au public d'exercer son droit d'accès en vertu de la *Loi*. Les publications *Info Source* présentent également les coordonnées des ministères et organismes fédéraux ainsi que des résumés des causes de la cour et des statistiques sur les demandes d'accès à l'information et de renseignements personnels.

**Besoin de connaître :** Restriction de l'accès aux renseignements protégés ou classifiés aux personnes qui ont besoin d'accéder aux renseignements et de connaître ceux-ci pour exécuter leurs tâches.

**Nouvel usage compatible :** Usage compatible n'ayant pas été présenté initialement dans la description appropriée des fichiers de renseignements personnels du chapitre de l'institution dans *Info Source*.

**Fins non administratives :** Utilisation de renseignements personnels pour une fin qui n'est pas liée à une décision touchant directement la personne. Cela comprend l'utilisation de renseignements personnels à des fins de recherche, de statistique, de vérification et d'évaluation.

**Biens non publics :** Les BNP sont définis à l'article 2 de la *Loi sur la défense nationale* (LDN) et comprennent tous les fonds et biens reçus pour les organismes des BNP ou administrés par eux ou par leur entremise, ainsi que tous les fonds et biens donnés aux membres des FAC ou par eux-mêmes pour leur bénéfice et leur bien-être collectifs.



**NPP Functional Authorities:** Subject matter experts who are responsible for the various CFMWS NPP functions.

**Original purpose:** Purpose that was first identified when initiating the collection of personal information and that is directly related to an operating program or activity of the institution. A purpose that is not consistent with the original purpose is considered to be a secondary purpose.

**Personal Information:** Information that is about an identifiable individual and recorded in any form, as defined in section 3 of the *Privacy Act*. Examples include information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual.

**Personal information Bank (PIB):** Description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the PIB has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.

**Privacy:** An individual's right to be left alone and to be free of unwarranted intrusions. It is also the right of an individual to retain control over his or her personal information and to know the uses, disclosures and whereabouts of that information.

**Autorités fonctionnelles des BNP :** Experts en la matière chargés des diverses fonctions des BNP au sein des SBMFC.

**Fin originale :** Fin initiale identifiée au début de la collecte des renseignements personnels qui est liée directement à un programme ou à une activité d'ordre opérationnel de l'institution. Une fin qui ne correspond pas à la fin originale est traitée comme étant une fin secondaire.

**Renseignements personnels :** Renseignements, quels que soient leur forme et leurs supports, concernant un individu identifiable, tel que défini à l'article 3 de la *Loi sur la protection des renseignements personnels*. Par exemple, les renseignements relatifs à la race, la nationalité, l'origine ethnique, la religion, l'âge, l'état civil, l'adresse ou les études, ainsi que les antécédents médicaux, criminels, financiers ou d'emploi d'un individu. Les renseignements personnels comprennent aussi un numéro ou un symbole d'identification, comme le numéro d'assurance social, attribué à un individu.

**Fichier de renseignements personnels (FRP) :** Description de renseignements personnels organisés ou extraits soit en se servant du nom d'une personne, d'un numéro d'identité ou de tout autre symbole ou code désignant uniquement cette personne. En général, les renseignements personnels décrits dans le fichier de renseignements personnels ont été ou sont utilisés ou sont disponibles à des fins administratives et relèvent d'une institution fédérale.

**Vie privée :** Droit d'un individu à son intimité et à être protégé contre toute intrusion injustifiée. Il s'agit aussi du droit d'un individu de garder le contrôle de ses renseignements personnels et de savoir à quelles fins ils sont utilisés, divulgués et où ils sont conservés.

**Privacy breach:** The improper or unauthorized creation, collection, access, use, disclosure, retention and/or disposal of personal information. A privacy breach may occur within an institution or off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

**Privacy Commissioner of Canada:** An Officer of Parliament who investigates complaints from individuals regarding the handling of personal information by federal government institutions. In addition, the Commissioner has the authority to conduct compliance reviews of the privacy practices of government institutions as the practices relate to the collection, retention, accuracy, use, disclosure and disposal of personal information by government institutions subject to the Act. The Commissioner has the powers of an ombudsman and can make recommendations with respect to any matter which has been investigated or reviewed. In addition, the Commissioner can report on institutional activities in annual or special reports to Parliament.

**Privacy impact assessment (PIA):** Policy process for identifying, assessing, and mitigating privacy risks. Government institutions are required to develop and maintain PIAs for all new or modified programs and activities that involve the use of personal information for an administrative purpose.

**Atteinte à la vie privée :** Création, collecte, utilisation, divulgation, conservation ou retrait inappropriée ou non autorisée de renseignements personnels, ou accès inapproprié ou non autorisé à de tels renseignements. Une atteinte à la vie privée peut survenir au sein d'une institution ou à l'extérieur, et être le résultat d'erreurs de bonne foi ou d'actes malveillants commis par des employés, des tiers, des partenaires ou des intrus.

**Commissaire à la protection de la vie privée :** Haut fonctionnaire du Parlement chargé de faire enquête sur les plaintes portées par des particuliers à l'égard du traitement de renseignements personnels par les institutions fédérales. En outre, le commissaire a le pouvoir de mener des examens de conformité à l'égard des pratiques de protection des renseignements personnels des institutions fédérales, en ce qui concerne la collecte, la conservation, l'exactitude, l'utilisation, la divulgation ou le retrait des renseignements personnels par les institutions fédérales assujetties à la Loi. Le commissaire dispose également des pouvoirs d'un ombudsman et peut formuler des recommandations concernant toute question ayant fait l'objet d'une enquête ou d'un examen. Par ailleurs, le commissaire peut faire rapport relativement aux activités institutionnelles dans les rapports annuels ou spéciaux présentés au Parlement.

**Évaluation des facteurs relatifs à la vie privée (ÉFVP) :** Processus d'élaboration des politiques permettant de déterminer, d'évaluer et d'atténuer les risques d'entrave à la vie privée. Les institutions fédérales doivent consigner et tenir à jour des ÉFVP pour les activités et les programmes nouveaux ou modifiés qui utilisent des renseignements personnels à des fins administratives.

**Privacy notice:** Verbal or written notice informing an individual of the purpose of a collection of personal information and of the government institution's authority for collecting it, including creating, using and disclosing information. The notice, which must reference the PIB described in *Info Source*, also informs the individual of his or her right to access, and request the correction of, the personal information and of the consequences of refusing to provide the information requested.

**Privacy practices:** All practices related to the creation, collection, retention, accuracy, correction, use, disclosure, retention and disposal of personal information.

**Privacy protocol:** Set of documented procedures to be followed when using personal information for non-administrative purposes, including research, statistics, audit, and evaluation. These procedures ensure that the individual's personal information is handled in a manner that is consistent with the principles of the Act.

**Web analytics:** The collection, analysis, measurement and reporting of data about Web traffic and use visits for the purpose of understanding and optimizing Web usage.

**Avis de confidentialité :** Avis verbal ou écrit présenté à un individu afin de communiquer les fins de la collecte de renseignements personnels, et l'autorité de l'institution fédérale pour procéder à cette collecte, y compris la création, l'utilisation et la divulgation des renseignements. L'avis, qui doit renvoyer au FRP décrit dans *Info Source*, informe également l'individu de ses droits d'accès et de correction de ses renseignements personnels, ainsi que des conséquences d'un refus de fournir les renseignements demandés.

**Pratiques relatives à la protection de la vie privée :** Toutes les pratiques relatives à la création, la collecte, la conservation, l'exactitude, la correction, l'utilisation, la divulgation et le retrait des renseignements personnels.

**Protocole relatif à la protection des renseignements personnels :** Ensemble de procédures documentées à respecter lors de l'utilisation de renseignements personnels à des fins non administratives, y compris la recherche, les statistiques, la vérification et l'évaluation. Ces procédures visent à s'assurer que le traitement des renseignements personnels de particuliers soit conforme avec les principes de la *Loi*.

**Web analytique :** La collecte, l'analyse, la mesure et le compte rendu des données sur l'achalandage des sites Web et les visites d'utilisateurs pour bien comprendre l'usage du Web et l'optimiser.

## **ANNEX B: GUIDELINES FOR THE DISCLOSURE OF PERSONAL INFORMATION PURSUANT TO SUBSECTION 8(2) OF THE *PRIVACY ACT***

These guidelines identify the authorities to make discretionary disclosure decisions, clarify the circumstances under which personal information managed under the NPP accountability framework may be disclosed, without the consent of the individual to whom it relates, pursuant to subsection 8(2) of the *Privacy Act* and also clarify the retention requirements in this regard.

### **1. Guidelines**

Subsection 8(2) of the Act describes the different circumstances under which personal information under the control of a government institution may be disclosed without the consent of the individual to whom the information pertains. Such disclosures are discretionary and are subject to the provisions of any other Act of Parliament.

Subsection 8(2) does not take precedence over specific statutory prohibitions, and **only applies where no other statutory provision exists**. Therefore, where another federal statute forbids the disclosure of personal information (e.g., section 241 of the *Income Tax Act*), the personal information cannot be disclosed by the institution.

Disclosures under subsection 8(2) should be limited to the information requested and no more than is necessary to fulfill the purpose for which it will be used. Moreover, only relevant information pertaining to the individual identified in the request may be released; **any information about other individuals should be severed from the record prior to disclosure**.

Pursuant to subsection 9(1) of the Act, when personal information is disclosed for a use or purpose not included in the relevant Personal Information Bank (PIB), a record of the use or disclosure shall be attached to the personal information and should include the following:

- the name and title of the person authorizing the use or disclosure;
- the name of the institution, person, organization or body receiving the information;
- a description of the use or purpose of disclosure; and,
- a copy of the information disclosed, or a description in sufficient detail to allow a determination of exactly what information was used or disclosed.

Additional guidelines concerning the disclosure of personal information pursuant to specific paragraphs of subsection 8(2) of the Act follow. Managers should consult with the CFMWS NM ATIP for guidance, or if they would like an informal review of the records prior to making a disclosure.

**Note:** These guidelines do not apply to routine disclosures made under subsection 8(2) of the Act, as these should be governed by personal information sharing agreements and also described in the relevant PIBs. Consult the CFMWS NM ATIP if these instruments are not already in place.

## **2. Application**

### **Paragraph 8(2)(a) – Original purpose or consistent use**

Managers and designated staff may disclose personal information for the purpose for which the information was obtained or compiled by the program, or for a use consistent with that purpose, as described in the relevant personal information bank (PIB) described in the Info Source.

If the relevant PIB does not clearly describe the original purpose or consistent uses, or if no PIB exists, employees should consult the CFMWS NM ATIP prior to disclosing personal information.

### **Paragraph 8(2)(b) – Act of Parliament or Regulation**

Managers and designated staff may disclose personal information for any purpose, in accordance with any *Act* of Parliament or any regulations made there under that authorizes its disclosure. For example, the *Auditor General Act* specifically authorizes departments to disclose information to the Auditor General or a member of his or her office.

If the legal authority to disclosure personal information is not clearly identified, or for any request received under the *Security of Canada Information Sharing Act* (SCISA), managers must consult the CFMWS NM ATIP prior to responding. It is possible that the legal authority of another organization to request information or require the production of information may not constitute an authority to disclose personal information under this provision.

### **Paragraph 8(2)(c) – Subpoenas, Warrants, Court orders and Rules of court**

Warrants or subpoenas are usually served in the location where the records are held or on persons who are thought to hold the requested records. Sometimes parties to a civil proceeding will serve a notice to produce, a similar order or summons on a public servant, requiring him/her to appear at a pre-trial examination and to bring certain documents. These documents should be carefully scrutinized by the Legal Services, to verify the validity of the warrants, subpoenas, court orders and notices for the production of information, and to determine the proper form of compliance.

In some cases, it may be appropriate to ask the courts for permission to sever from the records, certain sensitive information that is not relevant to the issue before the court. In exceptional circumstances, section 37 of the *Canada Evidence Act* allows a government official to ask the court not to disclose even relevant information.

#### **Paragraph 8(2)(d) – Attorney General**

Managers and designated staff may disclose personal information to the Attorney General for use in legal proceedings involving the Crown, in consultation with Legal Services.

#### **Paragraph 8(2)(e) – Federal investigative bodies**

Requests from federal investigative bodies (specified in Schedule II of the *Privacy Regulations*) for personal information, along with the responsive records and/or recommendations, if applicable, must be immediately forwarded to the CFMWS NM ATIP who is responsible for making decisions under this provision.

Personal information may only be disclosed to aid in a specific, lawful enforcement or investigative activity and should not be disclosed in relation to a vague inquiry.

Pursuant to subsection 8(4) of the *Privacy Act* and section 7 of the *Privacy Regulations*, the CFMWS NM ATIP shall retain these records for a minimum of two years, and make them available to the Privacy Commissioner, upon request.

#### **Paragraph 8(2)(f) – Provinces, foreign states and international bodies**

Paragraph 8(2)(f) of the Act allows for the disclosure of personal information to a province or foreign state for purposes of administering or enforcing any law or carrying out a lawful investigation as long as there is an agreement or arrangement in place.

The Minister of Justice and Attorney General of Canada entered into umbrella agreements with all of the provinces and the Yukon, with the exception of the North West Territories, when the *Privacy Act* was proclaimed in force in 1983. It should be noted that these 8(2)(f) umbrella agreements only authorize federal institutions to disclose personal information in response to one-time or infrequent requests for disclosure from a provincial institution (defined in each of the said agreements).

There are a number of requirements to be considered in allowing paragraph 8(2)(f) disclosures:

- disclosure may only be done at the written request of the other jurisdiction;
- the request must specify the personal information being requested and the purpose for which it will be used, and the purpose must relate to the administration of an act or for law enforcement (not in relation to a vague inquiry);

- these are one-way disclosures from the federal institution to the other jurisdiction and the agreements do not encompass exchanges of information from the other jurisdictions back to the federal institution; and,
- the institution may, but is not obliged to disclose the requested information, as paragraph 8(2)(f) is discretionary.

Furthermore, as some Charter issues may arise from the use of this section, a subpoena, warrant or Court order may be required prior to disclosing personal information to a provincial organisation.

Managers should therefore consult the CFMWS NM ATIP prior to disclosing personal information to a province, foreign state or international body under this paragraph.

### **Paragraph 8(2)(g) – Member of Parliament**

Managers and designated staff may disclose personal information to a Member of Parliament (MP – includes both members of the House of Commons and the Senate) for the purpose of assisting the individual to whom the information relates in resolving a problem. Only the specific information required for the resolution of the problem may be disclosed under this provision.

It should be noted that once Parliament has been dissolved prior to an election, and until a new MP is sworn in, this provision may not be applied. Once an MP has resigned, personal information may be provided to the former MP only with the express consent of the individual.

### **Paragraph 8(2)(h) – Audit purposes**

Managers and designated staff may disclose personal information to officers or employees of the National Defence Assistant Deputy Minister (Review Services) and CFMWS Compliance and Assurance Section for internal audit purposes only and not as part of any decision-making process concerning the individual to whom the information relates.

### **Paragraph 8(2)(i) – Archival purposes**

Staff responsible for the retention and disposal of files are authorized to forward files that contain personal information to the Library and Archives Canada and Federal Records Centres located across the country for storage and disposal, in accordance with the retention and disposal schedules.

### **Paragraphs 8(2)(j) – Research or statistical purposes**

Requests for the disclosure of personal information for research or statistical purposes should be forwarded to the CFMWS NM ATIP, as only a delegate under the *Privacy Act* can make decisions under this provision.

### **Paragraph 8(2)(k) – Native claims research**

Managers should consult the CFMWS NM ATIP for an invasion-of-privacy test prior to disclosing personal information for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada.

### **Paragraph 8(2)(l) – Payment of a benefit and collection of a debt**

Managers and designated staff may disclose personal information to any government institution for the purpose of locating an individual in order to collect a debt owing to the Crown or to make a payment owing to the individual by the Crown.

The scope of this provision is rather limited. It aims to more easily find individuals who have a debt to the Crown and to more easily disburse federal benefits. It is important to understand that it does not permit the disclosure of personal information to determine if the individual is a debtor or not, nor does it authorize the disclosure of more information than is necessary to recover money from the individual. Thus, only the information necessary to locate the individual may be communicated under this provision.

### **Paragraph 8(2)(m) – Public interest**

Requests for the disclosure of personal information in the public interest should be forwarded to the CFMWS NM ATIP, as only a delegate under the *Privacy Act* may make a discretionary decision under this provision, for any purpose where (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or (ii) disclosure would clearly benefit the individual to whom the information relates:

The CFMWS NM ATIP will conduct an invasion-of-privacy test, prior to making a disclosure of personal information in the public interest.



## **ANNEXE B : LIGNES DIRECTRICES SUR LA DIVULGATION DE RENSEIGNEMENTS PERSONNELS EN VERTU DU PARAGRAPHE 8(2) DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**

Les présentes lignes ont pour objet d'établir les personnes autorisés à prendre des décisions discrétionnaires relatives à la divulgation, à clarifier les circonstances dans lesquelles peuvent être divulgués des renseignements personnels gérés dans le cadre de responsabilisation des BNP sans le consentement de la personne qu'ils touchent, en vertu du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*, et à préciser les exigences de conservation de ces renseignements.

### **1. Lignes directrices**

Le paragraphe 8(2) de la *Loi* décrit les différentes circonstances dans lesquelles des renseignements personnels qui relèvent d'une institution fédérale peuvent être divulgués sans le consentement de la personne qu'ils touchent. Ces divulgations sont discrétionnaires et sont assujetties aux dispositions de toute autre loi fédérale.

Le paragraphe 8(2) de la *Loi* n'a pas préséance sur des interdictions fondées sur d'autres lois précises et **ne s'applique que lorsque aucune autre disposition législative n'existe**. Par conséquent, lorsqu'une autre loi fédérale interdit la divulgation de renseignements personnels (p. ex. article 241 de la *Loi de l'impôt sur le revenu*), ceux-ci ne peuvent pas être divulgués par l'institution.

Les renseignements divulgués en vertu du paragraphe 8(2) de la *Loi* devraient se limiter aux renseignements demandés et nécessaires à l'atteinte de l'objectif auquel ils serviront. En outre, seuls les renseignements pertinents qui concernent la personne visée par la demande peuvent être divulgués; **tout renseignement qui concerne d'autres personnes devrait être retranché du document avant la divulgation.**

*En vertu du paragraphe 9(1) de la Loi, lorsque des renseignements personnels sont divulgués à des fins qui ne figurent pas dans le fichier de renseignements personnels pertinent, un relevé des cas d'utilisation ou de divulgation doit être joint aux renseignements personnels et devrait comprendre ce qui suit :*

- *le nom et le titre de la personne qui autorise l'utilisation ou la divulgation;*
- *le nom de l'institution, de la personne, de l'organisation ou de l'organisme qui reçoit les renseignements;*
- *une description de l'utilisation ou de l'objectif de la divulgation;*
- *une copie des renseignements divulgués ou une description suffisamment détaillée pour permettre de déterminer exactement les renseignements qui ont été utilisés ou divulgués.*

D'autres lignes directrices sur la divulgation de renseignements personnels en vertu d'alinéas précis du paragraphe 8(2) de la *Loi* suivent. Les gestionnaires devraient consulter le GN AIPRP SBMFC pour obtenir des directives ou demander un examen non officiel des documents avant une divulgation.

**Nota** : Les présentes lignes directrices ne s'appliquent pas aux divulgations courantes en vertu du paragraphe 8(2) de la *Loi*, car celles-ci devraient être régies par des ententes d'échange de renseignements personnels et décrites dans les FRP pertinents. Consulter le GN AIPRP SBMFC si ces instruments ne sont pas encore en place.

## **2. Application**

### **Alinéa 8(2)a) – Objectif initial ou utilisation compatible**

Les gestionnaires et le personnel désigné peuvent divulguer des renseignements personnels aux fins auxquelles ils ont été obtenus ou compilés par le programme ou pour une utilisation compatible avec ces fins, comme il est décrit dans le FRP pertinent dans *Info Source*.

Si le FRP pertinent ne décrit pas clairement l'objectif initial ou l'utilisation compatible ou si aucun FRP n'existe, les employés devraient consulter le GN AIPRP avant la divulgation de renseignements personnels.

### **Alinéa 8(2)b) – Loi fédérale ou règlement**

Les gestionnaires et le personnel désigné peuvent divulguer des renseignements personnels aux fins qui sont conformes à toute loi fédérale ou à tout règlement pris en vertu de celle-ci qui autorise cette divulgation. Par exemple, la *Loi sur le vérificateur général* autorise expressément les ministères à divulguer des renseignements au vérificateur général ou à un membre de son bureau.

Si l'autorisation légale de divulguer les renseignements personnels n'est pas clairement précisée, ou pour toute demande reçue en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), les gestionnaires doivent consulter le GN AIPRP SBMFC avant de répondre. Il est possible que l'autorisation légale d'une autre organisation pour demander des renseignements ou exiger la production de renseignements ne constitue pas une autorisation de divulguer des renseignements personnels en vertu de la présente disposition.

### **Alinéa 8(2)c) – Assignations à témoigner, mandats, ordonnances du tribunal ou règles de procédure**

Habituellement, les assignations à témoigner et les mandats sont signifiés à l'endroit où les documents sont conservés ou aux personnes considérées comme étant en possession des documents demandés. Parfois, les parties à une procédure civile remettent à un fonctionnaire un avis de production de renseignements, une ordonnance similaire ou une assignation exigeant qu'il se présente à un interrogatoire préliminaire muni de certains documents. Il faut acheminer une telle demande, à savoir un mandat, une assignation à témoigner, une ordonnance d'un tribunal et un avis de production de renseignements, aux services juridiques, qui l'examinera attentivement pour en vérifier la validité et déterminer les mesures qui s'imposent.

Dans certains cas, il peut être approprié de demander au tribunal la permission de retrancher des documents certains renseignements de nature délicate qui ne se rapportent pas à la question débattue devant le tribunal. Dans des circonstances exceptionnelles, l'article 37 de la *Loi sur la preuve au Canada* permet même à un représentant du gouvernement de demander au tribunal de ne pas divulguer des renseignements pertinents.

### **Alinéa 8(2)d) – Procureur général**

Les gestionnaires et le personnel désigné peuvent divulguer des renseignements personnels au procureur général aux fins d'utilisation dans le cadre de poursuites judiciaires concernant l'État, en consultation avec les services juridiques.

### **Alinéa 8(2)e) – Organismes d'enquête du gouvernement fédéral**

Les demandes de renseignements personnels provenant d'organismes d'enquête du gouvernement fédéral (énumérés à l'annexe II du *Règlement sur la protection des renseignements personnels*) ainsi que les documents correspondant aux demandes et les recommandations, s'il y a lieu, doivent être immédiatement transmis au GN AIPRP SBMFC, qui est responsable de la prise d'une décision en vertu de la présente disposition.

Des renseignements personnels peuvent seulement être divulgués s'ils facilitent une activité d'application de la loi ou d'enquête légale précise, et ils ne devraient pas être divulgués en réponse à une demande de renseignements vague.

En vertu du paragraphe 8(4) de la *Loi* et de l'article 7 du *Règlement sur la protection des renseignements personnels*, le GN AIPRP SBMFC doit conserver ces documents pendant au moins deux ans et les mettre à la disposition du commissaire à la protection de la vie privée sur demande.

## **Alinéa 8(2)f – Provinces, états étrangers et organismes internationaux**

L'alinéa 8(2)f de la *Loi* permet la divulgation de renseignements personnels à une province ou à un État étranger aux fins d'administration ou d'application de toute loi ou de réalisation d'une enquête légale, à condition qu'un accord ou une entente soit en vigueur.

Le ministre de la Justice et le procureur général du Canada ont conclu des ententes-cadres avec toutes les provinces et le Yukon, mais pas avec les Territoires du Nord-Ouest, lorsque la *Loi* est entrée en vigueur en 1983. Il est à noter que ces ententes-cadres autorisent seulement les institutions fédérales à divulguer des renseignements personnels en réponse à des demandes ponctuelles ou peu fréquentes d'institutions provinciales (définies dans chacune des ententes-cadres susmentionnées).

Un certain nombre d'exigences doivent être prises en compte pour permettre la divulgation de renseignements en vertu de l'alinéa 8(2)f :

- la divulgation peut seulement être effectuée en réponse à une demande écrite d'une autre administration;
- la demande doit préciser les renseignements personnels demandés et les fins auxquelles ils seront utilisés, lesquelles fins doivent se rapporter à l'administration ou à l'application d'une loi (il ne doit pas s'agir d'une demande de renseignements vague);
- la divulgation est à sens unique, c'est-à-dire que les renseignements sont communiqués par l'institution fédérale à une autre administration publique, et les ententes ne couvrent pas la communication de renseignements d'une autre administration à l'institution fédérale;
- l'institution fédérale peut, sans y être obligée, divulguer les renseignements demandés, car l'alinéa 8(2)f est discrétionnaire.

De plus, étant donné que l'utilisation du présent alinéa peut soulever certaines questions fondées sur la *Charte canadienne des droits et libertés*, une assignation à témoigner, un mandat ou une ordonnance du tribunal peut être nécessaire avant la divulgation de renseignements personnels à une organisation provinciale.

Les gestionnaires devraient donc consulter le GN AIPRP SBMFC avant de divulguer des renseignements personnels à une province, à un état étranger ou à un organisme international en vertu du présent alinéa.

### **Alinéa 8(2)g) – Députés**

Les gestionnaires et le personnel désigné peuvent divulguer des renseignements personnels à un député (membres de la Chambre des communes et du Sénat) pour aider la personne touchée par les renseignements à résoudre un problème. Seuls les renseignements précis nécessaires à la résolution du problème peuvent être divulgués en vertu de la présente disposition.

Il est à noter qu'entre la dissolution du Parlement avant une élection et l'assermentation d'un nouveau député, la présente disposition ne s'applique pas. Une fois qu'un député a démissionné, des renseignements personnels peuvent seulement être divulgués à cet ancien député avec le consentement exprès de la personne.

### **Alinéa 8(2)h) – Vérification**

Les gestionnaires et le personnel désigné peuvent divulguer des renseignements personnels au personnel du sous-ministre adjoint (Service d'examen) de la Défense nationale et de la Section de la conformité et de l'assurance des SBMFC aux fins de vérification interne seulement et non pas dans le cadre de tout processus décisionnel visant la personne que les renseignements concernent.

### **Alinéa 8(2)i) – Archivage**

Le personnel responsable de la conservation et de l'élimination des documents du Ministère est autorisé à transmettre des documents contenant des renseignements personnels à Bibliothèque et Archives Canada et aux centres fédéraux de documents situés partout au pays aux fins d'entreposage et d'élimination, conformément aux calendriers de conservation et d'élimination.

### **Alinéa 8(2)j) – Recherche ou statistiques**

Les demandes de divulgation de renseignements personnels aux fins de recherche ou de statistiques devraient être transmises au GN AIPRP SBMFC, car seule une personne détenant des pouvoirs conférés par la *Loi* peut prendre des décisions en vertu de la présente disposition.

### **Alinéa 8(2)k) – Recherche sur les revendications autochtones**

Les gestionnaires devraient consulter GN AIPRP SBMFC pour qu'il prenne en considération le critère d'atteinte à la vie privée avant la divulgation de renseignements personnels aux fins de recherche sur les revendications, les conflits ou les griefs d'autochtones du Canada ou de validation de ces revendications, de ces conflits ou de ces griefs.

### **Alinéa 8(2)l) – Versement de prestations ou perception d'une dette**

Le personnel peut divulguer des renseignements personnels à toute institution gouvernementale pour trouver une personne qui a une dette envers l'État ou à laquelle l'État doit verser un paiement.

La portée de la présente disposition est plutôt limitée. Elle vise à faciliter la recherche de personnes qui ont une dette envers l'État et le versement des prestations fédérales. Il est important de comprendre qu'elle ne permet pas la divulgation de renseignements personnels pour déterminer si une personne est un débiteur ni la divulgation de renseignements autres que ceux qui sont nécessaires pour recouvrer un montant auprès de la personne. Par conséquent, seuls les renseignements nécessaires pour trouver la personne peuvent être communiqués en vertu de la présente disposition.

### **Alinéa 8(2)m) – Intérêt public**

Les demandes de divulgation de renseignements personnels devraient être transmises au GN AIPRP SBMFC, car seule une personne détenant des pouvoirs conférés par la *Loi* peut prendre des décisions discrétionnaires en vertu de la présente disposition lorsque : (i) l'intérêt public l'emporte nettement sur toute atteinte à la vie privée qui pourrait découler de la divulgation; (ii) la personne touchée par les renseignements tirerait un avantage certain de la divulgation.

Le GN AIPRP SBMFC prendra en considération le critère d'atteinte à la vie privée avant de procéder à la divulgation de renseignements personnels dans l'intérêt public.