Commissariat
à la protection de
la vie privée du Canada

UN GUIDE POUR LA PRÉSENTATION D'ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE AU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA

Nos attentes

TABLE DES MATIÈRES

1. PROCESSUS D'EFVP

L'EFVP est un processus qui permet de déterminer si des initiatives comportant l'usage de renseignements personnels posent des risques pour la protection de la vie privée, de mesurer, décrire et quantifier ces risques ainsi que de proposer des solutions dans le but de les éliminer ou de les ramener à un niveau acceptable. Le gouvernement canadien a été un pionnier à l'échelle internationale pour ce qui est du recours aux EFVP pour s'assurer que la protection de la vie privée est prise en compte dans le cadre de l'élaboration de programmes et d'initiatives. En vertu de la Politique d'évaluation des facteurs relatifs à la vie privée du gouvernement du Canada, entrée en vigueur en 2002, la plupart des institutions fédérales doivent élaborer et mettre à jour des EFVP afin de déterminer si les programmes et initiatives de prestation de services prévoyant la collecte, l'utilisation ou la communication de renseignements personnels respectent les lois, politiques, lignes directrices et pratiques exemplaires en matière de protection de la vie privée. Plus récemment, dans le cadre du processus de renouvellement des politiques du SCT et dans le but d'aider les institutions fédérales à simplifier leurs processus d'EFVP, la Politique d'EFVP a été remplacée par la Directive sur l'évaluation des facteurs relatifs à la vie privée. Tout comme la Politique, la Directive s'applique aux 250 institutions fédérales énumérées dans l'annexe de la *Loi sur la protection des renseignements personnels*, y compris aux sociétés d'État mère et à leurs filiales en propriété exclusive. Elle ne s'applique pas à la Banque du Canada.

La Directive, entrée en vigueur le 1er avril 2010, sera mise en œuvre par étapes à compter du 1er avril 2011. En vertu de celle-ci, les administrateurs généraux doivent mettre en place un processus d'élaboration et d'approbation des EFVP. On y énonce également les exigences à respecter pour établir ou modifier des fichiers de renseignements personnels (FRP)[1] et réaliser une EFVP de base pour les activités et programmes

[1] Un fichier de renseignements personnels (FRP) est une liste de tous les renseignements personnels détenus par une institution fédérale qui ont été, sont ou peuvent être utilisés à des fins administratives ou qui sont récupérables à partir du nom de la personne ou d'un numéro, symbole ou autre indication permettant de l'identifier. En vertu de la *Loi sur la protection des renseignements personnels*, les institutions fédérales doivent rendre des comptes au public quant à la façon dont elles utilisent ces renseignements en diffusant une description de ses FRP dans *Info Source*, rendue publique chaque année par le SCT. Les gens consultent *Info Source* pour savoir comment et où leurs renseignements personnels sont utilisés et conservés afin d'être en mesure d'exercer leur droit d'accès et de correction.

Le présent document vise à faire la lumière sur notre processus d'analyse des risques pour la protection de la vie privée associés aux initiatives gouvernementales et à exposer nos attentes à l'égard des institutions fédérales concernant le type de renseignements et le niveau de détails que nous souhaiterions voir dans les rapports sur les évaluations des facteurs relatifs à la vie privée (EFVP) que nous examinons. La Directive du Secrétariat du Conseil du Trésor (SCT) sur l'évaluation des facteurs relatifs à la vie privée d'avril 2010 ne précisant pas de format obligatoire pour les EFVP (le contenu obligatoire est décrit à l'annexe C de la Directive), les institutions ont le loisir d'adapter, ou de personnaliser, leurs processus et leurs rapports en la matière pour permettre la meilleure analyse possible des risques pour la protection de la vie privée et le respect optimal des obligations à l'égard de la population canadienne concernant la protection de la vie privée et la transparence du processus. Nos suggestions ont pour but d'aider les institutions à ce chapitre.

comportant des renseignements personnels qui ont été nouvellement établis ou qui ont subi des modifications substantielles. L'EFVP de base doit inclure une description générale du programme ou de l'activité, le pouvoir législatif ainsi qu'une échelle d'évaluation du risque normalisée indiquant le type de renseignements personnels recueillis de même que la catégorie d'utilisation et de communication envisagée. Elle établit les exigences de base à l'égard des renseignements devant être communiqués au SCT conformément aux obligations en matière de gestion des risques pour la protection de la vie privée. La Directive stipule toutefois que l'EFVP de base n'est qu'un point de départ. Il incombe aux responsables des ministères de déterminer s'il y a lieu de faire une analyse plus poussée, qui pourrait comprendre l'élaboration d'une EFVP plus détaillée.

Le CPVP a été parmi les premiers à promouvoir le recours aux EFVP comme mesure préventive. Il appuie sans réserve leur utilisation à titre d'important exercice d'atténuation des risques liés à la protection de la vie privée et d'outil de planification pour les institutions fédérales. Le Commissariat a fait équipe avec le SCT pour l'élaboration de la première Politique d'EFVP et a consulté ce dernier dans le cadre de la nouvelle directive. Les EFVP peuvent révéler les risques pour la protection de la vie privée et cibler des mesures facilitant l'observation de la Loi, veiller à ce que les problèmes relatifs à la protection de la vie privée qui préoccupent le public soient résolus ou atténués, assurer une responsabilité relativement à l'utilisation de renseignements personnels et informer de manière transparente les Canadiennes et les Canadiens quant à la façon dont sont traités leurs renseignements personnels que le gouvernement a en sa possession.

Les EFVP fournissent également aux gestionnaires et aux décideurs l'information dont ils ont besoin pour faire des choix réfléchis en matière de conception de politiques, de programmes et de systèmes, réduisant ainsi considérablement les risques de devoir mettre fin à des programmes ou à des services, ou encore de leur apporter d'importantes modifications après leur mise en œuvre, afin de se conformer aux exigences relatives à la protection de la vie privée. Grâce au respect des bonnes pratiques en la matière énoncées dans le processus d'EFVP, les opérations sont mieux gérées et plus efficaces, et les Canadiennes et les Canadiens comprennent la façon dont le gouvernement traite leurs renseignements personnels et ont confiance que cette tâche sera exécutée de manière responsable.

En vertu de la nouvelle directive du SCT sur les EFVP, les institutions doivent faire une EFVP pour des programmes et activités lorsque :

- des renseignements personnels sont utilisés ou le seront dans le cadre d'un processus décisionnel touchant directement des personnes;
- des modifications importantes aux programmes ou aux activités déjà en place comportant des renseignements personnels qui sont utilisés ou qui le seront à des fins administratives;
- la sous-traitance ou le transfert des programmes ou des activités à un autre palier de gouvernement ou au secteur privé donne lieu à une modification importante des programmes ou des activités.

Dans de telles circonstances, les institutions doivent au moins effectuer une EFVP de base et pourraient décider d'examiner et de documenter davantage les risques liés à la protection de la vie privée dans une évaluation plus approfondie si les responsables de l'institution estiment que c'est nécessaire. En vertu de la Directive, l'institution doit envoyer, au même moment, une copie de l'EFVP de base approuvée au CPVP et au SCT. Il est indiqué dans la Directive que les agents du SCT examineront l'EFVP de base uniquement pour s'assurer qu'elle contient les renseignements requis. Par ailleurs, le SCT procédera à l'examen et à l'approbation des descriptions des fichiers de renseignements personnels annexées comme il est prévu dans la *Loi sur la protection des renseignements personnels*. La Directive énonce que le SCT ne donnera pas d'autres commentaires ou avis sur les EFVP et n'examinera pas les documents ou autres renseignements qui ne font pas partie de l'évaluation de base. Cependant, le CPVP fera un examen approfondi des EFVP et de tous les documents connexes et fournira des conseils, commentaires, services de consultations et recommandations aux institutions.

Aux termes de la Directive, les responsables des institutions ont la responsabilité de déterminer si les risques pour la protection de la vie privée d'une initiative sont suffisamment d'une importance qui justifie le recours à davantage de documentation, une analyse plus poussée ou des stratégies accrues d'atténuation des risques. On convient que ce ne sont pas toutes les initiatives qui nécessiteront plus qu'une EFVP de base afin de bien évaluer et atténuer les risques pour la protection de la vie privée; le cas échéant, les institutions n'auront pas à aller au-delà des exigences associées à une EFVP de base. Le CPVP ne fait pas une évaluation approfondie de toutes les EFVP portant sur des initiatives gouvernementales utilisant des renseignements personnels qu'il reçoit. Nous réservons plutôt nos ressources pour les initiatives qui, de notre point de vue, représentent le plus de risques. Il n'est pas rare que nous ayons besoin de renseignements supplémentaires pour faire l'examen de ces initiatives plus complexes et/ou intrusives. Prévoyant ce genre de situation, la Directive stipule que les institutions devront fournir au CPVP tout renseignement qu'il pourrait demander en vue de mieux comprendre les risques et l'incidence de l'initiative pour la protection de la vie privée. Au cours de l'examen d'une initiative, le personnel du CPVP peut consulter les institutions par téléphone ou par courriel et planifier des réunions pour discuter de préoccupations et poser des questions. Nos commentaires et conseils sont transmis aux ministères sous forme de lettres de recommandations auxquelles ils doivent répondre.

Depuis l'adoption de la Politique d'EFVP en 2002, le SCT a fourni aux institutions fédérales de nombreux outils et documents d'orientation pour les aider à rédiger leurs EFVP, dont les Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée, fondées sur la Politique. Les institutions pouvaient y trouver des conseils détaillés afin de déterminer s'il y avait lieu de réaliser une EFVP ainsi qu'une section sur la présentation des rapports. De plus, le SCT offrait un outil d'apprentissage en ligne, également fondé sur l'ancienne politique, aux institutions fédérales.[2] D'autres renseignements pertinents se trouvent également dans la réglementation prise en vertu de la *Loi sur la protection des renseignements personnels* de même que dans des politiques, directives et lignes directrices connexes du SCT, dont la Politique sur la protection de la vie privée et la Directive sur le numéro d'assurance sociale. Le SCT serait en train d'élaborer un guide de

[2] Voir l'annexe B pour une liste des outils et ressources concernant les EFVP.

l'utilisateur dans le but d'aider les institutions à respecter les exigences de la nouvelle directive. Nous espérons que notre document d'orientation permettra de compléter l'information fournie par le SCT et aidera les institutions fédérales à comprendre nos besoins en matière de renseignements supplémentaires et notre rôle particulier dans le processus d'examen des EFVP. En raison de notre mandat de gardien du droit à la vie privée des Canadiennes et des Canadiens, nous devons avoir une vue d'ensemble des risques pour la protection de la vie privée et nous devons constamment remettre en question la pertinence des programmes, projets ou initiatives portant atteinte à la vie privée qui utilisent les renseignements personnels des Canadiennes et des Canadiens. Pour ce faire, il est possible que nous ayons à exiger de la part des institutions qu'elles nous fournissent des renseignements et une analyse plus détaillés.

2. EXAMEN PAR LE CPVP DES ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE

Depuis qu'il est chargé de l'examen des EFVP, soit depuis l'adoption de la Politique d'EFVP du SCT en 2002, le CPVP a analysé les EFVP en fonction de la *Loi sur la protection des renseignements personnels* et des principes universels relatifs à la protection de la vie privée et à l'équité dans le traitement de l'information du *Code type sur la protection des renseignements personnels* (le *Code type*) de l'Association canadienne de normalisation. Ces principes, énoncés dans les premières lignes directrices du SCT à l'égard des EFVP, étaient à la base du questionnaire d'analyse des facteurs relatifs à la vie privée de la Politique que les ministères étaient invités à utiliser pour orienter leur examen des risques. Le CPVP continuera à utiliser les principes du Code type pour l'examen des EFVP reçues dans le cadre de la Directive simplifiée, même si le questionnaire ne s'y trouve plus. L'adhésion des institutions gouvernementales aux dix principes n'est pas obligatoire; le Commissariat encourage toutefois celles-ci à y adhérer sur une base volontaire. Ces principes sont largement acceptés et reconnus à l'échelle internationale et ils fournissent un cadre logique et cohérent pour l'analyse des facteurs relatifs à la vie privée. Le CPVP tient également compte de nombreuses autres politiques et directives du SCT dans le cadre de son examen, de même que des lignes directrices largement reconnues portant sur les pratiques exemplaires comme les Lignes directrices concernant les ententes d'échange de renseignements personnels du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) et les Principes généralement reconnus en matière de protection des renseignements personnels de l'Institut canadien des comptables agréés. Cependant, nous tiendrons compte en premier lieu de la nécessité, de la proportionnalité et de l'efficacité de ces initiatives gouvernementales qui présentent, selon nous, le plus grand risque potentiel d'atteinte au droit à la vie privée des Canadiennes et des Canadiens.

2.1 Utilisation du critère en quatre parties énoncé dans *R. c. Oakes* pour la nécessité et la proportionnalité

Comme l'ont démontré récemment des programmes controversés bien en vue du gouvernement, il est important de bien évaluer, dès le départ, les risques généraux que posent certaines initiatives pour la protection de la vie privée, ainsi que leur incidence sociale. En effet, les risques que présentent certains programmes et certaines initiatives du gouvernement doivent être mesurés et évalués en fonction de leur incidence potentielle sur notre société démocratique, nos libertés civiles et notre droit fondamental à la vie privée tel qu'il est reconnu dans le droit canadien, notamment dans la Loi *sur la protection des renseignements personnels*, la *Charte canadienne des droits et libertés* et leur jurisprudence connexe. La *Loi sur la protection des renseignements personnels* établit les droits à la vie privée fondamentaux des Canadiennes et des Canadiens en fonction de leur interaction avec le gouvernement fédéral. La Cour suprême du Canada a reconnu en de nombreuses occasions que les

[3] *Dagg c. Canada (ministre des Finances)* [1997] 2 R.C.S. 403; *Canada (Commissaire à l'information) c. Canada (Commissaire de la Gendarmerie royale du Canada)*, [2003] 1 R.C.S. 66; *Lavigne c. Canada (Commissariat aux langues officielles)* [2002] 2 R.C.S. 773; *H.J. Heinz Co. of Canada c. Canada (Procureur général)* [2006] 1 R.C.S. 441.

intérêts de nature privée méritent d'être protégés en vertu de la Charte et que la *Loi sur la protection des renseignements personnels* est de nature quasi constitutionnelle[3].

Par conséquent, nous attendons des entités fédérales qui entreprennent des EFVP relativement à des initiatives ou à des technologies particulièrement intrusives ou portant atteinte à la vie privée qu'elles prouvent avant toute chose que l'initiative ou le programme est nécessaire à l'atteinte d'un but précis et légitime, qu'il ou qu'elle a des chances d'être efficace dans l'atteinte de ce but, que l'atteinte à la vie privée est proportionnelle aux avantages qui en découleront et qu'aucun autre moyen qui porterait moins atteinte à la vie privée ne permettrait d'atteindre le même objectif. Afin d'orienter cette analyse, nous demanderons aux ministères de répondre aux quatre questions suivantes fondées sur le critère utilisé dans *R. c. Oakes*[4] pour évaluer les limites raisonnables des droits et libertés dans une société libre et démocratique :

- Peut-il être démontré que la mesure est nécessaire pour répondre à un besoin précis?
- Est-elle susceptible d'être efficace pour répondre à ce besoin?
- L'atteinte à la vie privée est-elle proportionnelle à l'avantage obtenu?
- Existe-t-il un moyen d'arriver au même but tout en réduisant l'atteinte à la vie privée?

Dans le contexte des EFVP, nous demandons aux entités fédérales d'établir d'abord que les programmes et les initiatives qui empiètent sur la vie privée sont liés de manière rationnelle à un objectif public urgent et important. Cette démonstration doit être claire et précise et ne pas répéter simplement le mandat de l'institution, par exemple « application de la loi » ou « contrôle frontalier ».

Nous demandons également aux institutions de nous montrer la façon dont la collecte ou l'utilisation proposée des renseignements personnels répondront précisément au besoin tel qu'il a été décrit. Pour ce faire, il faut des preuves empiriques à l'appui de l'initiative afin d'empêcher la collecte de renseignements personnels « au cas où » ou la conservation de renseignements qui pourraient s'avérer utiles à des fins non encore déterminées.

Par la suite, nous demandons aux institutions de nous montrer comment elles comptent s'assurer que la collecte, l'utilisation et la communication des renseignements personnels sont effectuées de manière à porter le moins possible atteinte à la vie privée. Cette analyse vise à dissuader les institutions de recueillir ou de partager des renseignements de façon excessive. Enfin, nous demandons aux entités d'envisager le recours à d'autres méthodes qui porteraient moins atteinte à la vie privée et/ou à d'autres renseignements pour atteindre leurs objectifs, tels que des données anonymes ou regroupées, un contrôle de sécurité physique au lieu d'un contrôle de l'identité, lequel exige la collecte d'une grande quantité de renseignements personnels, ou des technologies permettant de protéger la vie privée.

[4] *R. c. Oakes* [1986] 1 R.C.S. 103.

2.2 Utilisation du Code type sur la protection des renseignements personnels

Après avoir répondu aux questions initiales du critère en quatre parties et justifié la collecte et l'utilisation des renseignements personnels proposées, les institutions doivent démontrer que les renseignements détenus par le gouvernement le sont de façon sécuritaire. Pour ce faire, elles doivent effectuer une analyse des risques du projet, du programme ou de l'initiative par rapport aux dix principes universels relatifs à la protection de la vie privée et à l'équité dans le traitement de l'information du Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation. Comme il en a été question ci dessus, nous estimons que ces principes fournissent un cadre logique et accessible pour réaliser l'analyse des facteurs relatifs à la vie privée. Le CPVP s'attend à ce que l'EFVP contienne des descriptions complètes et exactes de la façon dont ces dix principes sont pris en compte dans l'élaboration des initiatives fédérales impliquant des renseignements personnels.

Les dix principes, légèrement modifiés pour leur adaptation au secteur public, se trouvent ci-après, accompagnés d'exemples d'attentes possibles du CPVP quant au contenu de l'EFVP présentés en italique à la suite des principes. Ces exemples ne sont pas exhaustifs, mais ils offrent un aperçu du genre de renseignements que nous voulons obtenir en vue de l'examen des EFVP. L'annexe C présente une liste de vérification de la présentation souhaitée pour l'EFVP ainsi que les documents connexes que nous exigeons habituellement.

2.2.1 Responsabilité

Les institutions fédérales sont responsables des renseignements personnels dont elles ont la gestion et doivent désigner une ou des personnes qui devront veiller au respect des principes énoncés ci-dessous. Cela est également conforme aux exigences de la section 6 de la Directive sur l'évaluation des facteurs relatifs à la vie privée et comprend la responsabilité associée à l'établissement d'un processus d'élaboration et d'approbation des EFVP ainsi qu'à l'établissement et à la modification, au besoin, des FRP.

Les institutions fédérales sont responsables des renseignements personnels qu'elles ont en leur possession ou sous leur garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. Elles devraient, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. La section 6.2.10 de la Politique du SCT sur la protection de la vie privée reprend

En vertu de ce principe, le CPVP s'attendrait à voir ce qui suit : des documents sur la structure administrative en place relativement à la protection de la vie privée, y compris des commentaires formulés par les directions générales responsables des services juridiques, de l'accès à l'information et de la protection des renseignements personnels et des technologies de l'information d'une institution et des processus définis permettant de déterminer si les projets proposés doivent faire l'objet d'une EFVP, de les réaliser, de mettre en œuvre des mesures pour atténuer les risques et de faire une vérification à des fins d'assurance de la conformité. Nous nous attendons aussi à ce qui suit : les rapports d'EFVP sont approuvés à l'échelon approprié, la formation sur les enjeux et les procédures

ce principe et prévoit la nécessité de s'assurer que des clauses de protection de la vie privée appropriées sont prévues aux contrats conclus avec des organisations du secteur privé, d'autres ministères fédéraux ou des partenaires du secteur public lorsque ceux-ci donnent lieu à une circulation intergouvernementale ou transfrontalière de renseignements personnels.

Les institutions fédérales devraient mettre en œuvre des politiques et des pratiques destinées à donner suite aux principes : la mise en œuvre de procédures spécifiques pour protéger les renseignements personnels, de mécanismes de traitement des plaintes, des demandes de renseignements et des recours, la formation du personnel et la rédaction de documents où seraient expliqué au public de manière transparente les politiques et procédures.

en matière de protection de la vie privée est bien documentée et les employés reçoivent fréquemment des mises à jour, le libellé concernant la protection de la vie privée figure dans tous les contrats où des tierces parties traiteront des renseignements personnels, conformément aux documents d'orientation du SCT et aux pratiques exemplaires reconnues à l'échelle internationale, et des vérifications régulières de la protection de la vie privée sont exécutées comme prévu et les constatations relevées, mises en œuvre.

2.2.2 Détermination des fins de la collecte des renseignements

Les fins auxquelles des renseignements personnels sont recueillis doivent être établies et documentées par l'institution avant la collecte ou au moment de celle-ci. Les institutions doivent déterminer si les renseignements qu'elles envisagent de recueillir sont nécessaires et raisonnables dans le contexte de leurs programmes ou activités. Cette mesure se veut conforme à la *Loi sur la protection des renseignements personnels* et à la section 5 de la Directive du SCT sur les pratiques relatives à la protection de la vie privée, et est liée au principe de limitation de la collecte.

Les fins auxquelles des renseignements personnels sont recueillis devraient être précisées au public au moyen d'*Info Sourc*e et d'autres mécanismes de communication, et/ou directement à la personne concernée. Cette mesure est conforme à l'article 4 de la *Loi sur la protection des renseignements personnels* et est incorporée par renvoi dans l'échelle d'évaluation du risque de la Directive du SCT sur l'EFVP. À défaut du consentement de la personne concernée,

En vertu de la Loi sur la protection des renseignements personnels, les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités; le CPVP s'attendrait donc à voir une description claire du programme et les raisons justifiant la collecte de chaque renseignement; une description du pouvoir législatif pour la collecte; une liste claire de tous les éléments de données recueillis; des copies de tout document pertinent comme des formulaires de demande soulignant les fins de la collecte ou des avis en ligne concernant l'utilisation; une copie d'une description à jour du fichier de renseignements personnels (FRP); un énoncé de toute nouvelle utilisation compatible proposée des renseignements préalablement recueillis et une justification claire de la façon dont cette utilisation est raisonnablement et directement liée aux fins initiales de la collecte (cela pourrait comprendre une analyse des attentes

les renseignements relevant d'une institution fédérale ne peuvent servir qu'aux fins auxquelles ils ont été recueillis de même que pour les usages qui sont compatibles avec ces fins.

Le CPVP est d'avis que la définition d'un « usage compatible » devait être interprétée de façon restrictive, et qu'une vérification du critère du « lien raisonnable et direct » devrait être effectuée. Ce principe est étroitement lié à celui de la limitation de la collecte, ainsi qu'à celui de la limitation de l'utilisation, de la communication et de la conservation. Les renseignements peuvent aussi être utilisés aux fins auxquelles ils sont communiqués à l'institution, conformément au paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*, ce qui procure à l'institution une plus grande certitude selon laquelle elle est autorisée à se servir des renseignements personnels aux fins auxquelles ces renseignements lui ont été communiqués aux termes du même paragraphe. Celles-ci pourraient comprendre l'utilisation des renseignements en vue de recouvrer des dettes dues à la Couronne, par exemple, ou leur utilisation dans des circonstances où l'intérêt du public l'emporte sans conteste sur l'ingérence dans la vie privée.

raisonnables de la personne concernée par les renseignements envers leur utilisation à cette fin); un énoncé présentant toute utilisation secondaire prévue des renseignements; la question de savoir si les renseignements sont recueillis directement auprès de la personne et, dans la négative, les raisons sous-jacentes; une description de la façon dont les renseignements personnels utilisés à des fins de planification, de prévision ou de statistiques seraient présentés de manière anonyme ou dépersonnalisée.

2.2.3 Consentement

Les pratiques équitables en matière de renseignements stipulent généralement qu'une personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. Cependant, le consentement de la personne joue un rôle relativement mineur dans les lois sur la protection des données visant le secteur public, y compris dans la *Loi sur la protection des renseignements personnels*. Les institutions fédérales recueillent une grande quantité de renseignements personnels sans le consentement des personnes concernées, puisque le gouvernement a le pouvoir législatif de le faire. Il est aussi possible de recueillir, d'utiliser et de communiquer des renseignements

Ce principe est étroitement lié à celui de la détermination des fins de la collecte des renseignements, en vertu duquel le CPVP s'attendrait à voir ce qui suit : une copie du libellé sur les formulaires ou les sites web; une description claire des fins de collecte; les raisons expliquant la décision de ne pas solliciter le consentement de l'intèressé, comme le prévoit la Loi sur la protection des renseignements personnels; pour les sites web, une copie de l'énoncé de confidentialité en vertu duquel les renseignements personnels sont fournis à l'institution.

à l'insu de la personne concernée et sans son consentement si tenter d'obtenir ce consentement va à l'encontre du but visé – par exemple, lorsqu'on recueille des renseignements aux fins d'application de la loi, de détection d'une fraude ou de sa prévention.

Il est à noter que même si le consentement est obtenu lorsqu'il y a lieu de le faire, cela n'élimine pas l'exigence selon laquelle l'institution doit avoir l'autorité légitime de recueillir des renseignements personnels, ni celle selon laquelle ces renseignements doivent être directement liés au programme ou à l'activité. Si le consentement n'est pas nécessaire, les fins de la collecte doivent être énoncées de sorte que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

L'énoncé des fins de la collecte peut revêtir différentes formes. On peut, par exemple, se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisé, s'il y a lieu, et comprend que ceux-ci peuvent être communiqués ou le seront en vertu d'un pouvoir conféré par la loi ou par certaines dispositions de la *Loi sur la protection des renseignements personnels*.

2.2.4 Limitation de la collecte

Seuls les renseignements personnels nécessaires aux fins déterminées doivent être recueillis. Tel qu'il est stipulé à l'article 4 de la *Loi sur la protection des renseignements personnels*, les institutions ne doivent pas recueillir de renseignements de façon arbitraire et peuvent seulement recueillir les renseignements ayant un lien direct avec leurs programmes ou leurs activités. Les institutions devraient veiller à ce que tant la quantité que la nature des renseignements recueillis soient restreintes à ce qui est nécessaire pour réaliser les fins déterminées. Ce principe est étroitement lié à celui de la détermination des fins de la collecte des renseignements et à celui du consentement.

En vertu de ce principe, le CPVP s'attendrait à voir ce qui suit : une justification claire quant au besoin de recueillir chaque élément de données, conformément à l'obligation énoncée dans la Loi sur la protection des renseignements personnels voulant que les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités; une indication précisant qu'un exercice de minimisation des données a été entrepris afin de veiller à ce que chaque élément de donnée soit nécessaire, et que cet exercice sera repris régulièrement; une indication stipulant que l'information recueillie à partir d'un autre ministère à des fins d'utilisation secondaire est épurée de tous les éléments non essentiels avant l'utilisation.

2.2.5 Limitation de l'utilisation, de la communication et de la conservation

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'y autorise ou l'exige. Ces renseignements ne peuvent être conservés que pendant la période de temps nécessaire à ces fins. La *Loi sur la protection des renseignements personnels* précise que les renseignements personnels peuvent être utilisés ou communiqués sans le consentement de la personne uniquement dans les circonstances prévues à l'article 8. Tel qu'il a été mentionné précédemment pour le principe de la détermination des fins de la collecte des renseignements, les renseignements peuvent aussi être utilisés aux fins auxquelles ils pourraient être communiqués à l'institution, conformément au paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*. Les institutions qui envisagent de se servir de renseignements personnels à des fins nouvelles doivent s'assurer soit que le consentement est obtenu, soit que la nouvelle utilisation constitue un « usage compatible ».

En vertu de ce principe, le CPVP s'attendrait à voir ce qui suit : une description des utilisations spécifiques et de la communication proposée de l'information; un énoncé clair restreignant l'utilisation de l'information aux fins désignées; une politique de conservation et un calendrier d'élimination clairs également notés dans la FRP; un processus de destruction de l'information, conformément à la Loi sur la protection des renseignements personnels et à son règlement; des exemplaires des PE ou des accords avec des tiers à qui l'information sera communiquée afin

Pour que l'utilisation ou la communication soit compatible, elle doit avoir un lien raisonnable et direct avec les fins pour lesquelles les renseignements ont été recueillis ou compilés. Les institutions devraient élaborer des lignes directrices et des procédures pour la conservation des renseignements personnels, et celles-ci devraient préciser les durées minimales et maximales de conservation, conformément à la *Loi sur la protection des renseignements personnels* et au Règlement sur la protection des renseignements personnels. Les institutions devraient détruire, effacer ou dépersonnaliser les renseignements personnels dont elles n'ont plus besoin aux fins précisées. Ce principe est étroitement lié à celui du consentement, à celui de la détermination des fins de la collecte des renseignements et à celui de l'accès aux renseignements personnels.

d'en régir l'utilisation, la conservation et la communication, ainsi que des clauses visant les entrepreneurs et les sous-traitants de l'information et stipulant que l'institution d'origine a le droit de procéder à la vérification du respect de la vie privée.

2.2.6 Exactitude

Le principe d'exactitude précise que les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés. La *Loi sur la protection des renseignements personnels* demande aux institutions fédérales de veiller, dans la mesure du possible, à ce que les renseignements personnels soient à jour, exacts et complets. Au moment d'appliquer ce principe, il faut tenir compte des intérêts de la personne – les renseignements devraient être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient utilisés pour prendre une décision à son sujet.

En vertu de ce principe, le CPVP s'attendrait à voir ce qui suit : une description du processus utilisé par les entités afin de veiller à l'exactitude, en particulier lorsque des décisions administratives sont prises; une description de la façon dont les changements aux dossiers sont enregistrés et suivis; un énoncé concernant le recours au processus décisionnel automatisé fondé sur les profils de risque et la façon dont les décisions automatisées sont examinées pour en vérifier l'exactitude; une explication des processus accessibles aux personnes cherchant à corriger de l'information; une description du processus par lequel les deuxième ou tierces parties à qui l'information a été communiquée seront avisées des modifications et des corrections apportées au dossier; une description de la façon dont les pistes de vérification des transactions dans les dossiers sont suivies et évaluées.

2.2.7 Mesures de sécurité

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les institutions doivent protéger les renseignements personnels, quelle que soit la forme sous laquelle ils sont conservés. La nature des mesures de sécurité variera en fonction de la nature délicate des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements de nature plus délicate devraient être mieux protégés. Les méthodes de protection devraient comprendre des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux; des mesures administratives, par exemple des autorisations de sécurité et un accès sélectif; des mesures techniques, par exemple l'usage de mots de passe et du chiffrement. Les institutions doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels. Un soin particulier doit être apporté au moment du retrait ou de la destruction des renseignements personnels.

En vertu de ce principe, le CPVP s'attendrait à voir ce qui suit : une description des mesures de protection physiques et électroniques de l'information; une évaluation de la menace et des risques (EMR) dont l'accent est mis sur les risques et les préoccupations en matière de protection de la vie privée, ainsi qu'une discussion sur la façon dont ces préoccupations ont été traitées et réglées; une note indiquant que le cryptage est utilisé pour les renseignements personnels en transit ou immobiles; une description de la façon dont les journaux d'exploitation sur les transactions d'information sont contrôlés en vue d'éviter une utilisation inappropriée, notamment la consultation de l'information; un important contrôle de l'accès électronique, notamment des contrôles sur l'accès à distance et l'utilisation d'appareils mobiles; des politiques sur l'utilisation des dispositifs de stockage portatifs comme les clés USB; une description des contrôles d'accès en fonction des rôles et des étapes entreprises pour veiller à la destruction complète de l'information à la fin de son cycle de vie.

2.2.8 Transparence

Les institutions doivent faire en sorte que des renseignements précis sur leurs politiques et pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne. Elles doivent faire preuve de transparence au sujet de leurs politiques et pratiques concernant la gestion des renseignements personnels, et ces renseignements doivent être fournis sous une forme généralement compréhensible. Les renseignements fournis doivent comprendre le nom ou la fonction de même que l'adresse de la personne responsable de la politique et des pratiques de l'institution en matière de protection des renseignements personnels et indiquer à qui il faut acheminer les plaintes, les demandes de renseignements et les demandes de recours; le moyen d'accès aux renseignements personnels; la description du genre de renseignements personnels détenus, y compris une explication générale de l'usage auquel ils sont destinés; une copie de tout dépliant ou autre document d'information expliquant les politiques et les procédures concernant l'utilisation des renseignements personnels.

2.2.9 Accès aux renseignements personnels

La *Loi sur la protection des renseignements personnels* protège la vie privée de tous les citoyens et résidents permanents du Canada en ce qui concerne les renseignements personnels dont dispose une institution fédérale. Elle accorde également à ces personnes, ainsi qu'à celles qui se trouvent au Canada et qui ne sont ni des citoyens ni des résidents permanents, le droit d'accéder à leurs renseignements personnels que possède le gouvernement et à demander à ce que des corrections y soient apportées. La publication fédérale *Info Source* offre à la population un index des renseignements personnels conservés par les institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels*. La description de l'information contenue dans les FRP doit être claire et complète, car il s'agit de l'outil destiné à assurer la transparence pour le public et à servir de référence pour les personnes qui présentent des demandes d'accès aux renseignements

En vertu de ce principe, le CPVP s'attendrait à voir ce qui suit : un résumé de l'EFVP rédigé en langage simple et compréhensible publié sur le site Web de l'institution d'une façon accessible au grand public et présentant un lien vers la description pertinente du FRP dans Info Source; en ce qui a trait aux programmes qui contiennent des renseignements de nature particulièrement délicate ou qui portent atteinte à la vie privée, le CPVP s'attendrait à voir le plan de communications publiques décrit dans l'EFVP, y compris le recours à diverses méthodes comme des affiches, des dépliants et des annonces dans les médias, ainsi que le traitement détaillé de l'EFVP dans le rapport annuel de l'institution en vertu de la Loi sur la protection des renseignements personnels; une description de la consultation avec les intervenants clés de même que le traitement des risques ou préoccupations ayant trait à la protection de la vie privée sur le site Web; le nom et les coordonnées d'une personne responsable du traitement des renseignements personnels devraient pouvoir être facilement obtenus à partir du site Web ou de la principale ligne publique de l'institution.

En vertu de ce principe, le CPVP s'attendrait à ce que l'EFVP comprenne ce qui suit : une description du processus officiel d'accès à l'information; une description de tout processus officieux d'accès aux renseignements personnels et de correction de ceux-ci; une description à jour et complète de l'information associée à l'initiative contenue dans les FRP; une description du processus par lequel les renseignements détenus par des tiers sont corrigés à la suite d'une demande; une

personnels détenus par les institutions fédérales en vertu de la Loi. Bien que ce ne soit pas tous les renseignements personnels qui puissent être divulgués sur demande, les exceptions et les exclusions devraient être appliquées de la manière la plus restrictive possible.

description de la façon dont le grand public est avisé de ces processus, par exemple un lien ou un numéro sans frais affiché sur la page d'accueil du site Web de l'institution.

2.2.10 Possibilité de porter plainte à l'égard du non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec la ou les personnes responsables du respect de ceux-ci au sein de l'institution. Les institutions doivent instaurer des procédures de réception des plaintes et des demandes de renseignements concernant leurs politiques et leurs pratiques de gestion des renseignements personnels et y donner suite. Les procédures relatives aux plaintes devraient être facilement accessibles et simples à utiliser. Si une plainte au sujet de l'utilisation des renseignements personnels est jugée fondée, des mesures devraient être prises en vue de modifier les politiques et les pratiques afin de garantir que les problèmes systémiques sont décelés et réglés.

Le CPVP s'attendrait à ce que l'EFVP traite de ce principe des manières suivantes : en désignant clairement la personne responsable de la réception et du règlement des plaintes en matière de protection de la vie privée; en décrivant les plaintes qui ont pu être reçues dans le cadre d'une activité ou d'un projet pilote semblable et la façon dont elles ont été traitées; en intégrant les questions relatives à la vie privée dans l'évaluation des projets ou les rapports de faisabilité; en expliquant comment et quand les vérifications de la conformité touchant la protection de la vie privée seront entreprises; en intégrant des renseignements sur la façon de déposer une plainte auprès du CPVP en vertu de la Loi sur la protection des renseignements personnels; en détaillant certains problèmes particuliers ou systémiques cernés en matière de protection de la vie privée dans les rapports annuels.

2.3 Le recours au plan d'action pour assurer la pertinence de l'EFVP

Une fois les risques relatifs à la vie privée recensés et les mesures d'atténuation connexes proposées, le CPVP s'attend à ce que l'institution établisse un plan d'action afin de désigner un calendrier d'exécution précis pour éliminer ou atténuer les risques ciblés et, si possible, une personne ou un poste consultatif précis responsable de la prise des mesures.

L'EFVP se veut un document évolutif; il devrait donc être examiné et mis à jour régulièrement au fil de la progression, de la modification, de l'évolution ou de la cessation du projet ou de l'initiative. Le plan d'action peut constituer un excellent outil à cet égard. Il doit comprendre un échéancier des mises à jour, révisions et ajouts réguliers à l'EFVP, un calendrier relatif à la mise à jour de l'EMR pour le système de TI du projet ou de l'initiative, de même qu'un plan de vérification et de production de rapports quant au respect des dispositions relatives à la protection de la vie privée de tous les PE ou accords sur le partage de renseignements conclus avec des tiers. Le plan d'action doit également présenter le détail du calendrier de conservation et de la planification à long terme de l'élimination, de l'entreposage sécuritaire ou de la destruction éventuels des renseignements personnels en cause. Le plan d'action de l'EFVP fait partie intégrante du cadre global de gestion de la protection des renseignements personnels de l'institution.

2.4 EFVP pluri-institutionnelles

Étant donné l'augmentation du nombre d'initiatives horizontales et l'insistance actuelle du gouvernement sur les services axés sur les clients, nous recevons un nombre accru d'EFVP pluri-institutionnelles et pluri-gouvernementales. Pour chacun des groupes d'EFVP, il importe qu'un ministère ou organisme assume un rôle de leader politique en ce qui a trait à la protection de la vie privée, afin de garantir une communication cohérente avec le Commissariat et une désignation efficace des risques relatifs à la vie privée pour l'ensemble des institutions participantes. Cela permet également d'assurer la mise en œuvre efficace de stratégies d'atténuation des risques au sein des programmes et initiatives liés. Ces démarches visent à garantir une EFVP générale qui, entre autres, présenterait une analyse de rentabilisation justifiant la nécessité, par exemple, d'un partage accru de l'information, décrirait une stratégie de communication commune afin d'informer les Canadiennes et les Canadiens du partage accru de leurs renseignements entre les ministères et fournirait une base solide pour les pratiques attendues en matière de protection de la vie privée sur laquelle s'appuieraient tous les ministères et organismes participant à l'initiative.

ANNEX A
RESSOURCES, MODÈLES ET LIGNES DIRECTRICES CONCERNANT L'EFVP

Directive du SCT sur l'évaluation des facteurs relatifs à la vie privée
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308&section=text#cha8

Politique du SCT sur la protection de la vie privée
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510

Directive du SCT sur le numéro d'assurance sociale
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=13342

Politique du SCT sur l'évaluation des facteurs relatifs à la vie privée
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12450

Lignes directrices du SCT sur l'évaluation des facteurs relatifs à la vie privée
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12451

Outil d'apprentissage en ligne pour l'EFVP
http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-fra.asp

Institut des services axés sur les citoyens – Lignes directrices concernant les ententes d'échange de renseignements personnels
http://www.iccs-isac.org/fr/practice/privacy.html

Institut canadien des comptables agréés – Principes généralement reconnus en matière de protection des renseignements personnels
http://www.icca.ca/services-et-produits/protection-des-renseignements-personnels/gen-accepted-privacy-principles/index.aspx

Association canadienne de normalisation – Code type sur la protection des renseignements personnels
http://www.csa.ca/cm/ca/fr/privacy-code/publications/view-privacy-code

Organisation de coopération et de développement économiques – Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.
http://www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html

Commissariat à la protection de la vie privée du Canada – Ressources concernant l'EFVP
http://www.priv.gc.ca/pia-efvp/index_f.cfm

Direction du dirigeant principal de l'information du SCT – Rapport sur les pratiques exemplaires relevées au cours de la mise en œuvre de la politique et des lignes directrices sur l'EFVP
http://www.tbs-sct.gc.ca/pgol-pged/pia-best/pia-best00-fra.asp

Politique du SCT sur la protection de la vie privée
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510

Document d'orientation du SCT : Prise en compte de la protection des renseignements personnels avant de conclure un marché
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do_f.asp

Atelier sur l'EFVP à l'occasion de la 29e Conférence internationale des commissaires à la protection des données et de la vie privée (2007)
http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook12_bil.pdf

ANNEX B
LISTE DE VÉRIFICATION DE LA PRÉSENTATION DE L'EFVP ET DES DOCUMENTS CONNEXES

Présentation de l'EFVP

Idéalement, les EFVP doivent comprendre les sections suivantes afin de veiller à ce que des évaluations exhaustives et complètes soient effectuées et à ce que le personnel du CPVP chargé de l'examen des EFVP puisse procéder à l'analyse sans avoir à demander des renseignements supplémentaires aux institutions qui les présentent :

- Une lettre d'accompagnement signée par une personne investie des pouvoirs délégués appropriés.
- Un survol détaillé du projet comprenant les objectifs, motifs, clients et approches de même que les programmes ou partenaires impliqués.
- Une liste de tous les intervenants et de leurs rôles et responsabilités.
- Une liste de tous les éléments de données qui impliquent des renseignements personnels de même qu'une description connexe de la circulation des données.
- Une liste des lois et politiques pertinentes qui régissent le projet afin de démontrer l'autorisation légale de recueillir des renseignements personnels.
- Une analyse des facteurs relatifs à la vie privée désignant les risques en la matière associés au projet. Au minimum, les principes universels relatifs à la protection de la vie privée devraient être évalués.
- Un plan détaillé énonçant les mesures d'atténuation des risques qui seront prises afin de traiter des risques pour la protection de la vie privée désignés dans l'EFVP. Il importe de présenter tous les risques résiduels ou actuels qui ne peuvent être traités, et d'exposer la raison pour laquelle ils ne l'ont pas été.
- Un aperçu d'une stratégie de communication centrée sur la protection de la vie privée, si la mise en œuvre d'une telle stratégie est jugée appropriée.
- Des détails sur les procédures internes relatives à ce qui suit : réaction aux incidents en matière d'atteinte à la protection des renseignements personnels, demandes d'accès et de correction, plaintes.

Documentation connexe

Certains documents sont essentiels à la réalisation d'une analyse approfondie par le CPVP des projets qui soulèvent des risques en matière de protection de la vie privée. Sans ces documents clés, il est possible que de graves risques relatifs à la vie privée ne soient pas décelés, ce qui pourrait compromettre le droit à la vie privée des Canadiennes et des Canadiens. Les documents ci-après doivent être inclus dans la présentation de votre EFVP au CPVP afin de nous aider à désigner les risques pour la protection de la vie privée et à procéder à un examen dans les meilleurs délais :

- Les politiques et procédures de protection de la vie privée propres au projet.
- Un résumé des risques pour la protection de la vie privée désignés dans toute évaluation de la menace et des risques associée à l'initiative, et un compte rendu de toutes les mesures prises afin de les traiter.
- Une copie de tout instrument juridique, accord ou protocole d'entente utilisé utilisés dans le cadre de la définition des droits et responsabilités relatifs au partage de l'information entre les parties impliquées dans l'initiative.
- Une évaluation du couplage des données.
- Des copies des contrats conclus avec les tiers relativement au partage d'information.
- Des copies de tous les formulaires utilisés pour la collecte des renseignements personnels, y compris les avis d'utilisation et énoncés de confidentialité connexes.
- Des copies de tous les documents de sensibilisation du public qui ont été élaborés et qui portent sur la gestion des renseignements personnels.
- Une description des FRP.
- Une copie du résumé de l'EFVP qui sera publié sur le site Web de l'institution.

Notes

Commissariat
à la protection de
la vie privée du Canada

Pour plus de renseignements

Veuillez visiter notre site Web au **www.priv.gc.ca**
ou nous téléphoner

Sans frais : 1-800-282-1376
Tél. : 613-995-8210
ATME/ATS : 613-992-9190
Téléc. : 613-947-6850

N° de cat. : IP54-36/2011F-PDF
ISBN : 978-1-100-96938-1