Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat

Document d'orientation :

Prise en compte de la protection des renseignements personnels avant de conclure un marché

Publié à l'intention des institutions fédérales par le Secrétariat du Conseil du Trésor du Canada

Canada

N° de catalogue BT22-106/2006F-PDF
ISBN 0-662-71532-2

Ce document est disponible sur le site Web du
Secrétariat du Conseil du Trésor du Canada à http://www.tbs-sct.gc.ca/

Ce document est aussi disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Table des matières

1. Introduction

Objectif de ce document

Ce document d'orientation vise à fournir des conseils aux institutions fédérales lorsqu'elles songent à confier à la sous-traitance des activités dans le cadre desquelles des renseignements personnels portant sur des Canadiens et des Canadiennes sont traités par des organismes du secteur privé liés par contrat ou auxquels ces derniers ont accès.

Le présent document a été conçu pour donner suite aux risques liés à la divulgation possible de renseignements personnels de Canadiens et de Canadiennes aux autorités américaines aux termes de la *USA PATRIOT Act*.

Raison d'être de ce document

Il arrive fréquemment qu'une institution fédérale accorde à contrat la gestion d'un programme ou d'un service mettant en cause des renseignements personnels sur des Canadiens et des Canadiennes à une entreprise située au Canada, aux É.-U. ou dans un autre pays. Lorsque les renseignements sont conservés ou accessibles à l'extérieur du Canada, ils peuvent alors être assujettis non seulement aux lois canadiennes, mais également à celles de l'autre pays.

L'une de ces lois est la *USA PATRIOT Act*. La Loi autorise les responsables américains d'application de la loi à demander à un tribunal une ordonnance leur permettant de consulter les dossiers personnels de tout individu dans le cadre d'une enquête antiterroriste, et ce, à l'insu des individus ou des organismes concernés. En théorie, cela signifie que, suite à des activités gouvernementales de passation de marchés, les responsables américains pourraient consulter des renseignements au sujet des Canadiens et des Canadiennes par l'intermédiaire de sociétés américaines ou de leurs filiales, même si les données se trouvent au Canada.

Bien que le risque que les autorités américaines se servent de la *USA PATRIOT Act* de cette façon soit minime, ce risque existe néanmoins. D'où la nécessité de prendre en compte certaines considérations relativement aux marchés publics mettant en cause des renseignements personnels afin d'atténuer ces risques d'atteinte à la vie privée.

La commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, a bien résumé l'importance de la *USA PATRIOT Act* :

> Les inquiétudes suscitées par les répercussions de la USA PATRIOT Act sur la protection des renseignements personnels relatifs aux Canadiens et aux Canadiennes s'inscrivent en réalité dans un thème beaucoup plus large — la mesure dans laquelle le Canada et d'autres pays s'échangent des renseignements personnels relatifs à leurs citoyens et citoyennes, et la mesure dans laquelle les renseignements qui ont été

transmis à l'étranger à des fins commerciales peuvent être obtenus par des gouvernements étrangers. L'adoption de la USA PATRIOT Act a peut-être été simplement l'événement catalyseur qui a mis ces questions à l'avant-scène.

Le gouvernement du Canada prend la question de la vie privée très au sérieux. Il soutient l'affirmation de la commissaire à la protection de la vie privée du Canada selon laquelle la *USA PATRIOT Act* met en évidence le thème plus large de l'accès aux renseignements personnels relatifs aux Canadiens et aux Canadiennes par des gouvernements étrangers.

2. Au sujet du document d'orientation

Aperçu

Le document d'orientation a été conçu par le Secrétariat du Conseil du Trésor du Canada (le Secrétariat) après consultation avec des experts du domaine de la vie privée et de la passation de marchés du gouvernement fédéral. Il est fortement recommandé de suivre les conseils offerts dans ce document afin d'atténuer tout risque d'atteinte à la vie privée.

Chaque institution est tenue responsable et redevable de tout renseignement personnel dont elle a la charge. L'article 3 de la *Loi sur la protection des renseignements personnels* définit les renseignements personnels comme étant des « renseignements, quels que soient leur forme et leur support, concernant un individu identifiable ».

Ce document vise à fournir aux représentants du gouvernement fédéral concernés par la gestion des marchés un aperçu des stratégies possibles à leur disposition pour protéger les renseignements personnels et aborde les questions relatives à la vie privée soulevées par la sous-traitance qui peuvent être associées à la *USA PATRIOT Act* ou à d'autres lois étrangères semblables.

Avantages liés à l'utilisation du présent document

Le document d'orientation vous aidera de deux façons :

1. Tout d'abord, il permet aux fonctionnaires du gouvernement d'obtenir une aide immédiate, avant qu'ils n'entreprennent un processus de passation de marchés au cours duquel des renseignements personnels pourraient être traités dans le cadre d'un projet de marché. La première phase, qui est comprise dans les étapes 1 et 2 (sous « Étapes à suivre »), vous aidera à prendre une décision éclairée à savoir s'il est approprié d'impartir ou non, ou dans les cas où un marché a déjà été conclu, s'il devrait être renouvelé ou non.

2. Ensuite, lorsqu'on aura décidé d'aller de l'avant avec la passation d'un marché, les étapes 3 à 5 vous donneront des conseils en ce qui a trait aux clauses et au libellé qui peut être pris en considération dans le cadre de demandes de proposition (DP), d'énoncés de travail (ET) et de marchés, de façon à atténuer tout risque d'atteinte à la vie privée.

Qui devrait s'en servir?

Le document d'orientation contient des directives générales à l'intention de toutes les institutions gouvernementales assujetties à la *Loi sur la protection des renseignements personnels*. Cela représente près de 170 ministères, organismes fédéraux et sociétés d'État.

En conséquence, il s'avère utile pour tous les fonctionnaires fédéraux qui participent à des programmes, et à l'élaboration et à la prestation de services qui ont trait à la collecte, à l'utilisation, à la divulgation, à la conservation et à l'élimination de renseignements personnels.

La *Loi sur la protection des renseignements personnels* est accessible à partir du site Web du ministère de la Justice Canada à l'adresse : http://lois.justice.gc.ca/fr/P-21/index.html.

3. Points à prendre en considération

Utilisation du présent document dans un contexte plus large

Le document d'orientation ne constitue qu'un guide et les institutions gouvernementales ne devraient pas uniquement s'y fier au moment de préparer un contrat ou tout autre document. Le lecteur devrait prendre connaissance des conseils qu'il contient en tenant compte des politiques et procédures du gouvernement en vigueur en matière d'acquisition. On encourage les institutions à consulter leurs conseillers juridiques et du domaine de la vie privée afin d'éviter de mauvaise interprétation et pour déterminer quelles mesures de protection des renseignements personnels s'appliquent selon leurs circonstances particulières.

Il importe de se rappeler qu'il n'existe pas de panacée et que les diverses situations possibles au moment de conclure un marché doivent par conséquent être examinées en fonction de chaque cas.

Dispositions et consultations appropriées

Selon la *Politique sur les marchés* du Conseil du Trésor, il incombe aux autorités contractantes de garantir que les documents d'acquisition comportent des dispositions adéquates concernant la protection des renseignements du gouvernement.

Politique sur les marchés
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/Contracting/siglist_f.asp.

Lorsque des renseignements personnels peuvent être traités aux termes d'un marché, les institutions devraient envisager d'inclure des clauses suffisantes pour protéger les renseignements personnels en tant que responsabilité partagée.

Les représentants des programmes devraient faire connaître aux responsables des acquisitions leur intention de donner à la sous-traitance le traitement de renseignements personnels et, au besoin, ils devraient consulter les représentants des services juridiques et du domaine de la vie privée de l'institution.

Prise en compte des exigences liées aux marchés et à la sécurité

Bien que ce document porte principalement sur la façon de régler les inquiétudes et les risques d'atteinte à la vie privée, les conseils qu'il contient peuvent s'appliquer à d'autres renseignements protégés ou classifiés qui peuvent être consultés aux termes des marchés, tels qu'ils sont définis dans la *Politique du gouvernement sur la sécurité* (PGS).

Le but du document d'orientation est de compléter les exigences et conseils concernant la passation de marchés et la sécurité déjà en vigueur au gouvernement pour protéger les renseignements personnels et autre information de nature délicate.

Ces exigences et conseils sont énoncés dans d'autres publications gouvernementales, y compris dans ce qui suit :

Guide des clauses et conditions uniformisées d'achat
http://sacc.tpsgc.gc.ca/sacc/contents-f.jsp

Manuel de la sécurité industrielle
http://dsici.gc.ca/text/ISM/toc-f.asp

Politique du gouvernement sur la sécurité et ses normes connexes
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/siglist_f.asp.

Les questions qui concernent la sécurité et le caractère confidentiel des renseignements classifiés devraient être examinées en collaboration avec les agents de négociation de marchés et les agents responsables de la sécurité de l'institution. Les autorités contractantes devraient inclure des dispositions pertinentes dans la DP et le marché qui est éventuellement attribué pour répondre aux exigences en matière de sécurité et pour faire en sorte que les marchés de sous-traitance qui pourraient être autorisés contiennent également des clauses semblables.

Au besoin, une Liste de vérification des exigences relatives à la sécurité doit être remplie et des consultations doivent être entreprises avec la Direction de la sécurité industrielle canadienne et internationale de Travaux publics et Services gouvernementaux Canada (TPSGC).

Une évaluation de la menace et des risques peut également s'avérer nécessaire dans les cas où des renseignements protégés ou classifiés (ce qui peut comprendre des renseignements personnels) seront consultés ou traités aux termes du marché.

Les institutions doivent appliquer la PGS lorsqu'elles échangent de l'information du gouvernement du Canada. De plus, les procédures relatives à la PGS pour la protection et l'entreposage de l'information doivent être lues de concert avec ce document.

Le paragraphe 10.1 de la *Norme opérationnelle sur la sécurité matérielle* de la PGS est particulièrement pertinent et peut être consulté à l'adresse suivante : http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/osps-nosm1_f.asp.

4. Point de départ

Gagner la confiance

Du point de vue stratégique, l'expression « protection des renseignements personnels » suppose davantage que le simple fait d'assurer la sécurité et de maintenir le caractère confidentiel des renseignements personnels en les protégeant contre toute utilisation abusive ou toute divulgation illégale. La protection des renseignements personnels touche également la relation de confiance qui se tisse entre les individus qui fournissent des renseignements personnels et ceux qui en font la collecte. Elle signifie que les individus peuvent être plus à l'aise à l'égard du traitement par le gouvernement de leurs renseignements personnels.

Les considérations liées à la protection des renseignements personnels sont particulièrement pertinentes lorsqu'il s'agit de marchés qui peuvent donner lieu au transfert vers l'étranger de données et de renseignements personnels. Dans ces circonstances, les renseignements personnels sont assujettis à des lois étrangères et risquent éventuellement d'être consultés.

Les étapes qui sont énoncées dans la prochaine section ont pour objet de venir en aide aux responsables de programmes et aux experts du domaine de la vie privée dans leurs consultations avec leurs conseillers juridiques en vue de déterminer s'il y a lieu de passer des marchés qui nécessitent le traitement de renseignements personnels ou, dans certains cas, de revenir sur la décision de conclure un marché, s'il en a été décide ainsi au préalable.

Prise de décision éclairée

En guise de bonnes pratiques de gestion, les institutions fédérales se penchent sur les coûts et les avantages de conclure un marché pour l'obtention d'un service. Pour toutes les décisions touchant la passation de marchés, y compris celles qui mettront en cause des renseignements personnels, les institutions tiennent compte d'une série de facteurs importants, dont les coûts de l'exécution des programmes et le niveau de service requis, avant de passer le marché.

La première étape de ce processus consiste à cerner les risques d'atteinte à la vie privée. De plus amples renseignements sur cette étape initiale et sur les autres étapes essentielles sont fournis à l'Étape 1.0 et à l'annexe A.

Afin d'identifier toutes les mesures adéquates de protection des renseignements personnels et d'accès à l'information, les représentants du gouvernement devraient tenir compte de l'annexe B, Liste de contrôle pour la protection des renseignements personnels, au moment de formuler un contrat mettant en cause des renseignements personnels ou de l'information de nature délicate. La liste de contrôle est un outil pratique qui guide le chargé de projet à l'aide d'une série de questions relatives à la protection des renseignements personnels et à l'accès à l'information qui portent sur le contrôle, la collecte, l'utilisation, la divulgation, la sous-traitance et d'autres facteurs importants pour l'élaboration d'un contrat.

La décision de faire ou de faire faire est fondée sur des considérations liées à la protection des renseignements personnels, à la sécurité et à d'autres considérations importantes de l'analyse de rentabilisation, comme la qualité et la rapidité du service, la faisabilité de réaliser le programme ou le service à l'interne, le besoin de connaissances spécialisées, les obligations et les coûts liés au commerce.

Le processus décisionnel relatif à l'acquisition repose sur une analyse multidimensionnelle et devrait être précédé de consultations avec des responsables des marchés, de la protection de la vie privée et autres responsables concernés de l'institution fédérale en cause. Même lorsque des renseignements personnels de nature très délicate sont en cause, des stratégies adéquates d'atténuation des risques d'atteinte à la vie privée, comme des clauses contractuelles, peuvent être mises en œuvre afin de réduire le niveau de risque global avant d'entreprendre le processus d'adjudication de marchés.

Ce document d'orientation vise à promouvoir l'adoption d'une démarche équilibrée et constitue le fondement d'une décision éclairée sur l'opportunité de faire appel ou non à la sous-traitance.

S’il est décidé de conclure un marché, l’Étape 4.0 de ce document propose un libellé pour les clauses contractuelles, libellé qui devrait être intégré à l’entente contractuelle pour améliorer la protection des renseignements personnels et réduire les risques.

5. Étapes à suivre

Étapes 1 à 2, Étapes préliminaires à la passation de marchés

Étape 1.0 : Marchés mettant en cause des renseignements personnels

Lorsqu’il est déterminé qu’un programme ou service mettra en cause des renseignements personnels (tels qu’ils sont définis dans la *Loi sur la protection des renseignements personnels*) au sujet d’individus identifiables et que l’on envisage de passer un marché, l’analyse de l’institution devrait comprendre les facteurs suivants :

1.1 conformité à la *Loi sur la protection des renseignements personnels* et aux politiques du Conseil du Trésor en matière de protection des renseignements personnels;

1.2 critère d’atteinte à la vie privée;

1.3 évaluation des facteurs relatifs à la vie privée (EFVP) ou évaluation préliminaire des facteurs relatifs à la vie privée (EPFVP), si cette évaluation n’a pas déjà été effectuée.

1.1 *Loi sur la protection des renseignements personnels* et politiques du Conseil du Trésor en matière de protection des renseignements personnels

Lorsque les fonctions ou les services du gouvernement fédéral sont exécutés aux termes d’un marché par des tiers, il faut faire en sorte que ses obligations en matière de protection des renseignements personnels soient respectées. Les renseignements personnels doivent être gérés de manière que l’institution fédérale respecte les principes qui fondent les pratiques équitables de gestion des renseignements qui sont reconnus dans les articles 4 à 8 de la *Loi sur la protection des renseignements personnels*, le *Règlement sur la protection des renseignements personnels*, la *Politique sur la protection des renseignements personnels* du Conseil du Trésor et sa *Politique d’évaluation des facteurs relatifs à la vie privée*. Plus précisément, l’institution doit pouvoir recueillir les renseignements personnels mis en cause dans le marché et les renseignements doivent avoir, conformément à l’article 4 de la Loi, « un lien direct avec ses programmes ou ses activités ».

1.2 Critère d'atteinte à la vie privée

Le critère de l'atteinte à la vie privée a d'abord été élaboré pour les besoins de la *Politique sur la protection des renseignements personnels* du Conseil du Trésor. Selon ce critère, les institutions devraient tenir compte de trois facteurs de risque interreliés :

- la nature délicate des renseignements personnels, y compris les détails de ces renseignements ou la sensibilité de ceux-ci (p. ex. des renseignements de nature médicale), de même que le contexte dans lequel ils ont été obtenus;
- les attentes des individus à l'égard des renseignements personnels qui les concernent (y compris l'assurance que les renseignements les concernant ne seront communiqués qu'en cas de nécessité d'accès);
- la possibilité d'un préjudice si les renseignements personnels font l'objet d'une divulgation illégale ou d'une utilisation abusive, y compris le vol possible de l'identité ou leur accès par des gouvernements étrangers.

Les considérations liées à la vie privée mentionnées plus haut permettront aux institutions de cerner les risques potentiels en regard du mode d'exécution du programme proposé et qui doivent être atténués dans le cadre du processus d'adjudication des marchés. Pour obtenir des conseils supplémentaires sur cette question, veuillez vous reporter à l'annexe A, Critère d'atteinte à la vie privée.

1.3 *Politique d'évaluation des facteurs relatifs à la vie privée*

Les institutions assujetties à la *Loi sur la protection des renseignements personnels* sont également visées par la *Politique d'évaluation des facteurs relatifs à la vie privée* (EFVP) : http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_f.asp.

Aux termes de la Politique d'EFVP, les institutions doivent songer à effectuer une EFVP si un nouveau programme ou service suppose la collecte, l'utilisation ou la divulgation de renseignements personnels, ou si un changement fondamental est apporté à un programme ou service existant. Ce serait notamment le cas dans le cadre de la passation d'un marché pour un programme ou un service avec le secteur privé. L'administrateur général de l'institution a pour tâche de déterminer si des initiatives justifient le recours à une EFVP. Dans certains cas, si les institutions ne disposent pas encore des renseignements précis requis pour effectuer une évaluation exhaustive ou lorsqu'un changement au programme ou au service (ou au marché) n'est pas jugé suffisamment important pour justifier la tenue d'une EFVP complète, une EFVP préliminaire peut se révéler une option de choix.

Étape 2.0 : Évaluation des risques d'atteinte à la vie privée comparés à d'autres considérations

Selon les circonstances au sein de l'institution, une série d'autres facteurs pourraient être pris en compte à ce stade-ci. Les risques d'atteinte à la vie privée relevés et évalués à l'Étape 1.0 — notamment, la nature délicate des renseignements et le contrôle exercé par le fournisseur de service sur l'information — devront être comparés aux facteurs suivants avant qu'une décision finale soit prise.

2.1 Lois d'États étrangers

Dans le cadre des activités qu'elles mènent dans des circonstances qui permettent l'application de lois étrangères (p. ex. marchés de sous-traitance, changement de propriété), les institutions devraient se demander si l'économie et le contexte politique du pays étranger ainsi que ses lois ou son système de droit risquent d'avoir des répercussions néfastes sur les marchés ou les activités visées par les marchés. Dans certains cas, les différences qui existent dans un environnement étranger peuvent soulever des questions touchant les risques d'atteinte à la vie privée.

Les lois d'un pays étranger en matière de perquisition et de saisie, par exemple, peuvent exiger des sociétés qui sont établies dans les limites de son territoire ou qui sont liées à des sociétés sur ce territoire, qu'elles communiquent les renseignements qui relèvent d'elles ou auxquels elles peuvent avoir accès, y compris les renseignements détenus aux termes d'un marché ou d'une entente. Les scénarios qui suivent sont des exemples de la manière dont de telles lois pourraient éventuellement s'appliquer si le Canada en venait à passer un marché avec les sociétés suivantes :

Scénario A : Marché passé avec une société qui mène ses activités au Canada et nulle part à l'étranger

La société qui limite ses activités au Canada et qui maintient des renseignements personnels au Canada seulement est assujettie aux lois canadiennes. Il existe un risque d'accès indirect si, aux termes du marché, la société canadienne (l'entrepreneur) a le pouvoir de conclure des contrats en sous-traitance et donc de conclure des contrats de sous-traitance avec des sociétés qui sont établies à l'étranger ou qui ont des liens avec des organisations commerciales étrangères.

Scénario B : Marché passé avec une société qui mène ses activités au Canada et à l'étranger

Une ordonnance rendue conformément à une loi étrangère pourrait s'appliquer indirectement. Une société établie à l'étranger pourrait être tenue de communiquer des renseignements

personnels auxquels elle a accès ou dont elle peut obtenir l'accès, y compris des renseignements détenus par sa société canadienne affiliée. Selon la nature des lois étrangères et la facilité d'accès aux dossiers par la société étrangère, la société canadienne affiliée peut ne pas être mise au courant de l'existence d'une ordonnance exigeant la production de renseignements.

Scénario C : Marché conclu avec une société qui mène ses activités à l'étranger

Les organisations commerciales qui mènent leurs activités à l'étranger et qui détiennent des renseignements personnels sur des Canadiens et des Canadiennes dans ce pays doivent se conformer aux lois du pays étranger. La société établie à l'étranger pourrait être tenue de produire des renseignements personnels auxquels elle a accès ou peut obtenir accès du fait d'un marché ou d'une entente conclus avec une institution du gouvernement du Canada.

Les exemples qui précèdent pourraient s'appliquer à tout État étranger dont certaines lois peuvent contraindre des sociétés qui mènent leurs activités dans les limites de leur territoire à produire des renseignements. Il convient de préciser qu'il serait beaucoup plus difficile pour la plupart des gouvernements étrangers de cibler certains renseignements personnels pouvant être détenus par une société aux termes d'un marché conclu avec le gouvernement canadien que de les demander dans le cadre d'une entente bilatérale existante. Lorsqu'elle s'est penchée sur l'utilisation possible de la *USA PATRIOT Act* par les organismes américains d'exécution de la loi pour obtenir des renseignements sur les Canadiens et les Canadiennes, la commissaire à la protection de la vie privée du Canada a déclaré ce qui suit :

> …les organismes du gouvernement américain peuvent s'en remettre à d'autres procédures officielles pour obtenir des renseignements concernant les Canadiens et les Canadiennes qui seraient en la possession du gouvernement ou du secteur privé au Canada. Des accords de longue date en matière d'échange de renseignements, conclus entre les organismes de sécurité et d'application de la loi des deux pays, ainsi que le mécanisme de l'entraide juridique, sont les moyens les plus susceptibles d'être employés pour obtenir l'accès à des renseignements détenus au Canada.

Il y a lieu de noter que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ou des lois provinciales essentiellement similaires (adoptées en Colombie-Britannique, en Alberta et au Québec) régissent les pratiques en matière de protection des renseignements personnels des organisations commerciales qui mènent leurs activités au Canada. Aucune de ces lois n'empêche la passation de marchés mettant en cause des renseignements personnels, mais elles exigent des entrepreneurs situés au Canada d'inclure des clauses de protection des renseignements personnels dans tout marché de sous-traitance.

2.2 Analyse de l’application possible d’accords commerciaux internationaux

Avant de décider s’il convient de donner ou non à la sous-traitance un marché mettant en cause le traitement de renseignements personnels, les institutions doivent déterminer si des accords commerciaux internationaux s’appliquent à l’acquisition proposée (l’annexe C donne un bref aperçu des accords commerciaux clés). Si de tels accords s’appliquent à l’acquisition, le gouvernement du Canada doit faire en sorte que ses obligations en matière de commerce sont respectées et que les demandes de propositions sont conformes à ces obligations.

Dans la pratique, cela peut signifier que, dans certains cas, les institutions fédérales ne pourraient exiger que des renseignements demeurent au Canada. L’applicabilité d’accords commerciaux internationaux est par conséquent un facteur important et peut avoir une certaine influence dans les décisions de lancer un mode donné d’acquisition ou d’étudier des solutions de rechange.

Les représentants du gouvernement devraient consulter leurs conseillers juridiques pour déterminer l’application ou non des accords commerciaux internationaux.

Étapes 3 à 5, Conclusion de marchés

Étape 3.0 : Intégration de la protection des renseignements personnels aux marchés

S’il est décidé de conclure un marché, il reviendra aux institutions de garantir que des clauses adéquates de protection des renseignements personnels figurent dans les documents contractuels, tel qu’il est précisé aux étapes 3.0 et 4.0. Les institutions fédérales peuvent recourir à toute une gamme d’outils dans le cadre du processus d’acquisition pour s’assurer que chaque marché adjugé soit assorti d’une protection suffisante des renseignements personnels. Les critères d’évaluation, l’ET ainsi que les autres dispositions de la DP figurent parmi les moyens les plus efficaces de garantir une protection initiale des renseignements personnels. La conception initiale et la rédaction de ces documents d’acquisition devraient permettre d’établir les stratégies générales de protection des renseignements personnels et d’élaborer les dispositions clés qui garantiront une protection suffisante des renseignements personnels par l’entremise des marchés. Toutes les solutions efficaces relatives à la passation de marchés doivent intégrer les coûts de la mise en œuvre.

3.1 Demande de propositions / Énoncé des travaux

L’une des considérations liées au risque les plus fondamentales au moment d’établir des marchés qui donnent lieu au traitement de renseignements personnels consiste à faire en sorte que les renseignements seront recueillis, utilisés, conservés et divulgués aux seules fins précisées dans le marché et qu’ils ne seront accessibles qu’à des individus autorisés à les utiliser à ces fins (pour des raisons de nécessité d’accès). Selon l’entente, il pourrait être nécessaire de prévoir des

garanties contractuelles supplémentaires, surtout si les renseignements sont consultés ou détenus par un entrepreneur établi à l'étranger ou un entrepreneur qui a des liens avec un État étranger.

Les risques d'atteinte à la vie privée doivent être pris en considération dès cette première étape du processus d'acquisition. Il est essentiel que tous les soumissionnaires ou entrepreneurs éventuels connaissent toutes les exigences particulières qui sont liées à l'exécution du contrat à l'étape de la DP, étant donné que ces exigences auront une incidence sur les coûts. La décision d'inclure des dispositions expresses dans la DP ou l'ET devrait être fondée sur les considérations liées au risque dans leur ensemble, y compris les répercussions possibles sur la vie privée et le besoin d'inclure des clauses contractuelles pour atténuer les risques.

Les restrictions qui touchent l'accès à des renseignements personnels, leur utilisation et leur entreposage doivent se trouver dans les documents d'acquisition, dont la DP ou l'ET.

À l'étape de la DP ou de l'ET

Si, d'après les résultats du critère de l'atteinte à la vie privée et d'autres facteurs de risque, il est déterminé que le niveau de risque est suffisamment élevé, les institutions peuvent se poser les questions suivantes :

- Dans les cas où des accords commerciaux internationaux ne s'appliquent **pas**, faut-il que les travaux soient effectués et que les données soient conservées au Canada ou dans des installations du gouvernement du Canada (p. ex. dans des ambassades étrangères, des installations militaires à l'étranger)?
- L'entrepreneur est-il tenu de conserver les renseignements ou les bases de données gouvernementaux séparément des autres renseignements?
- L'entrepreneur doit-il prévoir un plan de sécurité et de gestion des renseignements (c.-à-d. une documentation qui précise la manière exacte dont les renseignements seront traités tout au long de leur cycle de vie et la manière dont on prévoit en assurer la sécurité)?
- Faut-il obtenir l'assurance que le soumissionnaire peut satisfaire aux exigences du marché ou démontrer certaines qualifications ou attestations avant la mise en marche du processus de DP (c.-à-d. les soumissionnaires sont-ils présélectionnés compte tenu de leur capacité de gérer des renseignements personnels)?
- L'entrepreneur devra-t-il fournir ou utiliser des systèmes, de l'équipement ou des documents particuliers aux fins de la protection des renseignements personnels et de la sécurité des renseignements gouvernementaux?
- À quoi l'entrepreneur aura-t-il accès (p. ex. des installations, des systèmes, des documents, des bases de données)?
- L'entrepreneur sera-t-il tenu de fournir et de tenir à jour une liste du personnel qui sera autorisé à avoir accès aux renseignements ou bases de données du gouvernement aux fins de l'exécution du contrat?
- Les renseignements relèveront-ils du gouvernement du Canada, et les responsabilités aux fins du traitement (c.-à-d. la collecte, l'utilisation, l'entreposage, l'élimination et la divulgation) des renseignements seront-elles précisées?
- L'entrepreneur devra-t-il maintenir des pistes de vérification et faire rapport de tous les accès et de toutes les divulgations de renseignements ou de bases de données du gouvernement?
- Sera-t-il nécessaire de fournir une preuve de destruction autorisée par le gouvernement?

Remarque : Tous les marchés de services comportent un ET ou une description des exigences, qui énonce clairement les travaux à exécuter, les objectifs à atteindre et l'échéancier à respecter. L'ET fera partie de la DP et du marché.

Si le risque d'atteinte à la vie privée est jugé élevé, les institutions fédérales peuvent songer à évaluer spécifiquement les stratégies des soumissionnaires en matière de protection des renseignements personnels. Dans les cas où les soumissionnaires sont tenus de déposer un plan de gestion des renseignements personnels dans le cadre du marché, les institutions fédérales peuvent demander que ces plans soient inclus en réponse à la DP dans la soumission à des fins d'évaluation dans le cadre du processus d'acquisition. L'institution fédérale pourra ensuite évaluer ces plans et leur accorder le poids qu'il convient dans les critères d'évaluation.

Étape 4.0 : Facteurs précis à prendre en considération concernant les DP et marchés mettant en cause des renseignements personnels

Note importante : Le *Guide des clauses et conditions uniformisées d'achat* (CCUA), publié par TPSGC, pourrait offrir une protection adéquate dans plusieurs cas où des dispositions contractuelles liées à des renseignements personnels sont adoptées. En conséquence, il est essentiel que les fonctionnaires consultent leurs collègues des services juridiques et du domaine de la vie privée concernant l'application d'un libellé contractuel additionnel ou révisé, en fonction de chaque cas.

Suivent certaines considérations liées à la protection des renseignements personnels qui seront utiles pour atténuer les risques d'une éventuelle divulgation non autorisée à des gouvernements étrangers et pour garantir un examen et une surveillance suffisants des marchés qui supposent le traitement de renseignements personnels. Dans certains cas, ces considérations liées aux clauses proposées peuvent déjà constituer des exigences en vertu d'autres politiques, directives ou lignes directrices sur la passation des marchés et la sécurité qui visent actuellement la plupart des institutions assujetties à la *Loi sur la protection des renseignements personnels*. Le fait d'inclure les suggestions ci-après n'a pas pour but de restreindre les exigences s'appliquant aux clauses sur la protection des renseignements personnels, mais vise à rappeler l'importance toute particulière des questions suivantes et la nécessité de les prendre en considération dans les DP et les clauses contractuelles.

4.1 Établir le contrôle

Il est important que la nature de la relation qui existe entre l'entrepreneur et l'institution fédérale ainsi que leurs rôles et obligations respectifs soient définis clairement dans le cadre des documents de marchés. Une institution fédérale ne peut pas recueillir de renseignements

personnels à moins que ces derniers soit liés directement à l'activité ou au programme de fonctionnement de l'institution.

L'institution doit examiner la portée de l'autorité juridique qu'elle détient dans le cadre d'un programme ou d'une activité donnée. Une fois que cette autorité a été déterminée, les marchés liés à la gestion des programmes et des services du gouvernement devraient comprendre des dispositions afin de veiller à ce que l'institution fédérale garde le contrôle sur les renseignements personnels ou tout autre document transférés à l'entrepreneur et, au besoin, sur les renseignements recueillis, créés, obtenus ou conservés par l'entrepreneur aux termes du marché. Cette façon de définir le contrôle est nécessaire afin de permettre à l'institution contractante de respecter ses exigences réglementaires aux termes de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*. Cela revêt une importance particulière dans les cas où des renseignements de nature très délicate doivent être entreposés ou traités dans un pays étranger par une société mère basée à l'étranger, une filiale ou un tiers, tel qu'un sous-traitant ou un mandataire. Les institutions fédérales peuvent établir le contrôle en définissant les droits de propriété de l'institution sur les documents dans le marché, y compris le droit de l'institution de les obtenir sur demande.

De plus, le gouvernement a le devoir d'inclure toute autre disposition précise liée au respect de la vie privée dans les ententes contractuelles afin de veiller à ce que la sous-traitance de programmes et de services du gouvernement n'occasionne pas une réduction de la protection des renseignements personnels. Il peut y avoir des cas où les institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels* entreprennent des ententes contractuelles avec des organisations du secteur privé qui sont assujetties à d'autres exigences législatives en matière de respect de la vie privée au niveau provincial ou fédéral, telle la LPRPDE. Les institutions fédérales confrontées à ce genre de scénario devraient, en consultation avec les responsables juridiques et de la vie privée de leur institution, effectuer une analyse législative et stratégique approfondie des exigences des deux lois et élaborer des clauses contractuelles qui respectent les principes ou les normes les plus rigoureux des deux lois en matière de respect de la vie privée.

4.2 Recours à la confidentialité à des fins liées au marché

Les institutions doivent garantir que des dispositions sont en place pour limiter l'accès (y compris l'accès non autorisé) ou la capacité d'obtenir l'accès à des renseignements personnels de nature délicate à des fins qui ne sont pas liées au marché, y compris toute divulgation ou tout accès par une société mère établie à l'étranger, d'autres filiales ou des tiers, comme des sous-traitants ou des mandataires qui ne sont pas directement nommés dans l'entente ou le marché principal. Lorsque des renseignements personnels de nature délicate sont consultés, les

institutions fédérales devraient soit ajouter une exigence selon laquelle l'entrepreneur doit identifier et désigner explicitement tous les employés de l'entrepreneur qui auront accès aux données personnelles ou exclusives ou indiquer les postes des employés qui pourront y accéder. Cela permettrait d'identifier tous les cas d'accès non autorisé, surtout lorsque des pistes de vérification sont utilisées.

4.3 Vérifications requises ou permises (y compris la vérification de retraçage et des pistes de vérification)

En plus des dispositions uniformisées relatives à la vérification, lorsque des renseignements personnels de nature délicate sont consultés, les institutions devraient envisager d'ajouter une exigence qui stipule que le fournisseur ou le fournisseur de services doit tenir à jour des renseignements précis pour permettre la tenue de vérifications d'information. Ainsi, les vérifications de la sécurité et de la vie privée nécessiteront le maintien, par l'entrepreneur, d'une certaine forme de piste de vérification (électronique ou imprimée) pour démontrer que quiconque a eu accès à des renseignements détenait l'autorisation requise.

4.4 Séparation des renseignements

L'autorité contractante devrait tenir compte de la possibilité d'inclure des dispositions destinées à garantir la mise en place de mécanismes exigeant que tous les renseignements personnels de nature délicate divulgués à un entrepreneur par le gouvernement du Canada ou recueillis ou créés conformément à un marché ou à une entente conclue avec le gouvernement du Canada soient conservés séparément des autres dossiers ou des données détenues par la société. Les institutions devraient définir la nature de la séparation, ce qui pourrait inclure une séparation matérielle des données (p. ex. données détenues sur bande magnétique), une séparation logique des données (p. ex. dossier ou identificateur d'utilisateur), ou une séparation matérielle combinée à une séparation logique.

Remarque : Les renvois, dans le contrat, à la séparation des renseignements, doivent correspondre aux modalités établies dans la DP et l'ET, ainsi que dans le Guide des CCUA de TPSGC.

4.5 Conditions relatives aux divulgations non liées au marché

L'institution fédérale devrait songer à imposer à l'entrepreneur des exigences précises auxquelles il devra satisfaire, et à obtenir l'autorisation préalable à l'égard de toutes les divulgations de renseignements personnels de nature délicate non liées au marché (voir 4.2, « Recours à la confidentialité à des fins liées au marché »).

4.6 Inspection

Dans les cas où une institution fédérale établit le contrôle (voir 4.1, « Établir le contrôle »), elle peut aussi souhaiter mettre en place de vastes pouvoirs d'inspection des locaux de l'entrepreneur lorsque des renseignements personnels de nature délicate sont en cause. Les marchés antérieurs se rapportant à l'élimination de dossiers ont révélé combien il est important d'inspecter les installations et les travaux qui sont exécutés aux termes d'un marché. Il est important que les institutions fédérales s'assurent (pas nécessairement au moyen d'une vérification) que les travaux sont exécutés de la manière prévue dans l'ET et qu'ils respectent les conditions énoncées dans la DP. Ainsi, si la DP et l'ET contiennent des conditions particulières (techniques ou autres), les institutions peuvent souhaiter d'accorder au Canada le droit d'inspecter les travaux pour s'assurer que le fournisseur de services effectue les travaux conformément aux spécifications énoncées dans la DP, l'ET et le marché.

4.7 Avis de manquement

Étant donné les obligations du gouvernement de protéger les renseignements personnels sous son autorité, la responsabilité d'en assurer le caractère confidentiel et la reddition de comptes en cas de manquements devrait être étendue à tout entrepreneur qui traite des renseignements personnels pour le compte d'une institution. Si un entrepreneur est réputé avoir divulgué des renseignements personnels, il devrait être disposé à assumer la responsabilité à l'égard de la divulgation illégale de renseignements personnels, des coûts associés à l'avis qui doit être donné aux individus dont les renseignements ont été divulgués et de la possibilité que le marché soit résilié. Les institutions devraient préciser que, immédiatement après que l'entrepreneur apprend que des renseignements confidentiels ont été divulgués, l'entrepreneur doit informer sur-le-champ l'institution fédérale de ce manquement.

4.8 Avis de sous-traitance et obligations du sous-traitant

Le cas échéant, l'institution fédérale devrait se pencher soigneusement sur la question de savoir si l'entrepreneur doit être autorisé ou non à donner à la sous-traitance les services énoncés aux termes du marché. Si la sous-traitance est permise, l'entrepreneur devra garantir que toute entente de sous-traitance qu'il conclura devra exiger du sous-traitant qu'il se conforme aux dispositions relatives à la protection des renseignements personnels énoncées dans le marché entre l'entrepreneur et l'institution fédérale. L'institution fédérale peut également envisager, en fonction de chaque cas, d'inclure, s'il y a lieu, une disposition selon laquelle l'entrepreneur doit faire approuver par écrit les dispositions sur la sous-traitance par l'institution avant la signature de l'entente de sous-traitance.

Étape 5.0 : Critères d'évaluation et exemple de DP et de libellé des marchés

L'évaluation complète des marchés fédéraux, entamée par le Secrétariat du Conseil du Trésor du Canada, a révélé que la majorité des marchés identifiés par les institutions comme présentant des risques possibles d'atteinte à la vie privée comportaient le traitement et la gestion de données. Pour aider ces institutions, les exemples suivants de clauses de DP se rapportent expressément à la mise sur pied de bases de données ainsi qu'à l'emplacement et au traitement de données, et ils sont destinés à ***s'appliquer seulement dans des circonstances*** où, selon l'évaluation, le risque d'atteinte à la vie privée est très élevé.

Définition : Une base de données consiste en une collecte organisée de données qui peuvent être consultées rapidement. Les bases de données se composent de champs, de dossiers et de tableaux. Un champ s'entend d'un seul élément d'information (p. ex. un numéro de téléphone); un dossier se compose d'une série de champs (p. ex. le nom, l'âge, le numéro de téléphone); et un tableau comporte une série de dossiers. Pour consulter l'information se trouvant dans une base de données, il faut disposer d'un système de gestion de base de données (SGBD). Un SGBD consiste en une série de programmes qui permettent à l'utilisateur de saisir, d'organiser et de choisir des données dans la base de données.

La création d'une base de données s'entend de l'établissement de la structure de la base de données, mais pas de son contenu en données. Il faut d'abord créer une base de données, puis y verser des données et, finalement, traiter les données se trouvant dans la base de données.

Note importante : Dans les situations où l'on considère que les renseignements personnels sont de nature très délicate, les clauses types suivantes peuvent être utilisées, le cas échéant, pour régler le risque de divulgation potentielle à des gouvernements étrangers. L'utilisation de ces clauses devrait se limiter aux situations où, en consultation avec les représentants des services juridiques et de la vie privée et, compte tenu des critères d'atteinte à la vie privée, il est déterminé qu'il existe un niveau élevé de risque d'atteinte à la vie privée (p. ex. renseignements sur la santé, sur le revenu ou de nature financière). Avant de mettre en application les clauses indiquées ci-après, les institutions doivent consulter les représentants des services juridiques et de la vie privée. Les fonctionnaires doivent, eux aussi, consulter les services juridiques avant de modifier ou d'adapter de telles clauses de manière qu'elles répondent à certains besoins d'un marché donné ou relativement à d'autres modes d'exécution de programmes. Lorsque les institutions sont assujetties aux exigences de la PGS, l'agent de sécurité ministériel peut prodiguer des conseils sur les procédures de sécurité imposées par la PGS.

Les exemples de clauses figurant ci-dessous devraient paraître tant dans la DP que dans l'entente contractuelle.

Exemple de clause s'appliquant à une DP et à une entente contractuelle

Le Canada doit faire en sorte que les lois, les règlements et les politiques du Canada en ce qui concerne la protection des renseignements personnels soient respectés. Le cas échéant, les institutions fédérales doivent garantir la protection des renseignements personnels conformément à la *Loi sur la protection des renseignements personnels*, L.R. (1985), ch. P-21, à la *Loi sur la protection des renseignements personnels et les documents électroniques*, (2000), ch. 5, et aux politiques fédérales sur la protection des renseignements personnels. Par conséquent, afin de s'acquitter de cette obligation dans les cas où le marché prévoit le traitement de renseignements personnels, le Canada demande ce qui suit à l'entrepreneur :

Base de données et traitement de données

Lorsque aucune obligation en matière de commerce internationale **ne s'applique** :	Lorsque des obligations en matière de commerce internationale **s'appliquent** :
Création d'une base de données	
1. La base de données doit être située au Canada et être accessible au Canada seulement.	1. La base de données doit être située et ne doit être accessible que dans les pays dont les lois n'ont pas priorité sur la *Loi sur la protection des renseignements personnels*, L.R. (1985), ch. P-21, la *Loi sur la protection des renseignements personnels et les documents électroniques*, (2000), ch. 5, ou les politiques du Conseil du Trésor en matière de protection des renseignements personnels et n'entrent pas en conflit avec ces lois, ni n'en empêchent l'application, soit expressément, soit par application subséquente.
2. La base de données doit être matériellement indépendante de toutes les autres bases de données, directement ou indirectement, qui sont situées à l'étranger.	2. La base de données doit être matériellement indépendante de toutes les autres bases de données, directement ou indirectement, qui sont situées dans des pays dont les lois ont priorité sur la *Loi sur la protection des renseignements personnels*, L.R. (1985), ch. P-21, la *Loi sur la protection des renseignements personnels et les documents électroniques*, (2000), ch. 5, ou les politiques du Conseil du Trésor en matière de protection des renseignements personnels et entrent en conflit avec ces lois ou en empêchent l'application, soit expressément, soit par application subséquente.

Traitement des données

1. Tous les aspects du traitement des données doivent être assurés et ne peuvent être accessibles qu'au Canada.	1. Tous les aspects du traitement des données doivent être assurés et ne peuvent être accessibles que dans les pays dont les lois n'ont pas priorité sur la *Loi sur la protection des renseignements personnels*, L.R. (1985), ch. P-21, la *Loi sur la protection des renseignements personnels et les documents électroniques*, (2000), ch. 5, ou les politiques du Conseil du Trésor en matière de protection des renseignements personnels et n'entrent pas en conflit avec ces lois, ni n'en empêchent l'application, soit expressément, soit par application subséquente.

Attestation du soumissionnaire, énonçant ce qui suit :

Le soumissionnaire atteste par les présentes qu'il a passé en revue les exigences de la présente DP, les clauses du marché qui sera attribué et, plus particulièrement, les exigences relatives à la protection des renseignements personnels. Le soumissionnaire atteste également qu'il se conformera à ces modalités et fera en sorte que les renseignements personnels qui sont gérés, consultés, recueillis, utilisés, divulgués, conservés, reçus, créés ou éliminés pour satisfaire aux exigences du marché, seront traités conformément à la *Loi sur la protection des renseignements personnels*, L.R. (1985), ch. P-21, à la *Loi sur la protection des renseignements personnels et les documents électroniques*, (2000), ch. 5, ainsi qu'aux politiques du Conseil du Trésor en matière de protection des renseignements personnels.

La présente attestation demeurera véridique et exacte pendant toute la durée du marché qui sera attribué et a le même effet que si elle était faite continuellement pendant toute la durée du marché qui sera attribué.

En outre, le soumissionnaire reconnaît que le ministre peut se fonder sur la présente attestation pour attribuer le marché. Si le soumissionnaire omet de se conformer à la présente attestation ou qu'une vérification ou inspection par le ministre révèle que le soumissionnaire a fait de fausses déclarations, le ministre a le droit de traiter tout marché attribué par suite de la présente soumission comme étant en défaut, et de le résilier conformément aux dispositions du contrat relatives au défaut.

Remarque : Il se peut que, dans certaines circonstances où le risque d'atteinte à la vie privée est élevé, il convienne que les institutions fédérales rendent l'accès par l'entrepreneur à des renseignements personnels conditionnel au maintien de la validité de l'attestation. Donc, si l'entrepreneur fait face à une ordonnance l'obligeant à produire des renseignements personnels, l'attestation ne sera plus valide et tout accès subséquent aux renseignements personnels ou toute divulgation subséquente de ceux-ci constituera un manquement au marché et, dans certains cas, un manquement aux lois canadiennes liées à la sécurité des renseignements et à la sauvegarde de la vie privée.

Personnes-ressources pour obtenir de plus amples renseignements

Les questions portant sur l'application de la *Politique sur la protection des renseignements personnels* et de la *Politique sur les marchés* du Conseil du Trésor devraient être adressées au centre de responsabilités concerné des institutions.

Si vous avez des questions concernant les directives formulées dans le présent document, n'hésitez pas à communiquer avec la Division des politiques de l'information, de la protection des renseignements personnels et de la sécurité, Direction de la politique sur les acquisitions et la gestion des projets du Secrétariat du Conseil du Trésor du Canada, au (613) 941-7176.

Références

Politique sur la protection des renseignements personnels
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/siglist_f.asp

Politique d'évaluation des facteurs relatifs à la vie privée
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_f.asp

Politique sur les marchés
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/Contracting/contractingpol_f.asp

Politique du gouvernement sur la sécurité
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_f.asp

Politique sur la gestion des risques
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/riskmanagpol_f.asp

Cadre de gestion intégrée du risque
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_f.asp

Guide des clauses et conditions uniformisées d'achat
http://sacc.pwgsc.gc.ca/sacc/contents-f.jsp

Manuel de la sécurité industrielle
http://www.ciisd.gc.ca/text/ISM/ch1-f.asp

Annexe A : Critère d'atteinte à la vie privée

Le critère d'atteinte à la vie privée sert de référence pour déterminer si un marché dans le cadre duquel des renseignements personnels seraient traités pourrait entraîner un préjudice ou un dommage à l'individu. Il y a trois principaux facteurs qui doivent être pris en considération dans le contexte du critère d'atteinte à la vie privée : la nature délicate des renseignements, les attentes des individus, ainsi que la probabilité et la gravité du préjudice.

1) La nature délicate des renseignements

Déterminer de quel type de renseignements personnels il est question dans le marché.

- Dans quelle mesure les renseignements personnels doivent-ils être détaillés (s'agit-il de données générales comme le nom et l'adresse ou de renseignements personnels très détaillés comprenant des renseignements longitudinaux)?
- Quelle est la gravité d'un manquement (déterminée par des facteurs tels le nombre d'individus pour lesquels on détient des renseignements personnels dans la base de données et la quantité de renseignements personnels recueillis)?
- S'agit-il de renseignements de nature personnelle extrêmement délicate (p. ex. des renseignements de nature médicale et financière) ou semblent-ils être assez anodins (p. ex. des renseignements généraux)?
- Quel est le but des travaux (c.-à-d. à des fins de statistiques, d'exécution du programme, d'application réglementaire ou à des fins d'application des dispositions pénales)?
- Quel est le contexte qui entoure les renseignements? (Le nom et l'adresse d'un individu peuvent être des renseignements anodins ou de nature extrêmement délicate selon le contexte; ainsi, le nom et l'adresse des individus qui participent à un programme d'emploi des jeunes sont de nature moins délicate qu'une liste semblable qui contient le nom et l'adresse des victimes de contamination de l'hépatite C et du VIH qui touchent une indemnisation.)
- Quel est le contrôle qu'exercera le fournisseur de services sur les renseignements?

Du point de vue de la protection des renseignements personnels, il faut accorder une attention particulière à la décision liée à la passation d'un marché supposant le traitement de renseignements de nature extrêmement délicate. Si les renseignements sont très détaillés et qu'ils sont de nature délicate et extrêmement personnelle, les institutions se doivent d'examiner des solutions de rechange qui permettent d'accroître leur contrôle direct sur les renseignements dans la mesure du possible. Sinon, les institutions doivent songer à adopter une norme très élevée de sécurité et de confidentialité qui pourrait bien dépasser largement les exigences minimales dans les cas où le traitement de tels renseignements est donné à contrat. Les Canadiens et les Canadiennes pourront ainsi être plus à l'aise lorsqu'il s'agit de leurs renseignements personnels.

Remarque : Le critère d'atteinte à la vie privée proposé ci-dessus est une adaptation du critère d'atteinte à la vie privé d'intérêt public qui est énoncé au paragraphe 6.13 du chapitre 2-4 de la *Politique sur la protection des renseignements personnels* du Conseil du Trésor.

2) Les attentes des individus

Déterminer ou établir les attentes des individus en ce qui concerne leurs renseignements personnels. **Les conditions qui régissent la collecte de renseignements personnels constituent habituellement le meilleur moyen de déterminer les attentes des individus.**

Dans les cas où des renseignements personnels ont déjà été recueillis par l'institution fédérale, vérifier quelles conditions ont été établies au moment où les renseignements ont été recueillis pour la première fois auprès de l'individu :

- Y a-t-il eu engagement ou promesse de ne pas communiquer les renseignements à une autre partie ou institution?
- Y a-t-il eu une mise en garde prévoyant que les renseignements pourraient être divulgués d'une manière qui est compatible avec l'objet premier de la collecte des renseignements?
- Les renseignements ont-ils été compilés ou obtenus aux termes de garanties qui font obstacle à une partie ou à la totalité des types de divulgation?
- Les renseignements ont-ils été fournis spontanément, librement ou volontairement, sans vraiment s'attendre à ce qu'ils soient tenus complètement confidentiels?

Si des renseignements personnels doivent être recueillis par l'institution fédérale de la part de l'entrepreneur, ou si celle-ci a pu exercer un certain contrôle sur les dossiers de l'entrepreneur, veillez à établir les conditions dont est assortie cette collecte ainsi que l'utilisation et la divulgation prévues des renseignements personnels, conformément aux pratiques équitables en matière de gestion des renseignements personnels énoncées dans la *Loi sur la protection des renseignements personnels* et dans son règlement d'application, ainsi que dans la *Politique sur la protection des renseignements personnels* du Conseil du Trésor. Par exemple :

- L'institution expliquera-t-elle clairement à l'entrepreneur ses obligations relativement à la collecte de renseignements personnels pour le compte du gouvernement du Canada?
- L'institution fera-t-elle en sorte que l'entrepreneur informe les individus de l'objet de la collecte et qu'il obtienne le consentement (dans les cas applicables) aux fins de la collecte, de l'utilisation et de la divulgation? Cela signifie aussi faire en sorte que les individus soient informés de tout pouvoir de nature législative touchant la collecte, de leur droit de refuser de fournir une partie ou la totalité des renseignements demandés et de toute conséquence possible de ce refus, et de leur droit d'accès et de correction.

- L’institution fera-t-elle en sorte que l’entrepreneur informe les individus des autres utilisations et divulgations possibles des renseignements?
- Un individu serait-il à l’aise avec l’idée que ses renseignements personnels pourraient être consultés par une tierce partie aux termes d’un marché?
- L’individu s’attendrait-il à ce qu’un tiers prenne part au traitement de tels renseignements personnels?
- Quel est le niveau de confidentialité et de sécurité auquel l’individu pourrait s’attendre?

3) Probabilité et gravité du préjudice

Déterminer la probabilité de préjudice si les renseignements personnels sont divulgués illégalement ou si une infraction à la sécurité ou une divulgation de renseignements confidentiels se produit. Le préjudice s’entend de tout dommage ou toute atteinte ayant des effets négatifs directs, par exemple, sur la carrière, la réputation, la situation financière, la sécurité, la santé ou le bien-être d’un individu. Les facteurs suivants permettront de déterminer la mesure du préjudice probable.

- Le marché comprendrait-il des renseignements personnels concernant quelques individus ou de nombreux individus (p. ex. le marché mettra-t-il en cause un ou deux individus ou comprendra-t-il des renseignements personnels qui concernent des centaines ou des milliers d’individus)?
- Si les renseignements sont jugés de nature délicate, peut-on supposer que toute divulgation engendre une probabilité de causer un préjudice mesurable (p. ex. usurpation d’identité, fraude, trouble émotif ou effets négatifs sur la carrière, la réputation, la situation financière, la sécurité, la santé ou le bien-être d’un individu)?
- Existe-t-il un risque en ce qui concerne l’application possible de lois étrangères (c.-à-d. la possibilité d’une divulgation à un gouvernement étranger à des fins non liées au marché)?
- Quelle pourrait être la gravité du préjudice possible?

Le tableau qui suit permettra de déterminer les risques qui sont liés à l’application possible de lois étrangères à la suite d’un marché qui suppose le traitement de renseignements personnels.

Risque inexistant	Les bases de données sont conservées et traitées dans les locaux du gouvernement du Canada uniquement ou les bases de données sont situées ou conservées à l'extérieur des locaux et le traitement est effectué par une société canadienne qui mène ses activités au Canada seulement. L'entreposage/l'archivage et l'élimination des dossiers sont effectués dans les locaux du gouvernement du Canada uniquement ou par une société canadienne qui exploite son entreprise au Canada.
Risque faible	Les bases de données sont situées ou conservées à l'extérieur des locaux du gouvernement du Canada et traitées par une société au Canada, et un sous-traitant étranger ou une société mère basée à l'étranger ou une filiale pourrait y avoir accès (avec une stratégie d'atténuation des risques en place). L'entreposage/l'archivage et l'élimination des dossiers sont effectués à l'extérieur des locaux du gouvernement du Canada par une société au Canada, et un sous-traitant étranger ou une société mère basée à l'étranger ou une filiale pourrait y avoir accès (avec une stratégie d'atténuation des risques en place).
Risque moyen	Les bases de données sont conservées et traitées par une société basée à l'étranger et sujette aux lois d'un gouvernement étranger (avec une stratégie d'atténuation des risques en place).
Risque élevé	Les bases de données sont conservées et traitées par une société établie à l'étranger et sujette aux lois d'un gouvernement étranger (sans qu'une stratégie d'atténuation des risques ne soit en place). L'entreposage/l'archivage et l'élimination des dossiers sont effectués par une société basée à l'étranger et sujette aux lois d'un gouvernement étranger.

Remarque : Les institutions pourraient souhaiter prendre en considération d'autres facteurs qui seraient propres à leurs situations. Pour cette raison, elles sont encouragées à élaborer des lignes directrices sur l'application du critère d'atteinte à la vie privée au sein de leur institution.

L'utilisation de **stratégies d'atténuation efficaces** par les institutions fédérales réduira le niveau de risques. Ces stratégies pourraient comprendre l'utilisation de solutions non technologiques, comme l'ajout des clauses de protection des renseignements personnels proposées dans le présent document ou la mise en œuvre de solutions technologiques, comme le chiffrement.

Annexe B : Liste de contrôle pour la protection des renseignements personnels

Le but de la liste de contrôle est d'assurer la prise en compte des exigences en matière de protection des renseignements personnels aux étapes préliminaires de la planification et de la mise en œuvre du processus de passation des marchés publics.

Remarques : Dans la présente liste de contrôle,

« **renseignements personnels** » désigne les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, conformément à l'article 3 de la *Loi sur la protection des renseignements personnels*;

« **document** » désigne tous éléments d'information, quels que soient leur forme et leur support, notamment correspondance, note, livre, plan, carte, dessin, diagramme, illustration ou graphique, photographie, film, microformule, enregistrement sonore, magnétoscopique ou informatisé, ou toute reproduction de ces éléments d'information, conformément à l'article 3 de la *Loi sur l'accès à l'information*.

OUI	NON	S.O.	DESCRIPTION
			Contrôle et responsabilité Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 1. Les types de documents ou renseignements personnels (énumérer les types de documents ou d'éléments d'information) visés par le marché : a) continueront de relever du gouvernement et d'être assujettis à la *Loi sur la protection des renseignements personnels* et à la *Loi sur l'accès à l'information*; b) demeureront la propriété exclusive de l'entrepreneur.
			2. L'entrepreneur doit charger un cadre de son organisation afin d'agir à titre de personne-ressource pour assurer la conformité aux exigences en matière de protection des renseignements personnels et de sécurité.
			3. L'entrepreneur doit fournir au gouvernement une liste à jour de tous les employés, sous-traitants ou mandataires participant à l'exécution du contrat qui auront accès à des renseignements personnels.
			4. Tous les employés, sous-traitants ou mandataires de l'entrepreneur qui pourraient avoir accès à des renseignements personnels dans le cadre de l'exécution du contrat doivent signer une entente de protection et de non-divulgation de l'information.
			5. L'entrepreneur est entièrement et uniquement responsable des actions des employés, sous-traitants et mandataires qui agissent pour son compte dans l'exécution de leurs fonctions aux termes du contrat.
			6. L'entrepreneur doit informer le gouvernement à l'avance de tout changement en ce qui a trait à la propriété d'une partie ou de la totalité de son entreprise.

OUI	NON	S.O.	DESCRIPTION
			Flux de données transfrontière Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 7. l'entrepreneur avisera immédiatement le gouvernement dans le cas de toute procédure liée a une faillite ou à une question d'insolvabilité ayant été portée contre ou par lui en vertu des lois qui s'appliquent en matière de faillite et d'insolvabilité ou de tout avis de recours des créanciers;
			8. qu'il est interdit à l'entrepreneur de communiquer et/ou de transférer des renseignements personnels (y compris les rubans d'archivage et les archives) à l'étranger, ou de permettre à des parties à l'extérieur du Canada d'y avoir accès, sans avoir obtenu préalablement le consentement écrit du gouvernement.
			9. qu'il est interdit à l'entrepreneur de communiquer et/ou de transférer des renseignements personnels à l'étranger, ou de permettre à des parties à l'extérieur du Canada d'y avoir accès, sans avoir obtenu préalablement le consentement écrit du gouvernement.
			Collecte de renseignements personnels Déterminer l'opportunité de mentionner dans l'entente contractuelle : 10. que la collecte de renseignements personnels doit se limiter aux renseignements dont l'entrepreneur a besoin pour se conformer aux modalités du contrat ou pour exercer ses droits en vertu de l'entente;
			11. que l'entrepreneur doit, sauf indication contraire par écrit, recueillir les renseignements personnels directement auprès de l'individu qu'ils concernent;
			12. qu'au moment de la collecte de renseignements personnels, l'entrepreneur doit informer l'individu auprès de qui il recueille ces renseignements : ▸ du but de la collecte;
			▸ de tout pouvoir législatif autorisant la collecte;
			▸ si la communication est volontaire ou si elle est requise par la loi;
			▸ des conséquences éventuelles du refus de communiquer les renseignements;
			▸ de son droit d'avoir accès à l'information et de la corriger;
			▸ du numéro du fichier de renseignements personnels qui contiendra les renseignements;
			13. que les employés de l'entrepreneur sont tenus de fournir leur identité aux individus auprès desquels ils recueillent des renseignements personnels et de donner à ces derniers un moyen de vérifier s'ils travaillent effectivement pour le compte du gouvernement et sont autorisés à recueillir les renseignements.
			Exactitude des renseignements personnels 14. Déterminer l'opportunité de mentionner dans l'entente contractuelle que l'entrepreneur doit s'efforcer dans toute la mesure du possible d'assurer l'exactitude et l'intégralité de tout renseignement personnel qu'il utilisera ou dont se servira le gouvernement dans le cadre d'un processus décisionnel qui influera directement sur l'individu faisant l'objet de ces renseignements.

OUI	NON	S.O.	DESCRIPTION
			Usage des renseignements personnels 15. Déterminer l'opportunité de mentionner dans l'entente contractuelle que, sauf indication contraire par écrit, l'entrepreneur doit utiliser les renseignements personnels dans le but exclusif de remplir les obligations qui lui incombent en vertu du contrat.
			Divulgation des renseignements personnels Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 16. il est interdit à l'entrepreneur de communiquer ou de transférer des renseignements personnels, sauf dans la mesure où cela est jugé nécessaire pour lui permettre de remplir les obligations qui lui incombent en vertu de l'entente ou sauf indication contraire par écrit;
			17. si l'entrepreneur reçoit une demande de divulgation de renseignements personnels à des fins non autorisées en vertu du marché, ou s'il constate que la divulgation pourrait être exigée par la loi, il doit immédiatement en informer le gouvernement et ne pas divulguer les renseignements sauf indication contraire par écrit.
			Demandes de renseignements Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 18. les individus qui désirent avoir accès à des documents ou aux renseignements personnels qui les concernent directement auprès de l'entrepreneur peuvent recourir à un processus informel;
			19. les responsabilités du gouvernement et de l'entrepreneur en ce qui concerne les demandes d'accès, en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, à des documents ou des renseignements personnels qui relèvent du gouvernement, mais qui sont conservés par l'entrepreneur.
			Correction des renseignements personnels 20. Déterminer l'opportunité de mentionner dans l'entente contractuelle les responsabilités du gouvernement et de l'entrepreneur en ce qui concerne les demandes de correction ou d'annotation des renseignements personnels conservés par l'entrepreneur, présentées en vertu de la *Loi sur la protection des renseignements personnels*.
			Conservation des documents ou des renseignements personnels Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 21. les exigences en matière de conservation et de retrait des documents et des renseignements personnels, y compris la période de conservation maximale ainsi que les méthodes d'élimination à utiliser;
			22. les conditions régissant l'élimination de documents éphémères créés ou générés par l'entrepreneur.
			Protection des renseignements personnels 23. Déterminer si l'entente contractuelle obligera l'entrepreneur à s'assurer que les renseignements personnels sont protégés contre les risques tels que le vol ou la perte, ainsi que l'accès, la divulgation, le transfert, la reproduction, l'utilisation, la

OUI	NON	S.O.	DESCRIPTION
			modification ou l'élimination non autorisés.
			Plaintes et enquêtes Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 24. que le gouvernement et l'entrepreneur doivent immédiatement s'aviser mutuellement du dépôt de plaintes en vertu de la *Loi sur l'accès à l'information,* de la *Loi sur la protection des renseignements personnels* ou d'une autre loi pertinente et du dénouement de ces plaintes;
			25. que les commissaires à la protection de la vie privée et à l'information ont le droit d'avoir accès à tout document ou renseignement personnel aux fins d'enquêtes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*.
			Vérification et inspection des documents ou des renseignements personnels Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 26. que le gouvernement peut à tout moment, pourvu qu'il donne un préavis raisonnable, se présenter dans les locaux de l'entrepreneur afin d'inspecter, de vérifier ou de faire vérifier par un tiers la mesure dans laquelle l'entrepreneur se conforme aux exigences du contrat relatives à la protection des renseignements personnels, à la sécurité et à la gestion de l'information, et que l'entrepreneur doit coopérer lors d'une telle vérification ou inspection;
			27. l'entrepreneur doit tenir des informations précises pour permettre la vérification des renseignements, c.-à-d. maintenir une piste de vérification quelconque (sous forme électronique ou sur papier).
			Avis de manquement Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 28. l'entrepreneur sera tenu d'aviser le gouvernement immédiatement s'il anticipe ou constate un manquement aux exigences du contrat en matière de protection des renseignements personnels ou de sécurité;
			29. l'entrepreneur sera tenu d'indemniser le gouvernement en cas de manquement aux obligations qui lui incombent en vertu du contrat.
			Sous-traitance Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 30. l'entrepreneur ne doit pas, sans avoir obtenu préalablement l'approbation écrite, confier en sous-traitance une partie des services ou des fonctions prévus dans le contrat;
			31. malgré toute approbation écrite relative à la sous-traitance, l'entrepreneur demeure entièrement responsable de la prestation des services en vertu du contrat principal ou du contrat de sous-traitance.

OUI	NON	S.O.	DESCRIPTION
			Résiliation ou expiration du contrat Déterminer l'opportunité de mentionner dans l'entente contractuelle ce qui suit : 32. tous les renseignements personnels et documents doivent être retournés à l'autorité contractante dès l'achèvement du contrat;
			33. l'entrepreneur continue d'être tenu de protéger les renseignements personnels même après l'achèvement du contrat.

Annexe C : Principaux accords régissant le commerce international

Accord sur le commerce intérieur

L'*Accord sur le commerce intérieur* (ACI) s'applique à la plupart des ministères fédéraux et à sept sociétés d'État. L'ACI vise les marchés de biens d'une valeur égale ou supérieure à 25 000 $ et les marchés de services et de travaux de construction de 100 000 $ ou plus. L'ACI ne s'applique pas aux marchés liés aux industries culturelles, à la culture autochtone ou à la sécurité nationale.

Accord de libre-échange nord-américain

L'*Accord de libre-échange nord-américain* (ALENA) s'applique à la plupart des ministères fédéraux et à dix sociétés d'État. L'ALENA vise les marchés de biens de plus de 38 000 $ (Canada–É.-U.) et 89 000 $ (Canada-Mexique), les marchés de services dont la valeur est égale ou supérieure à 89 000 $ et les marchés de travaux de construction de 11,5 millions de dollars ou plus. Dans le cas des sociétés d'État, l'ALENA s'applique à l'achat de biens et de services évalués à 445 000 $ ou plus et aux marchés de travaux de construction dont la valeur est égale ou supérieure à 14,2 millions de dollars.

Accord sur les marchés publics de l'Organisation mondiale du commerce

L'*Accord sur les marchés publics de l'Organisation mondiale du commerce* (AMP-OMC) s'applique à la plupart des ministères fédéraux. Il vise les marchés de biens ou de services dont la valeur est égale ou supérieure à 261 300 $ et les marchés de travaux de construction de 10 millions de dollars ou plus. L'AMP-OMC est un accord multilatéral qui vise à garantir une concurrence internationale accrue aux fins des marchés publics.

ALENA et AMP-OMC

Biens et services exclus pour le Canada

Les cinq groupes suivants de marchés de services sont entièrement exclus de l'application de l'ALENA et de l'AMP-OMC :

- recherche et développement;
- services de santé et services sociaux;
- services financiers et services connexes;
- services publics;

- services de communications, photographie, cartographie, imprimerie et publication.

Toutes les acquisitions peuvent être assujetties à la détermination, au cas par cas et selon les niveaux appropriés d'autorité, des besoins pour la protection des intérêts essentiels en matière de sécurité liée aux approvisionnements d'armes, de munitions ou de matériel de guerre, ou de tout approvisionnement indispensable à la sécurité nationale ou aux fins de la défense nationale. Advenant qu'un tel besoin soit déterminé, il se pourrait que l'acquisition soit exemptée des dispositions stipulées dans les ententes commerciales.

Les exceptions suivantes s'appliquent :

- les acquisitions à des fins de revente commerciale ou l'utilisation servant à la production de biens à des fins de revente commerciale;
- pour le Canada, les acquisitions effectuées en vertu de montants affectés aux petites entreprises et aux entreprises minoritaires;
- les acquisitions effectuées pour le compte de Transports Canada, de Pêches et Océans Canada, et d'équipement de communication lié aux codes 36, 70 et 74 de la classification fédérale des approvisionnements.

Remarque : Les plafonds susmentionnés ont par le passé changé au rythme de l'inflation et pour d'autres raisons. La notification de tels changements est faite par voie d'Avis sur la politique sur les marchés.

Source : Les renseignements qui précèdent ont été reproduits à partir du document de Travaux publics et Services gouvernementaux Canada intitulé « Occasions de marchés en vertu des accords commerciaux », sur le site Web du Centre de services aux entreprises du Canada / Nouvelle-Écosse.