Appendice B – Annexe 2 – Obligations en matière de protection des renseignements personnels de niveau 2 (jusqu'au niveau Protégé B inclusivement)

> **Remarque à l'intention de l'autorité contractante :** À moins d'indication contraire, toutes les clauses s'appliquent au travail Non classifié, Protégé A et Protégé B, ainsi qu'aux modèles de prestation de services IaaS/PaaS/SaaS.

1. Généralités

1.1 *Objectif*

La présente annexe fait état des obligations de l'entrepreneur en matière de protection des renseignements personnels en ce qui a trait à l'utilisation, à la collecte, au traitement, à la transmission, au stockage ou à l'élimination des données du Canada contenant des renseignements personnels. Les renseignements personnels contenus dans les systèmes de l'entrepreneur ou que l'entrepreneur est tenu de traiter (collecte, conservation, utilisation, divulgation et élimination) doivent être protégés en tout temps grâce à des mesures de protection administratives, matérielles et techniques nécessaires pour garantir que les renseignements personnels sont protégés en fonction du niveau de préjudice possible en cas d'atteinte à la vie privée et conformément à l'entente en matière de traitement des données conclue avec l'entrepreneur, à la présente annexe et aux mesures spécifiques de protection des renseignements personnels imposées à l'entrepreneur (collectivement, les « **obligations en matière de protection des renseignements personnels »**).

1.2 *Répartition des obligations en matière de protection des renseignements personnels*

Les obligations de l'entrepreneur contenues dans le présent document s'appliquent également à tous les sous-traitants dans la mesure où cela est applicable.

1.3 *Gestion du changement*

[S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS]

L'entrepreneur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir les exigences en matière de sécurité en fonction des besoins, afin de se conformer aux pratiques exemplaires en matière de sécurité et aux normes de l'industrie.

L'entrepreneur doit informer le Canada de tout changement ayant pour effet de dégrader de façon importante les services d'informatique en nuage offerts dans le cadre du présent contrat ou susceptibles d'avoir une incidence négative sur ces services, y compris des changements ou des améliorations d'ordre technologique, administratif ou autre. L'entrepreneur s'engage à offrir toutes les améliorations qu'il propose à l'ensemble de ses clients dans le cadre de son offre de services standard, sans frais supplémentaires pour le Canada.

2. Remerciements

Les parties reconnaissent que :

a) Toutes les données du Canada contenant des renseignements personnels sont soumises aux présentes obligations en matière de protection des renseignements personnels.

b) Nonobstant toute autre disposition de la présente annexe, les parties ont la responsabilité partagée d'élaborer et de maintenir des politiques, des procédures et des contrôles de sécurité en ce qui concerne les données du Canada.

c) L'entrepreneur ne doit pas avoir ou tenter d'obtenir la garde des données du Canada, ni permettre au personnel des services d'informatique en nuage d'accéder aux données du Canada avant la mise en œuvre des exigences en matière de sécurité requises en vertu de la présente annexe, au plus tard à la date d'attribution du contrat.

3. Propriété des données

(1) Le Canada demeure à tout moment le responsable du traitement des renseignements personnels par l'entrepreneur dans le cadre du contrat. Le Canada est responsable du respect des obligations du Canada en matière de protection des renseignements personnels en tant que responsable du traitement en vertu du droit applicable à la protection des données, en particulier de la justification de toute transmission de données à caractère personnel à l'entrepreneur (y compris la transmission de tout avis requis et l'obtention de tout consentement et/ou autorisation requis, ou l'obtention d'une base juridique appropriée en vertu du droit applicable à la protection des données), ainsi que des décisions et mesures prises par le Canada en ce qui concerne le traitement des renseignements personnels.

(2) L'entrepreneur est et restera à tout moment un sous-traitant en ce qui concerne les données contenant des renseignements personnels fournies par le Canada à l'entrepreneur en vertu du contrat. L'entrepreneur est responsable du respect des obligations qui lui incombent en vertu de la présente entente en matière de traitement des données et de ses obligations en tant que sous-traitant en vertu de la législation applicable en matière de protection de renseignements personnels (c'est-à-dire la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)).

(3) L'entrepreneur ne doit pas utiliser ou traiter d'une manière quelconque les données du Canada contenant des renseignements personnels ou en tirer de l'information à des fins de partage de données, de publicité ou à des fins commerciales similaires. Le Canada conserve tous les droits, titres et intérêts relatifs aux données des clients. L'entrepreneur n'acquiert aucun droit sur les données des clients, sauf pour ce qui est des droits que le client accorde à l'entrepreneur en vue de la prestation de services d'informatique en nuage au client.

(4) Toutes les données stockées, hébergées ou traitées au nom du Canada restent la propriété du Canada.

4. Demandes de renseignements personnels

(1) Le Canada et l'entrepreneur doivent établir une procédure mutuellement acceptable pour traiter les demandes d'accès aux dossiers en vertu de la *Loi sur l'accès à l'information* et

les demandes d'accès aux renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels* (demandes d'accès).

(2) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Dans les 30 jours civils suivant l'attribution du contrat, l'entrepreneur doit fournir un document décrivant la façon dont il aidera le Canada à traiter les demandes d'accès, y compris la façon dont il accusera réception d'une demande d'accès et la façon dont il fournira les renseignements demandés.

5. Assurance d'une tierce partie : Certifications

(1) L'entrepreneur doit s'assurer que les données du Canada, l'infrastructure de l'entrepreneur (y compris tout service IaaS, PaaS ou SaaS fourni au Canada) et les emplacements des services sont protégés par des mesures de sécurité appropriées qui respectent les exigences énoncées dans les pratiques et politiques de l'entrepreneur en matière de sécurité.

(2) **[**S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS**]** L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports d'audit suivants, en fournissant des rapports d'évaluation ou des certifications de tiers indépendants portant sur chaque niveau de service (par exemple, IaaS, PaaS, SaaS) prévu dans l'offre de services d'informatique en nuage, notamment :

a) ISO/IEC 27018:2014 Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) en nuage public agissant comme processeur de PII – Certification obtenue par un organisme de certification accrédité.

(3) Chaque certification fournie doit :

[S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS]

(i) Indiquer la raison sociale de l'entrepreneur ou du sous-traitant.

[S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS]

(ii) Indiquer la date de certification de l'entrepreneur ou du sous-traitant, ainsi que le statut de la certification.

[S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS]

(iii) Indiquer les services visés par le rapport de certification. Si la méthode de découpage est utilisée pour exclure des organismes de sous-traitance tels que l'hébergement de centres de données, le rapport d'évaluation de ces organismes doit être inclus.

(4) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Chaque audit donnera lieu à la production d'un rapport d'audit qui doit être mis à la disposition du Canada. Les certifications doivent être accompagnées

de pièces justificatives, telles que le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO, et doivent indiquer clairement toutes les constatations importantes faites par l'auditeur. L'entrepreneur doit rapidement remédier aux problèmes soulevés dans tout rapport d'audit, à la satisfaction de l'auditeur.

(5) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit avoir une certification ISO 27018 pendant toute la durée du contrat. Il doit fournir, au moins une fois par année, et rapidement à la demande du Canada, tous les rapports ou dossiers pouvant raisonnablement être exigés pour démontrer que les certifications de l'entrepreneur sont à jour et valides.

6. Protection des renseignements personnels

(1) L'entrepreneur doit démontrer, au moyen de rapports d'évaluation de tiers et de rapports d'audit, qu'il :

a) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Limite la création, la collecte, la réception, la gestion, l'accès, l'utilisation, la conservation, l'envoi, la divulgation et l'élimination des renseignements personnels aux seuls renseignements nécessaires à l'exécution des services d'informatique en nuage.

b) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] A mis en œuvre des processus et des contrôles de sécurité actualisés, tels que des contrôles de gestion de l'accès, la sécurité des ressources humaines, la cryptographie et la sécurité matérielle, la sécurité opérationnelle et la sécurité des communications, qui préservent l'intégrité, la confidentialité et l'exactitude de tous les renseignements, données et métadonnées, quel qu'en soit le format.

7. Vérification de la conformité

(1) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Si le Canada doit effectuer des vérifications de la sécurité et de la protection des renseignements personnels, des inspections ou des examens de renseignements supplémentaires (p. ex., la documentation, les flux de données, la description de la protection des données, l'architecture des données et les descriptions de la sécurité), les deux parties conviennent de négocier une solution de bonne foi et de tenir compte de la justification de la demande du Canada et des processus et des protocoles de l'entrepreneur.

(2) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit effectuer des vérifications de la protection des renseignements personnels et de la sécurité des ordinateurs, de l'environnement informatique et des centres de données qu'il utilise pour traiter les données du Canada contenant des renseignements personnels, comme suit :

a) Lorsqu'une norme ou un cadre prévoit des audits, un audit de cette norme ou de ce cadre de contrôle sera effectué au moins une fois par année.

b) Chaque audit sera réalisé conformément aux normes et règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable.

c) Chaque audit sera effectué par des auditeurs de sécurité qualifiés, indépendants et tiers qui (i) sont qualifiés selon le régime de certification de l'AICPA, de CPA Canada ou de l'ISO, et (ii) sont conformes à la norme ISO/IEC 17020 relative au système de gestion de la qualité, au choix et aux frais de l'entrepreneur.

(3) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Chaque audit donnera lieu à la production d'un rapport d'audit qui doit être mis à la disposition du Canada. Le rapport d'audit doit indiquer clairement toutes les constatations importantes faites par l'auditeur tiers. L'entrepreneur doit, à ses propres frais, remédier rapidement aux problèmes et combler les lacunes soulevées dans tout rapport d'audit, à la satisfaction de l'auditeur.

(4) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] À la demande du Canada, des preuves supplémentaires de l'entrepreneur, y compris des plans de sécurité des systèmes et de protection des renseignements personnels, des conceptions ou des documents d'architecture qui fournissent une description complète du système, y compris tous les éléments de données contenant des renseignements personnels, peuvent être fournis par l'entrepreneur ou un sous-traitant pour compléter la certification et les rapports de vérification décrits à l'article 5 (Assurance d'une tierce partie) afin de démontrer la conformité de l'entrepreneur aux certifications requises de l'industrie.

8. Protection des renseignements personnels dès la conception

L'entrepreneur doit démontrer qu'il protège les renseignements personnels dès la conception dans le cadre du cycle de développement de ses logiciels, et conformément à l'annexe 1 – Obligations en matière de sécurité, article 16 (Développement sécurisé).

9. Responsable de la protection des renseignements personnels

(1) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit, dans les 10 jours suivant la date d'entrée en vigueur du présent contrat, fournir au Canada les renseignements permettant d'identifier le responsable de la protection des renseignements personnels qui agira à titre de représentant de l'entrepreneur pour toutes les questions liées aux renseignements personnels et aux dossiers. L'entrepreneur doit fournir le nom et les coordonnées de cette personne, y compris le titre de son poste, son adresse courriel et son numéro de téléphone.

10. Évaluation des facteurs relatifs à la vie privée

(1) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit aider le Canada à effectuer une évaluation des facteurs relatifs à la vie privée conformément à la (Directive sur l'évaluation des facteurs relatifs à la vie privée), en aidant le Canada à obtenir les documents à l'appui, y compris une ÉFVP de base fournie par l'entrepreneur. L'entrepreneur s'engage à fournir un tel soutien dans les cinq à dix jours ouvrables suivant la demande ou dans un délai convenu d'un commun accord en fonction de la complexité de la demande du Canada.

11. Atteinte à la vie privée

(1) L'entrepreneur doit rapidement évaluer les incidents qui laissent soupçonner ou indiquer un accès ou un traitement non autorisé des renseignements personnels (« **incident** ») et y donner suite. Dès que l'entrepreneur prend connaissance d'un incident et détermine qu'il s'agit d'une atteinte à la vie privée entraînant le détournement ou la destruction accidentelle ou illégale, la perte, l'altération ou la divulgation non autorisée de renseignements personnels transmis, stockés ou traités dans les systèmes de l'entrepreneur ou dans l'environnement des services d'informatique en nuage, ou l'accès à de tels renseignements personnels, qui compromet la sécurité, la confidentialité ou l'intégrité de ces renseignements personnels (« atteinte à la vie privée »), l'entrepreneur doit informer le Canada d'une telle atteinte à la vie privée sans tarder, conformément à l'annexe 1 – Obligations en matière de sécurité, article 26.

(2) L'entrepreneur doit :

a) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Tenir un registre des brèches de sécurité faisant état d'une description de celles-ci, de la période visée, des conséquences de la brèche, du nom de la personne ayant signalé la brèche, du nom de la personne à qui la brèche a été signalée, ainsi que de la procédure de récupération des données.

b) Assurer un suivi, ou permettre au Canada d'assurer un suivi en ce qui concerne les divulgations de données du Canada, notamment les données qui ont été divulguées, à qui et à quel moment.

12. Renseignements personnels

Les sous-articles suivants s'appliquent aux situations où l'entrepreneur confirme qu'il a accès aux données du Canada, qu'il en a la garde et qu'il les contrôle.

12.1 Propriété des renseignements personnels et des dossiers

(1) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Pour offrir des services d'informatique en nuage, l'**entrepreneur ou le sous-traitant** étranger recevra et/ou recueillera des renseignements personnels auprès de tierces parties. L'**entrepreneur ou le sous-traitant** étranger reconnaît qu'il n'a aucun droit sur les renseignements personnels ou les dossiers et que le Canada est propriétaire des dossiers. À la demande du Canada, l'**entrepreneur ou le sous-traitant** étranger doit mettre immédiatement à la disposition du Canada tous les renseignements personnels et les dossiers dans un format acceptable pour le Canada.

12.2 Utilisation des renseignements personnels

(1) L'e**ntrepreneur ou le sous-traitant** étranger s'engage à créer, recueillir, recevoir, gérer, consulter, utiliser, conserver et éliminer les renseignements personnels et les dossiers uniquement dans le cadre des services d'informatique en nuage prévus dans le **contrat**.

12.3 Collecte de renseignements personnels

(1) Si l'e**ntrepreneur ou le sous-traitant** étranger doit recueillir des renseignements personnels auprès d'une tierce partie dans le cadre des services d'informatique en nuage, il doit se limiter aux renseignements nécessaires à l'exécution des services d'informatique

en nuage. L'**entrepreneur ou le sous-traitant** étranger doit recueillir des renseignements personnels auprès de la personne concernée et doit indiquer à cette personne (avant ou au moment de la collecte des renseignements personnels) :

a) que les renseignements en question sont recueillis pour le compte du Canada;

b) que les modalités d'utilisation des renseignements personnels s'appliqueront;

c) que la divulgation des renseignements personnels ou, s'il existe une obligation légale de divulguer les renseignements personnels, la nature de cette obligation légale;

d) que le refus de fournir les renseignements demandés pourrait avoir des conséquences;

e) qu'elle a le droit d'accéder à ses renseignements personnels et d'y apporter des corrections, le cas échéant;

f) que les renseignements personnels feront partie d'un fichier de renseignements personnels spécifique (au sens de la *Loi sur la protection des renseignements personnels*), et que la personne concernée a le droit de savoir quelle institution gouvernementale contrôle ce fichier de renseignements personnels si l'autorité contractante a fourni ces renseignements à l'**entrepreneur ou au sous-traitant** étranger.

(2) L'**entrepreneur ou le sous-traitant** étranger et leurs employés respectifs doivent s'identifier auprès des personnes dont ils recueillent les renseignements personnels et doivent fournir à ces personnes un moyen de vérifier qu'ils sont autorisés à recueillir les renseignements personnels en vertu d'un contrat avec le Canada.

(3) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Si l'autorité contractante le demande, l'**entrepreneur ou le sous-traitant étranger** doit élaborer un formulaire de demande de consentement à utiliser lors de la collecte de renseignements personnels, ou un message pour la collecte de renseignements personnels par téléphone. L'**entrepreneur ou le sous-traitant** étranger ne doit pas commencer à utiliser le formulaire ou le message avant d'avoir obtenu l'approbation de l'autorité contractante. L'entrepreneur doit également obtenir l'approbation de l'autorité contractante avant d'apporter des modifications à un formulaire ou à un message.

(4) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Si, au moment où il demande des renseignements personnels à un particulier, l'**entrepreneur ou le sous-traitant** étranger doute que la personne ait la capacité de consentir à la divulgation et à l'utilisation de ses renseignements personnels, il doit demander des instructions au responsable de la sécurité.

12.4 Maintien de l'exactitude, de la confidentialité et de l'intégrité des renseignements personnels

(1) L'**entrepreneur ou le sous-traitant** étranger doit veiller à ce que les renseignements personnels soient aussi précis, complets et à jour que possible. Il doit également protéger la confidentialité des renseignements personnels. Pour ce faire, il doit, à tout le moins :

a) éviter d'utiliser des identifiants personnels (p. ex., numéro d'assurance sociale) pour établir un lien entre plusieurs bases de données contenant des renseignements personnels;

b) séparer tous les dossiers de ses propres dossiers et renseignements;

c) limiter l'accès aux renseignements personnels et aux dossiers aux personnes qui ont besoin d'y accéder pour la prestation de services d'informatique en nuage (notamment en utilisant des mots de passe ou des contrôles d'accès biométriques);

d) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] offrir à toute personne à laquelle il donnera accès aux renseignements personnels une formation concernant l'obligation de protéger la confidentialité de ces renseignements et de les utiliser uniquement pour offrir des services d'informatique en nuage. L'**entrepreneur ou le sous-traitant** étranger doit dispenser cette formation avant de donner à une personne l'accès à tout renseignement personnel et il doit tenir un registre de la formation offerte et le mettre à la disposition de l'autorité contractante si celle-ci le demande;

e) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] si l'autorité contractante le demande, avant de permettre à quiconque d'accéder aux renseignements personnels, exiger que toute personne à laquelle l'**entrepreneur ou le sous-traitant** étranger donne accès aux renseignements personnels reconnaisse par écrit (sous une forme approuvée par l'autorité contractante) ses responsabilités en matière de protection de la confidentialité des renseignements personnels;

f) tenir un registre de toutes les demandes de consultation des renseignements personnels d'une personne et de toutes les demandes de correction d'erreurs ou d'omissions en ce qui concerne les renseignements personnels (peu importe si ces demandes proviennent directement de la personne concernée ou du Canada, au nom de cette personne);

g) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] indiquer, dans tout dossier pour lequel une personne demande des corrections, si l'**entrepreneur ou le sous-traitant** étranger a décidé de ne pas procéder à la correction pour quelque raison que ce soit. En pareil cas, l'**entrepreneur ou le sous-traitant** étranger doit immédiatement informer l'autorité contractante des détails de la correction demandée et des raisons pour lesquelles l'**entrepreneur ou le sous-traitant a décidé de ne pas apporter cette correction**. Si l'autorité contractante lui demande de procéder à la correction, l'entrepreneur doit le faire;

h) tenir un registre indiquant la date et la source de la plus récente mise à jour de chaque dossier;

i) tenir un journal d'audit qui enregistre électroniquement toutes les occurrences et tentatives d'accès aux archives stockées électroniquement. Le journal d'audit doit être présenté sous une forme qui peut être examinée à tout moment par l'**entrepreneur ou le sous-traitant** étranger et par le Canada;

j) sécuriser et contrôler l'accès à tout document sur papier.

12.5 Protection des renseignements personnels

(1) L'**entrepreneur ou le sous-traitant** étranger doit protéger les renseignements personnels en tout temps, en prenant toutes les mesures raisonnablement nécessaires pour les sécuriser et protéger leur intégrité et leur confidentialité, conformément aux mesures de sécurité décrites à l'annexe 1 – Obligations de sécurité.

12.6 Obligations législatives

(1) L'**entrepreneur ou le sous-traitant** étranger reconnaît que le Canada est tenu de traiter les renseignements personnels et les dossiers conformément aux dispositions de la *Loi sur la protection des renseignements personnels*, L.R.C., 1985, ch. P-21, de la *Loi sur l'accès à l'information*, L.R.C., 1985, ch. A-1, et de la *Loi sur la Bibliothèque et les Archives du Canada*, S.C. 2004, ch. 11. L'**entrepreneur ou le sous-traitant** étranger s'engage à se conformer aux exigences établies par l'autorité contractante qui sont raisonnablement nécessaires pour que le Canada puisse s'acquitter de ses obligations en vertu de ces lois et de tout autre texte de loi en vigueur de temps à autre.

(2) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'**entrepreneur ou le sous-traitant** étranger reconnaît que ses obligations en vertu du **contrat** viennent s'ajouter à toutes les obligations imposées par la *Loi sur la Loi sur la protection des renseignements personnels et les documents électroniques*, S.C. 2000, ch. 5, ou par tout autre texte de loi similaire en vigueur dans une province ou un territoire du Canada. Si l'**entrepreneur ou le sous-traitant** étranger estime qu'une obligation quelconque du **contrat** l'empêche de s'acquitter de ses obligations en vertu d'une de ces lois, il doit immédiatement informer l'autorité contractante de la disposition du contrat allant à l'encontre d'une disposition législative spécifique.

12.7 Obligation légale de divulguer des renseignements personnels

(1) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] Si l'entrepreneur reçoit une citation à comparaître, une ordonnance judiciaire, administrative ou arbitrale de la part d'un organisme exécutif ou administratif, d'un organisme de réglementation ou d'une autre autorité gouvernementale en ce qui concerne le traitement des renseignements personnels (« demande de divulgation »), il doit rapidement transmettre cette demande de divulgation au Canada sans y répondre, à moins d'indication contraire dans la loi applicable (notamment pour fournir un accusé de réception à l'autorité ayant présenté la demande de divulgation).

(2) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] À la demande du Canada, l'entrepreneur doit fournir les renseignements en sa possession pouvant raisonnablement être jugés pertinents en ce qui concerne la demande de divulgation et toute l'aide raisonnablement nécessaire pour que le Canada puisse répondre à la demande de divulgation en temps opportun.

12.8 Plaintes

Le Canada et l'**entrepreneur ou le sous-traitant** étranger conviennent chacun d'aviser immédiatement l'autre partie en cas de plainte 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 concernant les renseignements personnels. Chaque partie accepte de fournir à l'autre toute information nécessaire pour l'aider à répondre à la plainte et d'informer immédiatement l'autre partie de l'issue d'une telle plainte.

12.9 Exception

Les obligations énoncées dans les présentes conditions générales complémentaires ne s'appliquent pas aux renseignements personnels qui sont déjà dans le domaine public, sauf si ces renseignements sont dans le domaine public à la suite d'un acte ou d'une omission de l'entrepreneur ou de l'un de ses sous-traitants, agents ou représentants, ou de l'un de leurs employés.