Annexe 2 – Obligations en matière de protection de la vie privée

1. Généralités

1.1 *Objet*

La présente annexe a pour objet d'énoncer les obligations du contracteur en matière de protection de la vie privée en ce qui concerne l'utilisation, la collecte, le traitement, la transmission, le stockage ou l'élimination des données du Canada[1] contenant des renseignements personnels. Tous les renseignements personnels qui sont stockés dans les systèmes du contracteur ou que le contracteur est tenu de traiter (collecte, conservation, utilisation, divulgation et élimination) doivent être protégés en tout temps par la mise en œuvre de mesures de protection administratives, physiques et techniques nécessaires pour s'assurer que les renseignements personnels sont protégés en fonction du niveau de préjudice qui pourrait survenir si une atteinte à la vie privée devait se produire, et conformément aux dispositions de l'accord de traitement des données du contracteur, à la présente annexe et aux mesures précises de protection de la vie privée de l'entrepreneur (collectivement, les « **Obligations en matière de protection de la vie privée** »).

1.2 *Transfert des obligations en matière de protection de la vie privée*

Dans la mesure du possible, les obligations du contracteur contenues dans les présentes obligations en matière de protection de la vie privée s'appliquent du contracteur aux sous-traitants.

1.3 *Gestion du changement*

Le contracteur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir les obligations en matière de protection de la vie privée requises pour se conformer aux pratiques de sécurité des normes de l'industrie.

Le contracteur doit informer le Canada de tout changement qui dégrade de façon importante ou qui peut avoir une incidence négative sur les offres de services infonuagiques du présent contrat, y compris les changements ou améliorations de nature technologique, administrative ou autre qui sont apportés et qui pourraient avoir une incidence sur la collecte, l'utilisation, la divulgation ou l'élimination actuelles de données contenant des renseignements personnels. Le contracteur 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. Attestation

Les parties reconnaissent que :

(a) toutes les données du Canada contenant des renseignements personnels sont assujetties à ces obligations en matière de protection de la vie privée.

(b) nonobstant toute autre disposition de la présente annexe, les parties ont la responsabilité partagée de l'élaboration et du maintien des politiques, des procédures et des contrôles en matière de protection de la vie privée relatifs aux données du Canada.

(c) Le contracteur ne doit pas avoir ou tenter d'obtenir la garde des données du Canada, ni permettre à un membre de son personnel d'accéder aux données du Canada avant la mise

[1] Canada désigne le gouvernement du Canada

en œuvre des obligations en matière de protection de la vie privée, comme l'exige la présente annexe, à la date d'attribution du contrat ou avant.

3. Propriété des données

(1) Le Canada demeurera en tout temps le contrôleur des renseignements personnels traités par le contracteur, en vertu du contrat. Le Canada est responsable du respect de ses obligations en matière de protection de la vie privée en tant que responsable du traitement en vertu de la loi applicable sur la protection des données, en particulier de la justification de toute transmission de renseignements personnels au contracteur (y compris la fourniture des avis requis et l'obtention des consentements et/ou autorisations nécessaires, ou l'obtention d'un fondement juridique appropriée en vertu de la loi applicable sur la protection des données), ainsi que des décisions et actions du Canada concernant le traitement de ces données personnelles.

(2) Le contracteur est et restera en tout temps un sous-traitant en ce qui concerne les données contenant des renseignements personnels fournies par le Canada le contracteur en vertu du contrat. Il incombe au contracteur de respecter ses obligations en vertu du présent accord de traitement des données du contracteur et de respecter ses obligations en tant que sous-traitant aux termes de la loi applicable en matière de protection de la vie privée (c'est-à-dire la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

(3) Le contracteur ne doit pas utiliser ni traiter les données du Canada contenant des renseignements personnels, ni en tirer des renseignements à des fins de partage de données, de publicité ou autres fins commerciales similaires. Quant aux parties, le Canada conserve tous les droits, titres et intérêts relatifs aux données des clients. Le contracteur n'acquiert aucun droit sur les données des clients, autre que les droits que le client lui accorde pour fournir les services infonuagiques au client.

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

4. Demandes relatives à la protection de la vie privée

(1) Le Canada et le contracteur doivent établir un processus mutuellement acceptable pour traiter les demandes d'accès à l'information ou 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) Dans les 30 jours civils suivant l'attribution du contrat, le contracteur doit fournir un document qui décrit comment il aidera le Canada à traiter les demandes d'accès, y compris comment il accusera réception d'une demande d'accès et comment il fournira l'information demandée.

5. Assurance d'une tierce partie : Certifications

(1) Le contracteur doit s'assurer qu'en ce qui concerne les renseignements personnels, y compris les données du Canada qu'il peut héberger, stocker ou traiter, sur l'infrastructure du contracteur (y compris tout IaaS (infrastructure en tant que service), PaaS (plateforme en tant que service) ou SaaS (solution en tant que service) fourni au Canada et les points de service sont protégés par des mesures de sécurité et de protection des renseignements personnels appropriées qui sont conformes aux exigences énoncées dans les pratiques et les politiques du contracteur en matière de protection de la vie privée.

(2) Le contracteur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications suivantes, en fournissant des rapports d'évaluation ou des certifications de tiers indépendants qui portent sur chaque couche de service (par exemple IaaS, PaaS, SaaS) au sein de l'offre de services infonuagiques, y compris :

a) ISO/IEC 27018:2014 Technologies de l'information -- Techniques de sécurité -- Code de pratique pour la protection des informations personnellement identifiables (PII) dans les systèmes infonuagiques publics agissant comme processeurs de PII – Certification obtenue par un organisme de certification accrédité.

(3) Chaque certification fournie doit : (i) indiquer la raison sociale légale du contractant ou du sous-traitant concerné; (ii) indiquer la date de certification du contractant ou du sous-traitant et le statut de cette certification; (iii) indiquer les services inclus dans le champ d'application du rapport de certification. Si la méthode créée est utilisée pour exclure des organismes de sous-services tels que l'hébergement de centres de données, le rapport d'évaluation de l'organisme de sous-services doit être inclus.

(4) Chaque vérification donnera lieu à la production d'un rapport qui devra être mis à la disposition du Canada. Les certifications doivent être accompagnées de preuves à l'appui telles que le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO et doivent clairement divulguer toute constatation importante faite par le vérificateur. Le contracteur doit remédier rapidement aux problèmes soulevés dans tout rapport de vérification à la satisfaction du vérificateur.

(5) Le contractant est censé maintenir sa certification ISO 27018 pendant toute la durée du contrat. Le contractant doit fournir, au moins une fois par an, et sans délai à la demande du Canada, tous les rapports ou dossiers qui peuvent être raisonnablement requis pour démontrer que les certifications du contractant sont à jour et valides.

6. Conformité aux règles en matière de protection de la vie privée

(1) Le contractant doit démontrer par des rapports d'évaluation et des rapports de vérification par des tiers qu'il :

(a) limite l'accès aux renseignements personnels à ce qui est nécessaire pour exécuter les services infonuagiques, ainsi que la création, la collecte, la réception, la gestion, l'utilisation, la conservation, l'envoi, la divulgation et l'élimination des renseignements personnels;

(b) a mis en œuvre des processus et des contrôles de sécurité à jour, tels que des contrôles de gestion de l'accès, la sécurité des ressources humaines, la

cryptographie et la sécurité physique, opérationnelle et des communications qui préservent l'intégrité, la confidentialité et l'exactitude de toutes les informations, données et métadonnées, quel que soit le format.

7. Vérification de la conformité

(1) Si le Canada doit procéder à des vérifications, des inspections en matière de sécurité et de protection de la vie privée ou à un examen de tout renseignement supplémentaire (p. ex., documentation, flux de données, description de la protection des données, architecture des données et descriptions de la sécurité), les deux parties conviennent de négocier une solution de bonne foi et de tenir compte à la fois de la justification de la demande du Canada et des processus et protocoles du contracteur.

(2) Le contractant doit effectuer les vérifications de la sécurité et des mesures de protection des renseignements personnels des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter les données du Canada contenant des renseignements personnels comme suit :

(a) lorsqu'une norme ou un cadre prévoit des vérifications, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par an;

(b) chaque vérification sera réalisée conformément aux normes et aux règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable;

(c) chaque vérification sera effectuée par un vérificateur tiers qualifié et indépendant de la protection de la vie privée qui (i) est qualifié dans le cadre du régime de certification d'une organisation reconnue comme l'AICPA, CPA Canada ou ISO, ou détenant une certification reconnue dans le domaine de la vie privée et de la protection des renseignements personnels, et (ii) se conforme à la norme relative au système de gestion de la qualité ISO/IEC 17020, au choix et aux frais du contracteur.

(3) chaque vérification donnera lieu à la production d'un rapport de vérification qui devra être mis à la disposition du Canada. Le rapport de vérification doit clairement divulguer toute constatation importante faite par le tiers vérificateur. Le contractant doit, à ses propres frais, remédier rapidement aux problèmes et corriger les lacunes soulevées dans tout rapport de vérification à la satisfaction du vérificateur.

(4) À la demande du Canada, le contracteur ou un sous-traitant peut fournir des preuves supplémentaires du contracteur, y compris des plans, conceptions ou documents d'architecture de sécurité et de protection de la vie privée du système qui fournissent une description complète du système, y compris tous les éléments de données contenant des renseignements personnels, afin de compléter les rapports de certification et de vérification décrits à la section 5 (Assurance d'une tierce partie) et de démontrer que le contracteur se conforme aux certifications requises de l'industrie.

8. Protection de la vie privée dès la conception

Le contractant doit démontrer qu'il met en œuvre la protection de la vie privée dès la conception dans le cadre du cycle de vie de son développement de ses logiciels, et conformément à l'annexe 1 – Obligations en matière de sécurité, section 16 (Développement sécurisé).

9. Agent du service de la protection de la vie privée

(1) Le contractant doit, dans les 10 jours suivant la date d'entrée en vigueur du présent contrat, fournir au Canada les renseignements qui permettent de désigner une personne à titre d'agent du service de la protection de la vie privée qui agira comme représentant du contracteur pour toutes les questions liées aux renseignements personnels et aux dossiers. Le contractant doit donner le nom et les coordonnées de cette personne, y compris son titre professionnel, son adresse électronique et son numéro de téléphone.

10. Aider à la réalisation de l'évaluation des facteurs relatifs à la vie privée du Canada

(1) Le contractant doit aider le Canada à réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) conformément à la Directive sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308), en aidant le Canada à fournir les documents justificatifs, y compris une EFVP de base pour le Canada, fournie par le contracteur. Le contractant s'engage à fournir ce soutien dans les cinq à dix jours ouvrables suivant une demande ou dans un délai convenu d'un commun accord, selon la complexité de la demande du Canada.

11. Atteinte à la vie privée

(1) Le contractant doit évaluer les incidents qui créent des soupçons ou indiquent un accès non autorisé à des renseignements personnels ou un traitement non autorisé de tels renseignements (« **Incident** ») et y réagir rapidement. Dans la mesure où le contracteur apprend et détermine qu'un incident constitue une atteinte à la vie privée menant à l'appropriation illicite ou à la destruction, à la perte, à l'altération accidentelle ou illégale, à la divulgation non autorisée ou à l'accès à des renseignements personnels transmis, stockés ou par ailleurs traités dans les systèmes du contracteur ou dans l'environnement des services infonuagiques compromettant la sécurité, la confidentialité ou l'intégrité de ces renseignements personnels (« atteinte aux renseignements personnels »), le contracteur informera le Canada d'une telle atteinte aux renseignements personnels sans tarder, et conformément à l'annexe 1 – Obligations en matière de sécurité, section 26.

(2) Le contractant doit :

(a) tenir un registre des atteintes à la sécurité comprenant une description de l'atteinte, la durée, les conséquences de l'atteinte, le nom de la personne qui a signalé l'atteinte, et celui de la personne à qui l'atteinte a été signalée, et la procédure de récupération des données;

(b) suivre ou permettre au Canada de suivre les divulgations de données du Canada, y compris quelles données ont été divulguées, à qui et à quel moment.

12. Renseignements personnels

Les sous-sections suivantes s'appliquent aux situations où le contracteur confirme qu'il a accès aux données du Canada, qu'il en a la garde et le contrôle.

12.1 Propriété des renseignements personnels et des dossiers

(1) Pour exécuter les services infonuagiques, **le contracteur ou le sous-traitant** destinataire étranger recevra ou recueillera des renseignements personnels de tiers. **Le contracteur ou le sous-traitant** destinataire étranger reconnaît qu'il n'a aucun droit à l'égard des renseignements personnels ou des dossiers et que le Canada est le propriétaire des dossiers. Sur demande, **le contracteur ou le sous-traitant** destinataire étranger doit mettre immédiatement à la disposition du Canada tous les renseignements personnels et dossiers à la disposition du Canada dans un format acceptable pour le Canada.

12.2 Utilisation des renseignements personnels

(1) **Le contracteur ou le sous-traitant** destinataire étranger accepte d'accéder aux renseignements personnels et aux dossiers, de les créer, de les recueillir, de les recevoir, de les gérer, de les utiliser, de les conserver et de les éliminer uniquement pour exécuter les services infonuagiques conformément au contrat.

12.3 Collecte de renseignements personnels

(1) Si **le contracteur ou le sous-traitant** destinataire étranger doit recueillir des renseignements personnels auprès d'un tiers pour exécuter les services infonuagiques, **le contracteur ou le sous-traitant** destinataire étranger doit uniquement recueillir les renseignements personnels qui sont nécessaires pour exécuter les services infonuagiques. **Le contracteur ou le sous-traitant** destinataire étranger doit recueillir les renseignements personnels auprès de la personne à laquelle ils se rapportent et **le contracteur ou le sous-traitant** destinataire étranger doit informer cette personne (au plus tard au moment où il recueille les renseignements personnels) de ce qui suit :

(a) que les renseignements personnels sont recueillis au nom du Canada et seront fournis à ce dernier;

(b) les modalités d'utilisation des renseignements personnels;

(c) que la divulgation des renseignements personnels est volontaire ou, s'il existe une obligation légale de divulguer les renseignements personnels, le fondement de cette obligation légale;

(d) les conséquences, le cas échéant, du refus de fournir les renseignements;

(e) que la personne a le droit d'accéder à ses renseignements personnels et de les corriger;

(f) que les renseignements personnels feront partie d'un fichier de renseignements personnels précis (au sens de la *Loi sur la protection des renseignements personnels et/ou de toute autre loi applicable, telle que le RGPD*) et fourniront également à la personne des renseignements sur l'institution gouvernementale qui contrôle ce fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements au **contracteur ou au sous-traitant** destinataire étranger.

(2) **Le contracteur ou le sous-traitant** destinataire étranger et ses employés respectifs doivent s'identifier auprès des personnes auprès desquelles ils recueillent des renseignements personnels et doivent fournir à ces personnes un moyen de vérifier qu'elles sont autorisées à recueillir les renseignements personnels en vertu d'un contrat avec le Canada.

(3) Si l'autorité contractante le demande, **le contracteur ou le sous-traitant** destinataire étranger doit élaborer un formulaire de demande de consentement à utiliser lors de la collecte de renseignements personnels, ou un script pour la collecte des renseignements personnels au téléphone. **Le contracteur ou le sous-traitant** destinataire étranger ne doit pas commencer à utiliser le formulaire ou le script à moins que l'autorité contractante ne l'approuve au préalable par écrit. Le contracteur doit également obtenir l'approbation de l'autorité contractante avant d'apporter des modifications à un formulaire ou à un script.

(4) Au moment où il demande des renseignements personnels à une personne, si **le contracteur ou le sous-traitant** destinataire étranger doute que la personne ait la capacité de donner son consentement à la divulgation et à l'utilisation de ses renseignements personnels, **le contracteur ou le sous-traitant** destinataire étranger doit demander des instructions au responsable de la sécurité des marchés.

12.4 Préserver l'exactitude, la confidentialité et l'intégrité des informations personnelles

(1) **Le contracteur ou le sous-traitant** destinataire étranger doit s'assurer que les renseignements personnels sont aussi exacts, complets et à jour que possible. **Le contracteur ou le sous-traitant** destinataire étranger doit protéger la confidentialité des renseignements personnels. Pour ce faire, au minimum, **le contracteur ou le sous-traitant** destinataire étranger :

(a) ne doit pas utiliser d'identifiants personnels (par exemple, le numéro d'assurance sociale) pour relier plusieurs bases de données contenant des informations personnelles;

(b) doit séparer tous les dossiers des renseignements et dossiers **du contracteur ou du sous-traitant** destinataire étranger;

(c) doit limiter l'accès aux renseignements personnels et aux dossiers aux personnes qui ont besoin d'y accéder pour effectuer les services infonuagiques (par exemple, en utilisant des mots de passe ou des contrôles d'accès biométriques);

(d) doit fournir une formation à toute personne à laquelle **le contracteur ou le sous-traitant** destinataire étranger donnera accès aux renseignements personnels

concernant l'obligation de les garder confidentiels et de ne les utiliser que pour exécuter les services infonuagiques. **Le contracteur ou le sous-traitant** destinataire étranger doit dispenser cette formation avant de donner à une personne l'accès à des renseignements personnels et **le contracteur ou le sous-traitant** destinataire étranger doit tenir un registre de la formation et le mettre à la disposition de l'autorité contractante si celle-ci le demande;

(e) si l'autorité contractante le demande, avant de donner à quiconque l'accès aux renseignements personnels, demander à toute personne à qui **le contracteur ou le sous-traitant** destinataire étranger donne accès aux renseignements personnels de reconnaître par écrit (sous une forme approuvée par l'autorité contractante) ses responsabilités pour préserver la confidentialité des renseignements personnels;

(f) doit tenir un registre de toutes les demandes de révision de ses renseignements personnels faites par une personne, et toutes les demandes de corriger des erreurs ou omissions dans les renseignements personnels (que ces demandes soient faites directement par une personne ou par le Canada au nom d'une personne);

(g) doit inclure une inscription sur tout dossier dont une personne a demandé la correction si **le contracteur ou le sous-traitant** destinataire étranger a décidé de ne pas effectuer la correction pour une raison quelconque. Chaque fois que cela se produit, **le contracteur ou le sous-traitant** destinataire étranger doit immédiatement informer l'autorité contractante des détails de la correction demandée et des raisons de la décision de **le contracteur ou du sous-traitant** destinataire étranger de ne pas les faire. Si l'autorité contractante lui ordonne d'apporter la correction, le contracteur doit le faire;

(h) tenir un registre de la date et de la source de la dernière mise à jour de chaque dossier;

(i) tenir un journal de vérification qui consigne électroniquement tous les cas et tentatives d'accès aux dossiers stockés électroniquement. Le journal de vérification doit être dans un format qui peut être examiné par **le contracteur ou le sous-traitant** destinataire étranger et le Canada en tout temps;

(j) sécuriser et contrôler l'accès à toute copie papier des dossiers.

12.5 Protection des renseignements personnels

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

12.6 Obligations statutaires

(1) **Le contracteur ou le sous-traitant** destinataire étranger reconnaît que le Canada est tenu de traiter les renseignements personnels et les dossiers conformément aux dispositions des lois canadiennes suivantes : *Loi sur la protection des renseignements personnels*, *Loi sur l'accès à l'information*, L.R.C. (1985), ch. A-1, et *Loi sur la Bibliothèque et les Archives du Canada*, L.C. 2004, ch. 11 et toute autre loi applicable. **Le contracteur ou le sous-traitant** destinataire étranger accepte de se conformer aux exigences établies par l'autorité contractante qui sont raisonnablement nécessaires pour s'assurer que le Canada respecte ses obligations en vertu de ces lois et de toute autre législation en vigueur de temps à autre.

(2) **Le contracteur ou le sous-traitant** destinataire étranger reconnaît que ses obligations en vertu du contrat s'ajoutent à toutes les obligations qu'il a en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, ou toute autre législation similaire en vigueur dans une province ou un territoire du Canada. Si **le contracteur ou le sous-traitant** destinataire étranger estime que l'une des obligations du **contrat** l'empêche de respecter ses obligations en vertu de l'une de ces lois, **le contracteur ou le sous-traitant** destinataire étranger doit immédiatement informer l'autorité contractante de la disposition précise du **contrat** et de l'obligation précise en vertu de la loi avec laquelle **le contracteur ou le sous-traitant** destinataire étranger estime qu'elle est en conflit.

12.7 Obligation juridique de divulguer les renseignements personnels

(1) Si le contracteur reçoit une citation à comparaître, une ordonnance judiciaire, administrative ou arbitrale d'un organisme de direction ou administratif, d'un organisme de réglementation ou d'une autre autorité gouvernementale qui concerne le traitement des renseignements personnels (« demande de divulgation »), il transférera rapidement cette demande au Canada sans y répondre, sauf si la loi applicable l'exige (notamment pour fournir un accusé de réception à l'autorité qui a fait la demande de divulgation).

(2) À la demande du Canada, le contracteur fournira au Canada les renseignements raisonnables en sa possession qui peuvent répondre à la demande de divulgation et toute aide raisonnablement requise pour que le Canada puisse répondre à la demande de divulgation en temps opportun.

12.8 Plaintes

Le Canada et **le contracteur ou le sous-traitant** destinataire étranger conviennent par entente mutuelle de s'informer immédiatement si une plainte est reçue en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* ou de toute autre loi pertinente concernant les renseignements personnels. Chaque partie convient de fournir à l'autre tout renseignement nécessaire pour l'aider à répondre à la plainte et d'informer immédiatement l'autre partie de l'issue de cette plainte.

12.9 Exception

Les obligations énoncées dans les présentes conditions générales supplémentaires ne s'appliquent pas aux renseignements personnels qui sont déjà dans le domaine public, tant qu'ils

ne sont pas devenus partie du domaine public à la suite d’un acte ou d’une omission du contracteur ou de l’un de ses sous-traitants, agents ou représentants, ou de l’un de leurs employés.