VIE PRIVÉE ET SÉCURITÉ

1. **Définitions.**
   "Données personnelles" a la signification qui lui est donnée dans les Conditions générales.
   Le "**personnel**" désigne les employés et les consultants du fournisseur ayant accès aux données ou aux systèmes utilisés pour fournir le service SaaS et les services d'assistance liés au SaaS dans le cadre du contrat.

2. **Généralités. Le** Fournisseur doit maintenir un programme complet de sécurité de l'information destiné à protéger la sécurité et la confidentialité des Données et à se prémunir contre toute menace ou tout risque raisonnablement anticipé pour la sécurité ou l'intégrité de ces Données.

3. **Mesures techniques et organisationnelles et sécurité de l'information. Le** fournisseur doit respecter les mesures de sécurité suivantes en ce qui concerne son environnement de production :
   3.1. Garanties administratives.
   - 3.1.1. Politiques de sécurité de l'information. Le fournisseur doit avoir mis en place un cadre politique complet en matière de sécurité de l'information, comprenant notamment des politiques et des normes (ci-après dénommées collectivement "politiques de sécurité"), alignées sur les pratiques standard de l'industrie, le cas échéant. Ces politiques de sécurité doivent traiter des questions de sécurité de l'information et répondre aux exigences légales, réglementaires et contractuelles raisonnablement pertinentes/applicables et disposer, le cas échéant, de lignes directrices, de processus et de procédures d'appui qui exposent la manière dont le fournisseur s'acquittera de ses engagements en matière de sécurité. Les politiques de sécurité comprennent des mesures de protection administratives, technologiques et physiques appropriées pour : (i) protéger contre les menaces à la sécurité et à la confidentialité des données, y compris l'utilisation, l'accès ou la divulgation non autorisés ; (ii) assurer un niveau constant de protection des données à la fois pendant les opérations normales et dans des circonstances extraordinaires, comme lorsque le Fournisseur opère dans le cadre d'un scénario de continuité des activités ou de catastrophe ; (iii) limiter l'accès aux données à ceux qui ont "besoin de savoir" ; et (iv) assurer l'élimination des données en toute sécurité. Les politiques de sécurité doivent être approuvées par la direction générale, communiquées au personnel et révisées chaque année afin d'en garantir l'exactitude et l'exhaustivité et de tenir compte de l'évolution des normes et de l'évolution des menaces et des risques. Les politiques de sécurité prévoient des mesures disciplinaires en cas de violation.
   - 3.1.2. Confidentialité. Le personnel, les contractants et les consultants sont soumis à des obligations de confidentialité conformes à l'esprit du présent contrat.
   - 3.1.3. Sécurité du personnel. Le personnel doit avoir des descriptions de poste clairement définies qui comprennent les exigences et les responsabilités en matière de sécurité, et ces descriptions de poste doivent être revues périodiquement afin de garantir leur exactitude et leur exhaustivité. Le personnel doit faire l'objet d'une vérification de ses antécédents dans la mesure permise par la législation applicable, ce qui inclut, sans s'y limiter, la vérification de son identité, la vérification de son casier judiciaire, la vérification de ses emplois antérieurs, la vérification de ses diplômes, la vérification de ses références, ainsi que la vérification de la liste des ressortissants spécialement désignés de l'Office of Foreign Assets Controls du département du Trésor des États-Unis (Office of Foreign Assets Controls). Le personnel signe un accord de non-divulgation. Chaque année, le personnel doit également signer un "Accord d'utilisateur privilégié" ou un formulaire similaire, et reconnaître le code de conduite de l'entreprise. Le personnel doit participer chaque année à une formation au code de conduite et à des séances de sensibilisation à la sécurité de l'information et à la protection de la vie privée.
   - 3.1.4. Contrôle d'accès. Le Fournisseur maintiendra des procédures et des contrôles pour authentifier et limiter l'accès aux systèmes utilisés pour fournir le Service SaaS aux personnes autorisées. L'accès à ces systèmes sera accordé en fonction du besoin d'en connaître, en appliquant le principe du moindre privilège, le cas échéant. Le personnel disposant de privilèges administratifs est tenu d'utiliser l'authentification multifactorielle pour accéder à ces systèmes. Le personnel n'accède pas aux données et ne les visualise pas, sauf si cela est nécessaire pour fournir les services SaaS dans le cadre du contrat. L'accès doit être supprimé rapidement en cas de résiliation ou de changement de poste, le cas échéant.
   - 3.1.5. Gestion des risques. Le Fournisseur doit mettre en place un processus et procéder à des évaluations régulières et complètes des risques et vulnérabilités internes et externes raisonnablement prévisibles pour la confidentialité, l'intégrité et la disponibilité des données qui pourraient entraîner la divulgation non autorisée, l'utilisation abusive, l'altération, la destruction ou toute autre compromission de ces données, et concevoir et mettre en œuvre des mesures de sauvegarde pour réduire ces risques et vulnérabilités à un niveau raisonnable et approprié.
   - 3.1.6. Gestion des changements. Le fournisseur doit avoir mis en place un processus formalisé de gestion des

changements qui exige l'identification, la documentation, le test, l'approbation et l'examen après mise en œuvre des changements d'application et d'infrastructure susceptibles d'avoir un impact sur la sécurité, la stabilité et la disponibilité du système ou d'avoir d'autres effets négatifs sur le service SaaS. Les modifications proposées sont évaluées afin de déterminer si elles présentent un risque pour la sécurité et quelles mesures d'atténuation doivent être prises. L'accès aux systèmes de production doit être strictement limité et les développeurs ne doivent pas avoir la possibilité de migrer les modifications dans l'environnement de production.

3.1.7. Gestion des incidents. Le Fournisseur doit mettre en place un cadre de gestion des incidents conçu pour répondre rapidement et efficacement à tous les types d'événements opérationnels et de sécurité internes et externes qui menacent la confidentialité, l'intégrité ou la disponibilité du système utilisé pour fournir les Services SaaS et toutes les Données qu'il contient.

3.1.8. Continuité des activités et reprise après sinistre. Le service SaaS est conçu avec les ressources raisonnablement nécessaires pour assurer la disponibilité des services SaaS conformément aux niveaux de service et d'une manière qui permette la reprise dans le délai de rétablissement (RTO) établi à la suite d'une interruption de service. Les tests des composants nécessaires sont effectués selon ce qui est raisonnablement exigé pour garantir la capacité de récupération.

3.1.9. Audits organisationnels. Au moins une fois par an pendant la durée du contrat, le fournisseur demandera, à ses frais exclusifs, à un tiers qualifié de bonne réputation de procéder à une évaluation du contrôle de l'organisation des services (SOC) 2 du service SaaS afin d'évaluer l'adéquation de la conception et l'efficacité opérationnelle des contrôles pour répondre aux principes et critères des services de confiance pour la sécurité établis par la section 100 du TSP de CPA Canada/AICPA, Principes, critères et illustrations des services de confiance pour la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la protection de la vie privée (AICPA, Technical Practice Aids). Cette évaluation doit raisonnablement couvrir tous les sites utilisés pour fournir le service SaaS, ci-après dénommé "audit organisationnel". Outre la description et l'évaluation des contrôles en place, le rapport d'audit organisationnel comprendra également une description des contrôles organisationnels, opérationnels et commerciaux relatifs au Service SaaS, dans le cadre général du type d'audit organisationnel en question. Le Fournisseur mettra à la disposition du Client une copie du rapport SOC 2 résumant les conclusions de cet Audit Organisationnel, sur demande écrite.

3.2. Garanties techniques.

3.2.1. Séparation des données. Le Fournisseur veille à ce que les Données soient stockées, utilisées, consultées et éliminées dans un environnement sécurisé et à ce qu'elles soient à tout moment séparées logiquement des données de ses autres clients, y compris dans le cadre d'un scénario de continuité des activités ou de reprise après sinistre.

3.2.2. Configuration du système. Le système utilisé pour fournir le service SaaS doit être segmenté en zones de réseau distinctes protégées par des pare-feu ou des mécanismes équivalents afin d'atténuer le risque d'accès non autorisé et d'arrêter la propagation des infections par des logiciels malveillants au niveau des points d'accès internes et externes. Le fournisseur doit maintenir des procédures et des contrôles pour l'installation, la configuration, l'exploitation et la maintenance sécurisées des systèmes d'information (par exemple, postes de travail, serveurs, réseaux et applications), y compris des procédures de gestion des changements, de gestion des correctifs et de gestion des vulnérabilités. Les composants des systèmes doivent être configurés conformément aux lignes directrices en matière de renforcement et être dotés de systèmes antivirus et de détection d'intrusion, le cas échéant.

3.2.3. Développement d'applications. Le fournisseur utilisera des environnements distincts pour le développement, les essais, la mise à l'essai et la production, afin que toute modification de l'infrastructure et des logiciels soit développée et testée dans un environnement distinct avant d'être mise en œuvre dans la production, et afin de réduire le risque de modifications involontaires de l'environnement de production. Le fournisseur procède régulièrement à des examens et à des analyses du code de ses logiciels afin de réduire la probabilité qu'une vulnérabilité soit déployée en production.

3.2.4. Contrôle. Le Fournisseur doit maintenir des procédures et des contrôles pour détecter, prévenir et répondre aux attaques, intrusions ou autres défaillances des systèmes, y compris les actions à prendre en cas de suspicion ou de détection d'un accès non autorisé aux Données. Le Fournisseur doit mettre en place et maintenir des outils, y compris, mais sans s'y limiter, un système de gestion des incidents et des événements de sécurité (SIEM), pour permettre une surveillance continue appropriée de la santé et de la sécurité du Service SaaS, y compris la détection de menaces et d'incidents de sécurité éventuels. Ces outils surveillent la disponibilité du système, l'utilisation des ressources, les événements de sécurité, les modifications non autorisées du système et les activités inhabituelles, et disposent de notifications automatisées pour les problèmes de système et de sécurité en temps réel. Les événements surveillés sont mis en corrélation de manière centralisée et les journaux d'événements sont examinés régulièrement afin de permettre l'identification rapide des problèmes, la planification des capacités et la prise de mesures appropriées dans un délai raisonnable pour tout problème détecté lors de ces examens.

3.2.5. Gestion de la vulnérabilité. Afin d'identifier les vulnérabilités potentielles du Service SaaS, le Fournisseur effectuera régulièrement des évaluations de vulnérabilité. Ces évaluations comprennent des tests de

vulnérabilité des applications. Les correctifs et les mises à jour de sécurité seront appliqués en fonction de leur criticité.

3.2.6. Tests de sécurité. Au moins une fois par an, ou lors de la livraison de versions majeures, et à la seule discrétion du Fournisseur, ce dernier retiendra les services d'un tiers qualifié et réputé pour effectuer des tests de pénétration du Service SaaS et préparer un rapport sur ses conclusions.

3.2.7. Utilisation du cryptage. Le Fournisseur utilisera un cryptage approprié, à l'aide d'algorithmes et de longueurs de clés acceptés par l'industrie, pour protéger les Données stockées dans le Service SaaS, ou transmises sur des réseaux publics, en relation avec les Services SaaS.

3.2.8. Utilisation du stockage portable. Sauf demande explicite du Client ou nécessité de fournir des Services SaaS dans le cadre du présent Contrat, et protégées par cryptage, les Données ne doivent pas être copiées sur des systèmes informatiques ou des supports qui ne sont pas hébergés de manière permanente dans des Installations d'hébergement sécurisées (y compris des ordinateurs portables, des dispositifs de stockage portables ou des supports amovibles tels que des disques USB, des DVD et des cassettes).

3.3. Mesures de protection physiques et environnementales. L'accès aux zones du site du Fournisseur à partir desquelles le Service SaaS est géré et accessible doit être physiquement limité au seul Personnel autorisé et contrôlé par l'utilisation de badges d'accès. Les visiteurs et les tiers ne seront autorisés à accéder à ces zones de travail du Fournisseur qu'après avoir été dûment identifiés et autorisés.

3.4. Installations d'hébergement

3.4.1. Le Fournisseur hébergera l'équipement utilisé pour fournir les Services SaaS dans une zone physiquement sécurisée dont l'accès sera limité au personnel autorisé, ci-après dénommée " Locaux d'hébergement ". Les installations d'hébergement doivent être dotées de mesures de sécurité physique adéquates telles que, mais sans s'y limiter, des contrôles de périmètre comprenant une disposition permettant de détecter les accès non autorisés, l'enregistrement des accès, l'authentification forte, la vidéosurveillance et l'enregistrement des visiteurs.

3.4.2. Les installations d'hébergement doivent être raisonnablement protégées contre les menaces externes/environnementales telles que les incendies, les inondations ou d'autres formes de catastrophes naturelles ou causées par l'homme. Les mesures de protection comprennent des contrôles tels que des systèmes d'alarme de détection de fumée et d'incendie et/ou des systèmes automatiques d'extinction d'incendie.

3.4.3. Les infrastructures d'hébergement doivent disposer d'une protection pour les serveurs, le réseau et les autres équipements électroniques contre les problèmes liés à l'alimentation électrique.

3.4.4. Le Fournisseur doit revoir périodiquement les contrôles physiques et environnementaux afin de s'assurer qu'ils restent adéquats pour héberger l'équipement utilisé pour fournir les Services SaaS.

3.4.5. Lorsqu'un matériel ou un support n'est plus utilisé pour fournir les Services SaaS, le Fournisseur ou son sous-traitant rendra rapidement irrécupérables toutes les Données se trouvant sur ce matériel ou ce support, selon le cas.

4. Exigences en matière de protection de la vie privée

4.1. Demandes d'accès et de correction. Le Fournisseur transmettra au Client toutes les demandes d'accès ou de correction émanant des Personnes concernées (telles que définies dans l'Addenda relatif au traitement des données du Client) pour les Données à caractère personnel et coopérera raisonnablement avec le Client pour répondre à ces demandes, comme l'exige la Loi sur la protection des données applicable (telle que définie dans l'Addenda relatif au traitement des données du Client).

4.2. Notification de la violation et enquête. Dans le cas où le Fournisseur apprend que la sécurité, la confidentialité ou l'intégrité de toute Donnée a été compromise ("Violation de Données"), le Fournisseur fera des efforts commercialement raisonnables pour immédiatement, par écrit, conformément aux exigences de notification énoncées dans le Contrat, mais en aucun cas plus de deux (2) jours ouvrables (si possible) après la découverte ou la notification d'une telle Violation de Données, faire un rapport au Client et, si la loi ou la réglementation l'exige, à toute autre partie. Le Fournisseur doit également (i) enquêter rapidement et effectuer une analyse raisonnable des causes de la violation des données, (ii) dans la mesure où ces causes sont sous le contrôle du Fournisseur, développer et mettre en œuvre un plan approprié pour limiter l'effet et remédier à la cause de la violation des données ; et (iii) coopérer raisonnablement avec le Client en ce qui concerne toute enquête et/ou les efforts pour se conformer à toute notification ou autre exigence réglementaire applicable à la violation des données. Sous réserve de tout accord de confidentialité et/ou contractuel que le Fournisseur peut avoir avec d'autres parties, le Fournisseur donnera au Client toute information que le Client demande raisonnablement au sujet de l'incident.

4.3. Délégué à la protection des données. (DPD). Pour faciliter le respect de la législation applicable en matière de protection des données, le Fournisseur a engagé un délégué à la protection des données externe, indépendant et qualifié. Le DPD veille au respect par le Fournisseur de ses obligations en matière de protection des données en vertu du présent Contrat et fait office de point de contact principal du Client pour les questions relatives à la protection de la vie privée. Les coordonnées du DPD sont disponibles sur le OneSpan Privacy Center (https://www.onespan.com/privacy-center) sous "Privacy Highlights" - Data Protection Officer.

4.4. Le fournisseur a nommé un responsable de la sécurité de l'information qui supervise le respect par le fournisseur

des obligations en matière de sécurité de l'information en vertu du présent contrat et agit en tant que point de contact principal du client pour les questions de sécurité de l'information. De plus amples informations sont disponibles dans les points forts de la sécurité sur le site OneSpan Privacy Center (https://www.onespan.com/privacy-center).