ADDENDUM RELATIF À LA SÉCURITÉ

Le présent Addendum relatif à la sécurité est intégré et fait partie du contrat écrit entre insightsoftware et le Client qui fait référence au présent Document (le « **Contrat** ») et les éventuels termes débutant par une majuscule utilisés, mais non définis ici, auront la signification exposée dans le Contrat. En cas de conflit entre les conditions du Contrat et le présent Addendum relatif à la sécurité, cet Addendum relatif à la sécurité prévaudra. Le présent Addendum relatif à la sécurité expose les contrôles de sécurité et les normes gérés par insightsoftware (le « Programme de sécurité »). insightsoftware teste et évalue régulièrement son Programme de sécurité ainsi que le présent Addendum relatif à la sécurité, sous réserve toutefois, que lesdites mises à jour soient conçues pour renforcer et ne pas nuire matériellement au Programme de sécurité.

1. **Contrôles de sécurité d'entreprise d'insightsoftware.**

   a. **Contrôles administratifs.**
      i. **Équipe de sécurité des informations dédiée.** Le programme de sécurité d'insightsoftware est géré par une équipe de professionnels de la sécurité des informations, dirigée par le vice-président et le directeur de la sécurité des informations d'insightsoftware.
      ii. **Politique de sécurité**. insightsoftware gère une politique de sécurité écrite basée sur les normes 'du secteur et conforme aux lois en vigueur sur la protection des données (les « Lois sur la protection des données »). Cette politique est révisée et mise à jour chaque année et mise à la disposition de l'ensemble du personnel d'insightsoftware.
      iii. **Vérification des antécédents**. insightsoftware organise un examen des antécédents judiciaires de ses employés dans le cadre de son processus d'embauche, conformément aux lois en vigueur. Des vérifications des antécédents sont effectuées pour tous les employés dans certains pays et peuvent être réalisées sur demande dans d'autres pays.
      iv. **Formation de sensibilisation à la sécurité.** insightsoftware gère un programme documenté de formation à la sensibilisation à la sécurité pour son personnel, y compris les nouveaux employés et la formation continue.
      v. **Code de conduite ; contrats de confidentialité ; politique de sécurité des informations.** Le personnel d'insightsoftware est tenu de prendre connaissance et d'accepter plusieurs politiques et accords qui requièrent que les employés préservent la confidentialité des données clients et suivent les processus de sécurité liés aux données clients, y compris le Code de conduite d'insightsoftware, les contrats de confidentialité des employés et la politique de sécurité des informations d'insightsoftware.
      vi. **Gestion des risques et évaluation des menaces d'insightsoftware.** insightsoftware applique un processus documenté de gestion des risques. Le comité de sécurité des informations d'insightsoftware se réunit régulièrement pour examiner les rapports et les modifications matérielles intervenus dans l'environnement des menaces, identifier les déficiences de contrôle potentielles et faire des recommandations concernant de nouveaux contrôles ou des contrôles améliorés et des stratégies d'atténuation des menaces.
      vii. **Surveillance des informations sur les menaces externes.** insightsoftware examine les flux d'informations concernant les menaces externes, y compris les annonces de vulnérabilité US-Cert, les recommandations de sécurité des fournisseurs critiques et d'autres sources d'informations de confiance sur les vulnérabilités et les menaces.
      viii. **Gestion des risques concernant les fournisseurs.** insightsoftware évalue les fournisseurs qui traitent les données clients ou font partie d'une solution insightsoftware, afin de faire en sorte qu'ils appliquent des mesures de sécurité conformes aux obligations d'insightsoftware dans le présent Addendum de sécurité et conformément aux lois sur la protection des données.

   b. **Détection des incidents et réponse.**
      i. **Plan de réponse aux incidents.** insightsoftware gère un plan documenté de réponse aux incidents, lequel comprend le rapport des incidents, la réponse, les rôles et responsabilités, la hiérarchisation, la remontée et la réparation. Ce plan est régulièrement testé et mis à jour.
      ii. **Rapport des incidents de sécurité.** Si insightsoftware a connaissance d'une infraction à la sécurité entraînant une destruction, une perte, une altération, une divulgation non autorisée ou l'accès aux données clients, accidentels ou illégaux (un « incident de sécurité »), insightsoftware informera le Client sans retard indu et dans tous les cas, dans les 48 heures suivant la détermination d'un incident de sécurité qui a impacté ou impactera les données client.
      iii. **Enquête.** En cas d'incident de sécurité, insightsoftware prendra rapidement des mesures raisonnables pour contenir, enquêter et atténuer tout incident. Les éventuels journaux considérés comme pertinents pour un incident de sécurité seront conservés pendant au moins un an.

iv. **Communication et collaboration.** insightsoftware fournira au Client des informations opportunes au sujet de l'incident de sécurité dans la mesure connue d'insightsoftware, y compris, sans toutefois s'y limiter, la nature et les conséquences de l'incident de sécurité, les mesures prises et/ou proposées par insightsoftware pour atténuer ou contenir l'incident de sécurité, l'état de l'enquête d'insightsoftware et un point de contact pour obtenir des informations supplémentaires.

v. **Cyber-assurance.** insightsoftware gère une politique d'assurance Responsabilité des erreurs et omissions cyber/technologiques ayant reçu une note de catégorie alphabétique des titulaires de polices qui n'est pas inférieure à « A- » et une note de catégorie de taille financière qui ne soit pas inférieure à « VII » selon la dernière édition de l'A.M. Best's Key Rating Guide.

c. **Contrôles physiques et environnementaux des bureaux de l'entreprise insightsoftware.** Les contrôles techniques, administratifs et physiques d'insightsoftware dans ses bureaux d'entreprise couverts par sa certification ISO 27001 incluent entre autres les suivants :

i. L'accès physique aux bureaux de l'entreprise est contrôlé aux points d'entrée ;
ii. Un accès par badge est requis pour tout le personnel et les privilèges de badge sont révisés régulièrement ;
iii. Les visiteurs sont tenus de signer un registre ;
iv. Une surveillance vidéo par caméras en circuit fermé couvre les points d'entrée dans le bâtiment ;
v. Des systèmes de détection et de prévention des incendies ; et
vi. Des systèmes de contrôle de la température.

d. **Sécurité du système insightsoftware.**

i. **Protection contre les logiciels malveillants et les vulnérabilités.** Les ordinateurs portables, ordinateurs de bureau et serveurs de production d'insightsoftware sont protégés par une protection anti-malware avec mise à jour automatique et surveillance des vulnérabilités. Les e-mails, y compris les liens et pièces jointes, sont analysés à la recherche de logiciels malveillants avant d'être livrés.
ii. **Chiffrement des disques.** Les disques durs des ordinateurs portables d'insightsoftware sont chiffrés.
iii. **Application de correctifs.** Les correctifs de sécurité sont révisés et déployés au moins une fois par mois.
iv. **Élimination sécurisée.** insightsoftware suit un processus documenté pour l'élimination sécurisée des actifs qui stockent des données.
v. **Authentification multifacteurs**. L'accès à distance aux réseaux d'insightsoftware requiert une authentification multifacteurs.

e. **Développement sécurisé de logiciels.**

i. La sécurité fait partie de l'ensemble du cycle de vie de développement d'un logiciel.
ii. Les systèmes de développement sont distincts des systèmes de production.
iii. Les données clients ne sont pas transmises ni stockées dans des systèmes de développement.
iv. Le test de sécurité des applications est intégré au pipeline de développement de logiciels.
v. Un système de contrôle de code source est utilisé et authentifie et journalise la personne associée ainsi que tous les changements apportés au logiciel ou à la ligne de base du code personnalisé et à tous les fichiers de configuration et de build liés.
vi. Le code source est sauvegardé et protégé.

2. **Contrôles et garde-fous de sécurité dans le cloud.**

a. **Responsabilités de sécurité.** insightsoftware fournit son logiciel soit (i) dans les locaux, en installant le logiciel sur les ordinateurs du client, soit (ii) en tant que service hébergé, par lequel insightsoftware utilise des fournisseurs de cloud d'infrastructure en tant que service et/ou des installations de collocation sécurisées pour fournir aux Clients un accès au logiciel d'insightsoftware (« l'environnement du cloud »). En ce qui concerne le logiciel sur site d'insightsoftware, qui est installé sur les ordinateurs du Client, le Client est responsable du maintien de la sécurité des ordinateurs du Client, y compris l'ensemble des correctifs, des contrôles d'accès, des pare-feu, de la sécurité physique, des sauvegardes et du chiffrement. Lorsque le logiciel d'insightsoftware est fourni via un environnement de cloud, insightsoftware est chargé du maintien des contrôles de sécurité et des garde-fous décrits ci-dessous. insightsoftware gère un programme complet et documenté de sécurité en vertu duquel insightsoftware met en œuvre et gère des garde-fous physiques, administratifs et techniques conçus pour protéger la confidentialité, l'intégrité, la disponibilité et la sécurité du logiciel et des données clients.

b. **Audits et certifications d'insightsoftware.**

i. insightsoftware gère les audits et les certifications décrits à l'adresse https://legal.insightsoftware.com/contracts/ISO&SOC-certifications.pdf.

ii. Les rapports effectués par des auditeurs tiers indépendants sont mis à la disposition du Client sur demande.

c. **Lieu d'hébergement des données client.** insightsoftware utilise des organismes de sous-services dont les contrôles sont évalués par des audits SOC 2 pour vérifier qu'ils sont correctement conçus et opérés pour se conformer aux exigences de sécurité d'insightsoftware.

d. **Chiffrement.**
   i. **Chiffrement au repos**. Les données client résidant dans l'environnement du cloud sont chiffrées au repos.
   ii. **Gestion des clés de chiffrement.** Toutes les données cryptographiques sont protégées contre la divulgation ou l'utilisation non autorisées.
      1. Les clés de chiffrement sont créées conformément aux recommandations de puissance standard 'du secteur alors en cours.
      2. Toute clé devenue faible en raison d'algorithmes obsolètes ou soupçonnée d'être compromise est retirée et/ou remplacée par une clé mise à jour.
      3. Des certificats sont utilisés pour chiffrer les clés utilisées pour chiffrer les données.
   iii. **Chiffrement en transit.** Des protocoles sécurisés de transmission des données sont utilisés pour chiffrer les données confidentielles lors de leur transmission sur des réseaux publics.

e. **Sécurité du système et du réseau.**
   i. **Contrôles d'accès.** Tous les accès du personnel d'insightsoftware à l'environnement du cloud se font via un identifiant d'utilisateur unique avec un mot de passe complexe et une authentification multifacteurs. L'accès aux systèmes et aux données est fourni à ceux qui en ont besoin pour remplir leurs fonctions professionnelles et cohérent avec le principe du moindre privilège.
   ii. **Séparation des environnements.** insightsoftware sépare logiquement les environnements de production de environnements de développement et de test. L'environnement de cloud est séparé logiquement et physiquement des bureaux et réseaux d'insightsoftware.
   iii. **Gestion des changements.** insightsoftware gère un programme documenté de gestion des changements pour son logiciel.
   iv. **Pare-feu/Groupes de sécurité.** L'environnement de cloud d'insightsoftware utilise un pare-feu aux normes 'du secteur ou une technologie de groupes de sécurité avec des politiques par défaut de refus systématique pour accepter uniquement les protocoles de trafic réseau nécessaires à l'activité et protéger les systèmes contre les réseaux non fiables.
   v. **Révision des accès du personnel et des cessations d'emploi.** insightsoftware révise les privilèges d'accès de son personnel à l'environnement du cloud au moins une fois par trimestre et supprime rapidement l'accès de tous les membres du personnel qui quittent l'entreprise.
   vi. **Durcissement.** L'environnement du cloud est endurci à l'aide de pratiques standard 'du secteur pour le protéger des vulnérabilités, y compris en modifiant les mots de passe par défaut, en supprimant les logiciels inutiles, en désactivant ou en supprimant les services qui ne sont plus nécessaires et en appliquant régulièrement des correctifs comme décrit dans le présent Addendum de sécurité.
   vii. **Application de correctifs.** Les correctifs de sécurité sont révisés et appliqués aux systèmes à intervalles réguliers, conformément aux politiques et normes établies.
   viii. **Surveillance et journalisation.** Des outils et services de surveillance sont utilisés pour journaliser des activités et des changements spécifiques dans l'environnement du cloud. Ces journaux sont davantage surveillés et analysés à la recherche d'anomalies si nécessaire. Les journaux sont stockés en toute sécurité pour empêcher les manipulations.
   ix. **Protection des terminaisons.** L'environnement du cloud utilise des outils de détection des menaces à mise à jour automatique pour surveiller et fournir une protection contre les activités suspectes et les logiciels malveillants (ensemble, les « activités malveillantes ») sur les terminaisons concernées. insightsoftware ne surveille pas les données clients à la recherche d'activités malveillantes.
   x. **Gestion des vulnérabilités.** Les systèmes présents dans l'environnement du cloud sont automatiquement évalués à la recherche de vulnérabilités, lesquelles sont ensuite hiérarchisées en vue d'une résolution basée sur leur impact potentiel sur le logiciel d'insightsoftware.
   xi. **Tests de pénétration**. insightsoftware engage un ou plusieurs tiers indépendants pour réaliser des tests de pénétration de logiciels sélectionnés au moins une fois par an. Sur demande écrite du client, insightsoftware fournira au client un résumé exécutif de tout test de pénétration de ce type.

f. **Contrôles physiques et environnementaux du centre de données du cloud.** Pour faire en sorte que l'environnement du cloud dispose de contrôles physiques et environnementaux pour les centres de données hébergeant le logiciel, insightsoftware examine régulièrement les contrôles de sécurité de l'environnement du cloud audités dans le cadre

d'audits et de certifications par des tiers indépendants. Chaque fournisseur d'environnement de cloud dispose d'une certification d'audit annuel SOC 2 de type II et d'une certification ISO 27001, ou d'une infrastructure équivalente reconnue par 'le secteur. Ces contrôles comprennent, sans toutefois s'y limiter, les suivants :

i. L'accès physique aux installations et aux systèmes physiques est contrôlé ;
ii. Les privilèges d'accès physiques sont régulièrement révisés ;
iii. Les visiteurs sont tenus de présenter une pièce d'identité et de signer un registre ;
iv. Une surveillance vidéo par caméras en circuit fermé couvre les points d'accès ;
v. Des systèmes de détection et de prévention des incendies ;
vi. Une alimentation de secours et des systèmes redondants ;
vii. Des systèmes de contrôle de la température ; et
viii. Des processus conformes NIST 800-88 établis pour mettre hors service des actifs matériels.

g. **Suppression des données clients par insightsoftware.** Sous réserve des dispositions applicables du Contrat, lors de la survenue du dernier événement entre (i) l'expiration ou la résiliation du Contrat et (ii) l'expiration de toute « période de récupération » post-résiliation définie dans le Contrat, insightsoftware supprime rapidement les éventuelles données client restantes.

h. **Continuité de l'activité et reprise après sinistre.** Des systèmes de sauvegarde automatisés procèdent à des sauvegardes planifiées des bases de données de production. Pour le logiciel au sujet duquel insightsoftware organise des audits, un plan de continuité de l'activité et de reprise après sinistre est mis en place pour assurer la reprise des opérations et des service urgents en cas d'événement catastrophique qui cause une interruption majeure de l'activité. Le plan de continuité de l'activité et de reprise après sinistre contient des responsabilités détaillées et des tâches spécifiques pour les activités de réponse d'urgence et les opérations de reprise de l'activité basées sur des plages de temps prédéfinies. Le plan est révisé et testé annuellement afin de valider le caractère approprié des procédures documentées et de faire en sorte que le personnel comprenne le plan et le rôle qu'il joue dans l'exécution du plan.

3. **Droits d'audit du client.** Sur demande écrite et sans frais supplémentaires pour le client, insightsoftware fournira au client et/ou à son représentant tiers correctement qualifié (collectivement « l'Auditeur »), un accès à la documentation raisonnablement demandée prouvant la conformité d'insightsoftware à ses obligations en vertu du présent Addendum de sécurité sous forme, selon le cas, de (i) certification ISO 27001 d'insightsoftware, (ii) rapport d'audit SOC 2 de Type II d'insightsoftware et/ou rapport d'audit SOC 2 de Type II et/ou rapport d'audit SOC 1 de Type II, (iii) du questionnaire de recueil d'informations standardisé (SIG) sur les évaluations partagées d'insightsoftware rempli le plus récemment et (iv) du rapport récapitulatif de test de pénétration le plus récent pour le logiciel concerné (les « Rapports d'audit »). Au cas où insightsoftware ne serait pas en mesure de fournir un rapport d'audit, insightsoftware accepte de remplir tout questionnaire de sécurité des informations fourni par le client chaque année dans un délai de six (6) semaines suivant la demande écrite du client. Lorsque l'Auditeur est un tiers, ledit tiers pourra être invité à signer un contrat de confidentialité distinct avec insightsoftware avant toute révision des Rapports d'audit et insightsoftware pourra s'opposer par écrit à tout tiers si, selon l'opinion raisonnable d'insightsoftware, ledit tiers n'est pas correctement qualifié ou est un concurrent direct d'insightsoftware. Toute objection raisonnable de ce type par insightsoftware exigera que le client désigne un autre tiers. Les éventuels frais encourus par un Auditeur en relation avec tout examen de rapports d'audit ou avec un questionnaire fourni par le client seront à la charge exclusive de l'Auditeur.