Addendum relatif au traitement des données

Le présent Addendum relatif au traitement des données (ci-après dénommé « **Addendum** ») prend effet à la Date d'entrée en vigueur de l'Addendum et fait partie de l'accord (ci-après dénommé « **Accord** ») entre le Client et Kyriba (chacun dénommé une « **Partie** » ou collectivement les « **Parties** ») pour la fourniture des services SaaS. Le présent Addendum expose l'accord des Parties en ce qui concerne le traitement des Données à caractère personnel du Client et remplace et annule toute disposition existante concernant les Données à caractère personnel du Client dans l'Accord ou autre.

1. **Définitions ; Construction.**
   a. **« Date d'entrée en vigueur de l'addendum »** désigne la date d'entrée en vigueur de l'Accord et restera en vigueur tant que l'Accord restera en vigueur.
   b. **« Anonymisé »** signifie l'élimination et le masquage des Données à caractère personnel du Client, en utilisant l'obfuscation et des algorithmes cryptographiques de hachage non réversibles, de sorte que les données ne permettent en aucun cas d'identifier ou d'être relié à une personne.
   c. « **Droit applicable en matière de protection des données** » désigne, si et dans la mesure où elle est applicable, (a) la loi britannique sur la protection des données de 2018 et le RGPD de l'UE, tel qu'il fait partie de la loi européenne conservée au Royaume-Uni (« UK GDPR ») ; (b) le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des Données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/EC (« **Règlement général sur la protection des données** » ou « **RGPD** ») ; (c) les lois sur la protection des données aux États-Unis, y compris, mais sans s'y limiter, la loi californienne de 2018 sur la protection de la vie privée des consommateurs, § 1798.100 et suivants du California Civil Code, telle que modifiée par la loi californienne de 2020 sur les droits à la vie privée, et les règlements qui en découlent (collectivement les « **Lois américaines sur la protection des données** ») ; et (d) toute autre loi, règle, règlement, directive d'autorégulation ou législation d'application en matière de protection des données applicable aux services SaaS et au traitement par Kyriba des Données à caractère personnel du Client.
   d. **« Données à caractère personnel du Client »** désigne les informations personnelles qui peuvent être fournies par le Client à Kyriba et qui comprennent des informations identifiant, concernant, décrivant, pouvant raisonnablement être associées ou pouvant raisonnablement être liées, directement ou indirectement, à un individu, un consommateur, une personne concernée ou un ménage particulier, ou qui sont définies comme des « informations identifiables personnellement », des « informations personnelles », des « données à caractère personnel » ou un terme similaire en vertu du Droit applicable en matière de protection des données.
   e. **« Traitement »**, **« traité »** ou **« traiter »** a la même signification que celle énoncée dans le Droit applicable en matière de protection des données.
   f. « **Sous-traitant** » désigne tout sous-traitant (y compris tout tiers et toute société affiliée à Kyriba, mais à l'exclusion d'un employé de Kyriba) nommé par ou pour le compte de Kyriba ou pour traiter les Données à caractère personnel du Client.
   g. Les mots et expressions figurant dans le présent Addendum ont, dans la mesure du possible, la signification qui leur est donnée dans le Droit applicable en matière de protection des données.
   h. Tous les termes en majuscules qui ne sont pas définis dans le présent Addendum ont la signification qui leur est donnée dans l'Accord.
   i. En cas d'incompatibilité entre l'Accord et les dispositions de l'Addendum, les Parties conviennent que les dispositions du présent Addendum prévaudront.

2. **Relation entre les Parties.**
   a. Le Client est le « Responsable de Traitement » ou l'entreprise qui détermine la finalité et la manière dont les Données à caractère personnel du Client sont traitées par Kyriba. Le contrôle et la responsabilité des Données à caractère personnel du Client restent à tout moment entre les mains du Client.
   b. Kyriba est le « Sous-traitant » ou le prestataire de services qui traite les Données à caractère personnel du Client conformément aux instructions documentées du Client.

3. Obligations générales du Sous-traitant.

a. Kyriba traitera les Données à caractère personnel du Client conformément au Droit applicable en matière de protection des données et uniquement dans le but de fournir les services SaaS au Client. Kyriba (i) ne traitera pas les Données à caractère personnel du Client à des fins autres que celles énoncées dans le présent Addendum, comme requis par les instructions documentées du Client, ou comme requis par le droit applicable ; (ii) ne divulguera pas les Données à caractère personnel du Client à des tiers autres que les sociétés affiliées ou filiales de Kyriba, aux fins susmentionnées ou comme requis par la loi ; (iii) ne vendra pas, ne louera pas, ne publiera pas, ne divulguera pas, ne disséminera pas, ne mettra pas à disposition, ne transférera pas ou ne communiquera pas de toute autre manière les Données à caractère personnel du Client à un tiers pour une contrepartie monétaire ou toute autre contrepartie de valeur ; ou (iv) ne conservera pas, n'utilisera pas ou ne divulguera pas les Données à caractère personnel du Client en dehors de la relation commerciale entre Kyriba et le Client.

b. Kyriba ne doit pas combiner les Données à caractère personnel du Client que Kyriba reçoit de la part du Client, ou pour le compte du Client, avec des informations personnelles qu'elle reçoit d'une autre personne, ou pour le compte d'une autre personne, ou qu'elle collecte à partir de sa propre interaction avec un individu, à condition que Kyriba puisse combiner des informations personnelles pour réaliser tout objectif commercial tel que défini par le Droit applicable en matière de protection des données.

c. Si Kyriba doit traiter les Données à caractère personnel du Client comme l'exige le droit applicable aux services SaaS, Kyriba informera le Client de cette exigence légale avant de traiter les Données à caractère personnel du Client, à moins que la loi n'interdise une telle divulgation.

d. La finalité et la durée du Traitement, sa nature, le type de Données à caractère personnel du Client faisant l'objet du Traitement et les catégories de personnes concernées sont précisées dans la pièce jointe 1 - Programme de traitement des données joint aux présentes et incorporé aux présentes (« Pièce jointe 1 »).

e. Kyriba certifie qu'elle comprend et respectera les obligations de Traitement énoncées dans le présent Addendum.

4. Obligations générales du Responsable de Traitement.

a. Le Client est seul responsable de l'exactitude, de la qualité et de la légalité des Données à caractère personnel du Client.

b. Le Client s'est conformé et continuera de se conformer à l'ensemble du Droit applicable en matière de protection des données.

c. Le Client dispose de l'autorité, de la licence ou du consentement nécessaires pour fournir les Données à caractère personnel du Client et dispose d'une base légale (y compris tous les avis et consentements légalement requis), s'est conformé (et continuera de se conformer) à l'ensemble du droit applicable en matière de protection des données, en particulier pour le partage, la transmission et le traitement des Données à caractère personnel du Client avec, vers et par Kyriba aux fins des services SaaS et de l'Accord.

d. Le Client certifie que le traitement par Kyriba des Données à caractère personnel du Client conformément aux instructions documentées du Client et au présent Addendum n'entraînera pas la violation par Kyriba du Droit applicable en matière de protection des données.

e. Le Client a, et continue d'avoir, le droit de transférer ou de donner accès aux Données à caractère personnel du Client à Kyriba pour réception, transfert et Traitement conformément au présent Addendum.

f. Le Client a entrepris, et continuera à entreprendre, comme l'exige le Droit applicable en matière de protection des données, toutes les évaluations d'impact sur la protection des données ou les évaluations de sécurité pour faciliter le transfert des Données à caractère personnel du Client à Kyriba (que ce soit à l'intérieur ou l'extérieur du pays où les Données à caractère personnel du Client ont été collectées en premier lieu). Nonobstant ce qui précède et dans tous les cas, rien n'interdit à Kyriba d'accéder, de recevoir, de stocker, d'utiliser ou de traiter de toute autre manière les Données à caractère personnel du Client en dehors du pays de réception conformément aux termes du présent Addendum.

g. Le Client doit immédiatement notifier à Kyriba toutes les plaintes, réclamations, enquêtes ou demandes de renseignements émanant de tout organisme de réglementation qui pourraient se rapporter ou impliquer les Données à caractère personnel du Client que Kyriba traite.

h. Le cas échéant, le Client ne transférera ni ne divulguera aucune donnée à caractère personnel du Client contenant des « secrets d'État » ou des « données importantes » tels que définis par le droit applicable

en matière de protection des données, ou dont il est par ailleurs interdit de quitter le pays de transfert en vertu du droit applicable en matière de protection des données.

5. Conformité avec l'article 28 du RGPD.

a. Dans le cas où les Données à caractère personnel du Client concernent des personnes de l'UE ou du Royaume-Uni, Kyriba se conformera aux exigences énoncées à l'article 28 du RGPD ou du UK GDPR, selon le cas, et à la description du Traitement décrite dans la pièce jointe 1.

b. Kyriba (i) s'assurera que les employés de Kyriba autorisés à traiter les Données à caractère personnel du Client en vertu du présent Addendum sont liés par des conditions de confidentialité similaires à celles de l'Accord ou à l'obligation légale de confidentialité appropriée, (ii) compte tenu de l'état de la technique, des coûts de mise en œuvre, ainsi que de la nature, la portée, le contexte et les objectifs du Traitement, maintiendra des mesures de sécurité raisonnables et des mesures techniques et organisationnelles appropriées visées à l'article 32 du RGPD pour la protection, la confidentialité et l'intégrité des Données à caractère personnel du Client, (iii) contrôlera régulièrement la conformité à ces mesures, et ne diminuera pas matériellement la sécurité globale des services SaaS pendant sa fourniture des services SaaS conformément à l'Accord, (iv) dans la mesure où cela est légalement autorisé, informera rapidement le Client si Kyriba reçoit une demande d'un individu, d'un consommateur ou d'une personne concernée pour exercer ses droits en vertu du Droit applicable en matière de protection des données ou reçoit une demande ou une plainte d'un organisme de contrôle ou d'un autre tiers (« **Demande** »), (v) compte tenu de la nature du traitement, assistera le Client par des mesures techniques et organisationnelles appropriées, dans la mesure où cela est possible, pour l'accomplissement de l'obligation du Client de répondre aux demandes d'exercice des droits de l'individu, du consommateur ou de la personne concernée, et ne répondra pas à ces demandes, sauf si cela est nécessaire pour se conformer au Droit applicable en matière de protection des données, et (vi) sur demande écrite du Client, et sous réserve de la section 6.3 (données Client) de l'accord, supprimera ou restituera toutes les Données à caractère personnel du Client au Client dans les soixante (60) jours suivant la résiliation de l'Accord pour quelque raison que ce soit ou si les Données à caractère personnel du Client ne sont plus nécessaires pour exécuter les services SaaS ; toutefois, Kyriba peut conserver les Données à caractère personnel du Client lorsque cela est nécessaire pour que Kyriba se conforme au droit applicable ou à une obligation légale, ou aux droits de Kyriba.

6. Vérifications de la conformité.

a. Kyriba mettra à la disposition du Client toutes les informations raisonnablement nécessaires pour démontrer le respect des obligations fixées dans le présent Addendum au Client et permettra, dans la mesure où la loi l'exige, la contribution aux audits, y compris les inspections menées par le Client ou un autre auditeur mandaté par le Client.

b. Cet auditeur devra être lié par des engagements de confidentialité au moins aussi stricts que ceux prévus dans l'Accord. Dans l'éventualité d'une révision demandée, le Client devra donner à Kyriba un préavis raisonnable indiquant que les révisions seront effectuées en dehors des locaux, sous réserve des politiques de Kyriba, et ne devront pas interférer ou perturber de manière déraisonnable les activités commerciales de Kyriba. Les audits ont lieu dans les heures normales de bureau, sauf si un organisme de réglementation exige que la révision soit effectuée en urgence.

c. Dans la mesure où la loi le permet, le Client sera responsable de tous les coûts raisonnables et démontrables découlant de la fourniture d'une assistance par Kyriba, qui vont au-delà de ceux requis par la loi et conformément à la présente sous-section (c). Tous les rapports susmentionnés constituent des informations confidentielles des Parties.

7. Transferts ultérieurs.

a. Le Client reconnaît et accepte que les Données à caractère personnel du Client puissent être transférées en dehors des pays de l'Union européenne, de l'Espace économique européen, du Royaume-Uni ou d'autres territoires d'où proviennent les Données à caractère personnel du Client (« **Transferts ultérieurs** »), vers des pays reconnus par la Commission européenne, ou l'*Information Commissioner's Office UK* (« **ICO** »), ou d'autres territoires le cas échéant, comme des pays où il existe un niveau de protection adéquat mis à jour de temps à autre (« **Lieu autorisé** »).

b. Pendant la durée de l'Accord, les Parties, ou Kyriba et ses Sous-traitants ultérieurs, le cas échéant, doivent se conformer aux termes et conditions des Clauses contractuelles types (Module 2 -

Responsable de Traitement vers Sous-traitant ou Module 3 - Sous-traitant vers Sous-traitant ultérieurs) telles que définies dans la décision de la Commission du 4 juin 2021 (2021/91), telles qu'elles peuvent être modifiées, mises à jour, substituées ou remplacées de temps à autre (« **Clauses contractuelles types de l'UE** »), ou une forme équivalente aux Clauses contractuelles types, telles qu'approuvées par l'ICO, de temps à autre, pour l'exportation des Données à caractère personnel du Client des personnes concernées du Royaume-Uni (« **Addendum aux Clauses contractuelles types du Royaume-Uni** ») pour ces transferts ultérieurs.

c. Si le Client accepte un transfert ultérieur, ce transfert ultérieur sera soumis, le cas échéant, aux Clauses contractuelles types de l'UE, à l'Addendum aux clauses contractuelles types du Royaume-Uni ou à tout autre moyen alternatif validé par le Droit applicable en matière de protection des données, qui seront tous intégrés par référence et considérés comme exécutés du fait de la signature de chaque Partie sur l'Accord. Les clauses applicables sont disponibles sur : Clauses contractuelles types de l'UE [[Anglais]www.kyriba.com/contracts/eusccs / [[Français]www.kyriba.com/contracts/uecct] et Addendum aux Clauses contractuelles types du Royaume-Uni [www.kyriba.com/contracts/dpa/uksccs].

d. Les détails des transferts ultérieurs requis par les Clauses contractuelles types de l'UE et les Clauses contractuelles types du Royaume-Uni sont présentés dans la pièce jointe 2 - Annexe aux Clauses contractuelles types jointe aux présentes et intégrée aux présentes.

8. Sous-traitants.

a. Kyriba fait appel à des Sous-traitants ultérieurs pour mener à bien des activités de traitement spécifiques, telles que l'hébergement ou la maintenance. Les Sous-traitants ultérieurs utilisés à la date du présent Addendum sont précisés dans la pièce jointe sur la protection des données. En outre, le Client fournit une autorisation écrite générale à Kyriba pour engager un autre sous-traitant ultérieur dans le cadre de l'utilisation des services SaaS par le Client.

b. Changements de Sous-traitants ultérieurs. Si Kyriba souhaite remplacer l'un de ses sous-traitants ultérieurs existants ou engager un nouveau sous-traitant ultérieur (« **Changement** »), conformément à ce qui suit :

i. Kyriba informera le Client à l'avance de tout changement proposé en rapport avec l'utilisation des services SaaS par le Client ; donnant ainsi au Client la possibilité de s'opposer à un tel Changement. Le Client dispose d'un délai de sept (7) jours ouvrés à compter de la date de réception de ces informations pour s'opposer expressément au Changement pour des motifs raisonnables en envoyant une notification à Kyriba. Cette notification doit exposer les raisons de cette objection. Dans le cas où le Client envoie une notification s'opposant au nouveau sous-traitant ultérieur, les Parties chercheront à résoudre le problème par un accord mutuellement acceptable.

ii. Kyriba déploiera des efforts commercialement raisonnables pour mettre à la disposition du Client un changement des services SaaS ou de leur configuration par le Client afin d'éviter le traitement des Données à caractère personnel du Client par le nouveau sous-traitant ultérieur auquel il s'oppose.

iii. Si cinq (5) jours avant la date d'entrée en vigueur du Changement, les Parties n'ont pas réussi à s'entendre, le Client aura le droit de résilier l'Accord avec effet à la date d'entrée en vigueur du Changement.

iv. Si le Client ne résilie pas l'Accord conformément à la présente section, le Client sera considéré comme ayant accepté le Changement. Ce droit de résiliation est le seul et unique recours du Client si celui-ci s'oppose à tout nouveau sous-traitant ultérieur.

v. Kyriba signera un accord écrit avec tout sous-traitant ultérieur qu'elle engage afin de s'assurer que ledit sous-traitant ultérieur respecte les dispositions de la présente section et satisfait aux exigences prévues par le Droit applicable en matière de protection des données. Kyriba restera responsable du respect des conditions de la présente section par tout sous-traitant ultérieur.

9. Violation de la sécurité des informations. Kyriba applique des politiques et des procédures de gestion des incidents de sécurité, et en cas d'apparition de toute violation réelle de la sécurité affectant les Données à caractère personnel du Client transmises, stockées ou traitées par Kyriba, (la « **Violation de la sécurité des informations** »), Kyriba : notifiera au Client, sans délai excessif après en avoir pris connaissance, la Violation de la sécurité des informations, et remettra au Client un rapport écrit concernant la nature de la violation de la sécurité des informations, les catégories et le nombre approximatif de Données à caractère personnel

du Client affectées, si ces informations sont disponibles. Kyriba doit également, dans la mesure du possible, décrire les conséquences probables de la Violation de la sécurité des informations sur les Données à caractère personnel du Client ainsi que les mesures raisonnables que Kyriba juge nécessaires et raisonnables pour remédier à la cause de cette Violation de la sécurité des informations, dans la mesure où la remédiation est sous le contrôle raisonnable de Kyriba, y compris, le cas échéant, pour atténuer ses éventuels effets négatifs ; et procéder aussi rapidement que raisonnablement possible (i) à l'atténuation de tout impact négatif ou autre préjudice pour le Client et tout individu, consommateur et personne concernée affectés résultant de cette Violation de la sécurité des informations ; et (ii) à la prévention de Violations de la sécurité des informations similaires à l'avenir. Kyriba tiendra le Client pleinement informé de toutes les étapes de son enquête et de toutes les mesures prises à la suite de celle-ci.

10. **Violation de la sécurité des informations.** Kyriba applique des politiques et des procédures de gestion des incidents de sécurité, et en cas d'apparition de toute violation réelle de la sécurité affectant les Données à caractère personnel du Client qui déclencherait des obligations de notification aux organismes de réglementation ou aux individus en vertu du Droit applicable en matière de protection des données (la « **Violation de la sécurité des informations** »), Kyriba en informera le Client dans les meilleurs délais, après en avoir pris connaissance. Dans la mesure où Kyriba en a connaissance, Kyriba doit également, dans la mesure du possible, décrire les conséquences probables de la Violation de la sécurité des informations sur les Données à caractère personnel du Client, ainsi que les mesures raisonnables que Kyriba juge nécessaires et raisonnables pour remédier à la cause de cette Violation de la sécurité des informations, dans la mesure où la remédiation est sous le contrôle raisonnable de Kyriba, y compris, le cas échéant, pour atténuer ses éventuels effets négatifs ; et procéder dans les meilleurs délais (i) à l'atténuation de tout impact négatif ou autre préjudice pour le Client et tout individu, consommateur et personne concernée affectés résultant de cette Violation de la sécurité des informations ; et (ii) à la prévention de violations de la sécurité des informations similaires à l'avenir. Dans la mesure où Kyriba en est raisonnablement capable, Kyriba tiendra le Client pleinement informé de toutes les étapes de son enquête et de toutes les mesures prises à la suite de celle-ci.

11. **Agrégation de données.** Nonobstant toute disposition contraire et dans la mesure où les Données à caractère personnel du Client sont Anonymisées, Kyriba peut surveiller, collecter et utiliser ces informations à des fins commerciales conformément au Droit applicable en matière de protection des données, y compris, mais sans s'y limiter, le développement d'analyses, et peut conserver, utiliser et divulguer ces informations à ces fins, sans restriction.

PIÈCE JOINTE 1 - PROGRAMME DE TRAITEMENT DES DONNÉES

Ce programme de Traitement des données fait partie de l'Addendum et détaille les caractéristiques du Traitement des Données à caractère personnel du Client.

1. Description du traitement

Type de Données à caractère personnel du Client	Catégories d'individus, de consommateurs ou de personnes concernées	Finalité du Traitement	Durée du Traitement
Déterminées et contrôlées par le Client, à la discrétion du Client ; et peut inclure, sans s'y limiter, le nom, l'adresse e-mail, le numéro de téléphone, l'adresse IP, l'identifiant publicitaire, le nom d'utilisateur et le mot de passe, et les comptes financiers	Les employés, les représentants, les sous-traitants, les partenaires, les fournisseurs, les personnes d'intérêt ou les clients du Client	Fourniture de services SaaS dans le cadre de l'Accord	La durée du traitement correspond à la durée de l'Accord, sauf si le droit applicable ou une obligation légale l'exige ou si Kyriba protège ses droits.

2. Sous-traitants ultérieurs

Veuillez consulter la pièce jointe 2, annexe III ci-dessous.

Il est entendu que Kyriba peut changer, remplacer ou ajouter des sous-traitants ultérieurs conformément à la section 7 de l'Addendum.

PIÈCE JOINTE 2 - ANNEXE AUX CLAUSES CONTRACTUELLES TYPES

NOTE EXPLICATIVE :
Il doit être possible de distinguer clairement les informations applicables à chaque transfert ou catégorie de transferts et, à cet égard, de déterminer le(s) rôle(s) respectif(s) des Parties en tant qu'exportateur(s) de données ou importateur(s) de données. Cela ne nécessite pas nécessairement de remplir et de signer des annexes distinctes pour chaque transfert/catégorie de transferts ou relation contractuelle, lorsque cette transparence peut être obtenue au moyen d'une seule annexe. Toutefois, lorsque cela s'avère nécessaire pour garantir une clarté suffisante, des annexes distinctes doivent être utilisées.

kyriba

ANNEXE I

A. LISTE DES PARTIES

MODULE DEUX : Transfert du Responsable de Traitement au Sous-traitant
MODULE TROIS : Transfert du Sous-traitant au Sous-traitant ultérieur

Exportateur(s) de données : [*Identité et coordonnées du ou des exportateurs de données et, le cas échéant, de leur(s) délégué(s) à la protection des données ou de leur(s) représentant(s) dans l'Union européenne]*

- **Nom :** Le Client identifié dans l'Accord et/ou l'affilié de Kyriba, si applicable, tel qu'identifié dans l'Accord.

Importateur(s) de données : [*Identité et coordonnées du ou des importateurs de données, y compris toute personne-ressource responsable de la protection des données]*

- **Nom** : KYRIBA Corp.
- **Adresse** : 4435 Eastgate Mall, Suite 200, San Diego, California 92121 **Nom, fonction et coordonnées de la personne-ressource** : Équipe Kyriba chargée de la confidentialité des données : (privacy@kyriba.com)
- **Activités relatives aux données transférées en vertu des présentes clauses** : Kyriba est une société américaine et internationale avec ses filiales, qui fournit une solution de gestion de trésorerie et de liquidités sur la base d'un logiciel en tant que service et des services associés de support, de maintenance, de mise en œuvre et de formation
- **Rôle** Sous-traitant

Importateur de données :
KYRIBA CORP.
KYRIBA SEA PTE LTD
KYRIBA SOFTWARE TECHNOLOGY (SHANGHAI) LIMITED
KYRIBA (CHONGQING) SOFTWARE DEVELOPMENT CO.
KYRIBA HK LIMITED
KYRIBA JAPAN CO., LTD
RIM TEC, INC.

B. DESCRIPTION DU TRANSFERT

MODULE DEUX : Transfert du Responsable de Traitement au Sous-traitant
MODULE TROIS : Transfert du Sous-traitant au Sous-traitant ultérieur

Catégories de personnes dont les données à caractère personnel sont transférées

Les employés, les représentants, les sous-traitants, les partenaires, les fournisseurs, les personnes d'intérêt ou les clients du Client

Catégories de données à caractère personnel transférées

Déterminées et contrôlées par le Client, à la discrétion du Client ; et peut inclure, sans s'y limiter, le nom, l'adresse e-mail, le numéro de téléphone, l'adresse IP, l'identifiant publicitaire, le nom d'utilisateur et le mot de passe, et les comptes financiers.

Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, par exemple une stricte limitation de la finalité, des restrictions d'accès (y compris l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre des accès aux données, des restrictions pour les transferts ultérieurs ou des mesures de sécurité supplémentaires.

N/A

La fréquence du transfert (par exemple, si les données sont transférées de manière ponctuelle ou continue).

Le transfert est continu.

Nature du Traitement

Collecte, stockage, suppression, modification, transfert et autres traitements tels que définis dans l'accord entre l'exportateur de données et l'importateur de données ou la société affiliée de l'importateur pour la fourniture du logiciel de gestion de trésorerie et de liquidités en ligne de l'importateur de données en tant que service, et des services connexes de support, de maintenance, de mise en œuvre et de formation.

Finalité(s) du transfert et du Traitement ultérieur des données

Fourniture du logiciel de gestion de trésorerie et de liquidités en ligne de l'importateur de données en tant que service, et services connexes de support, de maintenance, de mise en œuvre et de formation.

La période pendant laquelle les données à caractère personnel seront conservées ou, si cela n'est pas possible, le critère utilisé pour déterminer cette période

La durée du Traitement correspond à la durée de l'Accord, sauf si le droit applicable ou une obligation légale l'exige ou si Kyriba protège ses droits.

Pour les transferts vers des sous-traitants ultérieurs ou des Sous-traitants , préciser également l'objet, la nature et la durée du traitement

Lorsqu'il s'agit de sous-traitants ultérieurs (voir la liste fournie), le transfert est limité au transfert nécessaire à l'exécution de l'Accord, et ce pendant toute sa durée.

C. ORGANISME DE CONTRÔLE COMPÉTENT

MODULE DEUX : Transfert du Responsable de Traitement au Sous-traitant
MODULE TROIS : Transfert du Sous-traitant au Sous-traitant ultérieurs

Identifier l'organisme ou les organismes de contrôle compétents conformément à la clause 13

Autorité française des données - CNIL

kyriba

ANNEXE II - MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR LA SÉCURITÉ DES DONNÉES

MODULE DEUX : Transfert du Responsable de Traitement au Sous-traitant
MODULE TROIS : Transfert du Sous-traitant au Sous-traitant ultérieur

NOTE EXPLICATIVE :
Les mesures techniques et organisationnelles doivent être décrites en termes spécifiques (et non génériques). Voir également le commentaire général sur la première page de l'annexe, en particulier sur la nécessité d'indiquer clairement quelles mesures s'appliquent à chaque transfert/ensemble de transferts.

Description des mesures techniques et organisationnelles mises en œuvre par le ou les importateurs de données (y compris toute certification pertinente) pour garantir un niveau de sécurité, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

[Exemples de mesures possibles :

- *Mesures de pseudonymisation et de cryptage des données à caractère personnel*
- *Mesures visant à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement*
- *Mesures visant à garantir la capacité de rétablir la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique*
- *Processus permettant de tester, d'évaluer et de mesurer régulièrement l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement*
- *Mesures d'identification et d'autorisation des utilisateurs*
- *Mesures de protection des données pendant la transmission*
- *Mesures de protection des données pendant le stockage*
- *Mesures visant à garantir la sécurité physique des lieux où sont traitées les données à caractère personnel*
- *Mesures visant à garantir l'enregistrement des événements*
- *Mesures visant à garantir la configuration du système, y compris la configuration par défaut*
- *Mesures relatives à la gouvernance et à la gestion de l'informatique interne et de la sécurité informatique*
- *Mesures pour la certification/assurance des processus et des produits*
- *Mesures visant à garantir la minimisation des données*
- *Mesures visant à garantir la qualité des données*
- *Mesures visant à garantir une conservation limitée des données*
- *Mesures visant à garantir la responsabilité*
- *Mesures visant à permettre la portabilité des données et à garantir leur effacement]*

Pour les transferts vers des sous-traitants ultérieurs ou des Sous-traitants, décrivez également les mesures techniques et organisationnelles spécifiques que le sous-traitant ultérieur (ou le Sous-traitant) doit prendre pour pouvoir fournir une assistance au Responsable de Traitement et, pour les transferts d'un Sous-traitant vers un sous-traitant ultérieur, à l'exportateur de données.

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par l'importateur de données conformément aux clauses 4(d) et 5(c) (ou document/législation joint) :

La plateforme SaaS de Kyriba est auditée par un cabinet comptable tiers réputé sur une base semestrielle pour s'assurer qu'elle répond à la norme Statement for Attestation Engagement No. 18 (SSAE 18)/Service Organization Control (SOC) 1 et sur une base annuelle pour s'assurer qu'elle répond aux normes SOC2, pour tous les services fournis à l'exception de FireApps. La certification SOC 2 Type II, définie par l'American Institute of Certified Public Accountants (AICPA), est reconnue dans le monde entier comme l'une des normes d'audit les plus strictes pour les prestataires de services. Cette certification a été conçue pour répondre aux besoins du nombre croissant de sociétés d'informatique et de cloud computing. Elle permet à l'organisation auditée de démontrer qu'elle respecte et dépasse les normes reconnues du secteur en matière de contrôle et de protection de toutes les données hébergées et traitées, pour le compte des clients de Kyriba.

Kyriba est également certifiée ISO27001.

Kyriba dispose d'un cadre de gestion des risques fondé sur les bonnes pratiques, qui gère les risques liés à la sécurité en décrivant le cycle de vie de la gestion des risques liés à la sécurité et définit les exigences en matière de compréhension, d'évaluation, de réponse et de surveillance des risques liés à la sécurité chez Kyriba.

La méthodologie d'évaluation des risques de Kyriba est basée sur :

- ISO/CEI 27001:2018
- ISO/CEI 31000 et 31010 Gestion des risques

Pour ajouter des détails supplémentaires et une structure à la méthodologie, Kyriba a incorporé des contrôles d'évaluation des risques sélectionnés du NIST faisant référence aux évaluations des risques, à la gestion des risques liés à la sécurité des informations et au guide technique des tests de sécurité des informations.

Afin d'obtenir une validation indépendante de la mise en œuvre des contrôles de sécurité, Kyriba engage régulièrement des sociétés externes de grande réputation pour effectuer des tests de pénétration de son application web ainsi que des analyses de vulnérabilité. Kyriba a également mis en œuvre un programme de sécurité logicielle qui aligne Kyriba sur les pratiques de développement de logiciels sécurisés telles que décrites par l'OWASP et le SANS. Ce programme comprend une analyse statique du code qui est effectuée sur la base de code Kyriba, une analyse dynamique automatisée du code et une formation au code sécurisé pour les développeurs Kyriba et le personnel de sécurité.

Kyriba se soumet à une analyse annuelle d'impact sur l'entreprise (BIA) et à une auto-évaluation annuelle SIG 7 (module cloud inclus).

L'organisation de Kyriba en charge des risques et de la conformité est très compétente et certifiée dans les domaines des risques et de la conformité, avec des certifications allant de CISSP, CRISC, GIAC et PMP. L'équipe chargée des risques et de la conformité a une connaissance approfondie des différents cadres de sécurité tels que ISO, PCI, FedRAMP, DOD et NIST, ainsi que de la conformité SOC.

Politique de confidentialité des données Client
Kyriba gère une Politique de confidentialité des données Client qui résume les procédures de Kyriba Corp. concernant les données d'utilisateur final collectées au nom de ses clients via les applications Kyriba Enterprise et les services connexes. La Politique de confidentialité des données Client est maintenue, mise en œuvre et contrôlée par le Bureau du responsable de la sécurité des systèmes d'information et est revue au moins une fois par an pour vérifier son exactitude et son applicabilité.

Conservation et élimination des données Client
Sauf disposition légale ou réglementaire contraire, Kyriba conservera les données à caractère personnel seulement

pour la durée nécessaire à l'objet de leur collecte. L'ensemble des données à caractère personnel inutiles se trouvant dans la base de données du serveur actif seront rendues inaccessibles dans un délai raisonnable, conformément aux normes du secteur, une fois qu'il aura été déterminé que lesdites données à caractère personnel ne sont plus nécessaires. Aux fins des besoins des Applications Kyriba Enterprise, des copies de données de production peuvent être utilisées dans des environnements de test externes, mais aucune donnée Client n'est utilisée dans un environnement de test ou de développement, à moins qu'elle n'ait été anonymisée. Toutefois, lesdites données contenant des données à caractère personnel sont protégées de la même façon et bénéficient de contrôles identiques à ce qui est mentionné dans la Politique de confidentialité des données Client.

Divulgation à des tiers
Kyriba est en droit de partager des données à caractère personnel avec les filiales et sociétés affiliées de Kyriba. Kyriba est également libre de partager des données à caractère personnel avec des prestataires de services sélectionnés pour effectuer des missions en son nom. Kyriba exige des prestataires de services auxquels elle divulgue des données à caractère personnel et qui ne sont pas soumis, le cas échéant, aux lois fondées sur la directive européenne sur la protection des données ou à la loi fédérale suisse sur la protection des données qu'ils (i) concluent les clauses contractuelles types pour le transfert international des données à caractère personnel adoptées par la Commission européenne ou (ii) soient soumis à une autre décision d'adéquation de la Commission européenne (par exemple, les sociétés situées au Canada).

Politique du système de gestion des clés de cryptage :
L'accès aux clés de cryptage stockées est enregistré à des fins d'audit et d'enquête sur les incidents, le cas échéant. La gestion des clés de sécurité doit être menée dans l'esprit des Federal Information Processing Standards (FIPS 140-2). Des politiques sont en vigueur pour fournir un environnement global visant à conserver :

- Sécurité : privilège d'accès minimal, supervision du contrôle de la sécurité du système
- Disponibilité : assurer que les durées minimales de disponibilité sont satisfaites
- Intégrité de traitement : supervision des interfaces / tâches
- Confidentialité : traitement des informations Client de façon confidentielle

Classification des données
La classification des données est en vigueur et est utilisée afin de définir les exigences en matière de protection, les droits et les restrictions d'accès, ainsi que les exigences et les paramètres de conservation et de destruction. Les données Client restreintes seront rendues inaccessibles lorsque le contrat avec celui-ci prendra fin. Ultérieurement, ces données pourront être supprimées ou autrement écrasées conformément aux normes du secteur en matière de processus de suppression/formatage. Tous les disques stockant les données Client sont cryptés au repos à l'aide d'un cryptage de 256 bits.

Données à caractère personnel
Kyriba prendra les précautions adéquates afin de protéger les Données à caractère personnel en sa possession de toute perte, mauvaise utilisation et accès non autorisé, divulgation, modification et destruction. Kyriba utilise des mesures de sécurité physiques, électroniques et administratives dans le but de protéger les Données à caractère personnel. Kyriba limite l'accès aux Données à caractère personnel aux seules personnes au sein de la société ayant à charge de conserver et de traiter lesdites Données à caractère personnel ou aux fournisseurs tiers approuvés impliqués dans le Traitement des données à caractère personnel. Les personnes bénéficiant d'un accès aux Données à caractère personnel seront informées de leurs responsabilités spécifiques de protéger la sécurité, la confidentialité et l'intégrité desdites données à caractère personnel. Kyriba réalise régulièrement des audits tels que SOC1, SOC2, ISO 27001, des tests d'intrusion dans le réseau ou les applications, des audits de code source, ainsi que d'autres audits récurrents ou planifiés relatifs à l'architecture, aux processus et aux procédures. Les audits sont réalisés par des tiers réputés. Le Bureau du responsable de la sécurité des systèmes d'information est chargé de commander tous les audits nécessaires pour se conformer aux engagements de Kyriba concernant la sécurité et l'intégrité des données Client.

Gestion des incidents
Kyriba dispose d'une politique de gestion des incidents rapportés en vigueur, afin de répondre aux accidents. Une Service Excellence Action Team (équipe SEAT) est en place et est chargée de la résolution des incidents majeurs susceptibles d'avoir un impact important sur la sécurité, la disponibilité, l'intégrité et la confidentialité des

technologies et des données Kyriba.
Kyriba a publié des documents internes visant à présenter étape par étape les modalités d'intervention de l'équipe SEAT et à définir la qualité de ses membres. Ces documents sont hautement confidentiels et ne devraient pas être diffusés hors de la société.

Reprise d'activité
Kyriba dispose de documents internes visant à présenter étape par étape les modalités de déclaration d'un sinistre et d'intervention de l'équipe SEAT et à définir la qualité de ses membres. Ces documents sont hautement confidentiels et ne devraient pas être diffusés hors de la société.

Des sauvegardes incrémentielles de l'application et des bases de données de Kyriba sont réalisées quotidiennement sur un serveur local. Les sauvegardes complètes sont effectuées une fois par semaine. En outre, les sauvegardes sont copiées sur un serveur de reprise d'activité à distance situé dans le centre de données alternatif. L'équipe des opérations techniques de Kyriba contrôle le statut des sauvegardes, afin d'assurer que celles-ci ont bien été effectuées sur le serveur local et copiées sur le serveur de reprise d'activité à distance.

Contrôle des services
De manière générale, des accords de niveau de service (SLA) sont conclus entre Kyriba et ses clients. Des outils de suivi sont en place pour un contrôle continu qui est assuré afin que Kyriba puisse s'autoévaluer au regard des engagements pris. L'équilibrage de charge vise à répartir la charge de travail sur plusieurs serveurs et machines virtuelles dans le cadre de l'architecture d'application Kyriba. De nombreux équilibreurs de charge sont utilisés au sein du système en vue d'aider à maximiser son évolutivité.

L'équipe des opérations techniques de Kyriba en interne est chargée de suivre et d'assurer la disponibilité de l'ensemble des systèmes exécutant les plateformes de production de Kyriba dans le monde entier.

Les systèmes de production maintiennent une hausse de la disponibilité de 99,9 % (infrastructure redondante) 24 heures sur 24 et 7 jours sur 7. Des politiques de pare-feu sont en place et sont gérées par l'équipe des opérations techniques de Kyriba.

Contrôle de la divulgation
Des mesures sont prises pour empêcher l'accès non autorisé, la modification ou la suppression des données pendant le transfert, et pour garantir que les transferts sont sécurisés et enregistrés. Ces mesures doivent comprendre :
- Le cryptage à l'aide d'un VPN pour l'accès à distance
- Le cryptage et d'autres méthodes sécurisées (par exemple, sFTP) pour le transport et la communication des données
- La création d'une piste d'audit des transferts de données liés aux services

Documentation interne
Kyriba met en place une documentation interne afin d'évaluer l'exposition des Données à caractère personnel traitées par Kyriba aux demandes et contrôles des organismes de surveillance et de sécurité.

ANNEXE III - LISTE DES SOUS-TRAITANTS

MODULE DEUX : Transfert du Responsable de Traitement au Sous-traitant
MODULE TROIS : Transfert du Sous-traitant au Sous-traitant ultérieur

NOTE EXPLICATIVE :
Cette annexe doit être complétée par les modules deux et trois, en cas d'autorisation spécifique des sous-traitants ultérieurs (clause 9(a), option 1).

Le Responsable de Traitement a autorisé le recours aux sous-traitants ultérieurs suivants :

1. Sociétés affiliées de Kyriba (à des fins de mise en œuvre, de support et de maintenance).
2. Amazon Web Services, Inc. (à des fins de fourniture d'infrastructure pour l'application de Kyriba) : UE.