Addendum relatif au traitement des données personnelles

Le présent addendum relatif au traitement des données personnelles (ci-après dénommé « **Addendum** ») entre en vigueur à la date d'entrée en vigueur de l'Addendum et fait partie intégrante du contrat (ci-après dénommé « **Contrat** ») conclu entre le Client et Kyriba (ci-après dénommés individuellement « **Partie** » ou collectivement « **Parties** ») pour la fourniture des Services SaaS.

Le présent Addendum définit l'accord entre les Parties concernant le Traitement des Données à caractère personnel du Client et remplace et annule toute disposition existante relative aux Données à caractère personnel du Client dans le Contrat ou ailleurs.

1. **Définitions.**
   a. **« Date d'entrée en vigueur de l'addendum »** désigne la date d'entrée en vigueur et reste en vigueur aussi longtemps que le Contrat reste en vigueur.
   b. **« Anonymisé »** désigne un processus qui consiste à utiliser un ensemble de techniques visant à rendre impossible, dans la pratique, l'identification de la personne concernée par quelque moyen que ce soit et de manière irréversible. Lorsque cette anonymisation est effective, les données ne sont plus considérées comme des données à caractère personnel et les exigences du RGPD ne sont plus applicables.
   c. « **Loi applicable en matière de protection des données personnelles**» désigne, si et dans la mesure où elles sont applicables, (a) la loi britannique de 2018 sur la protection des données personnelles et le RGPD de l'UE, dans la mesure où il fait partie du droit de l'UE conservé au Royaume-Uni (« RGPD britannique ») ; (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/CE (« **Règlement général sur la protection des données** » ou « **RGPD** ») ; les lois sur la protection des données personnelles aux États-Unis, y compris, mais sans s'y limiter, la California Consumer Privacy Act de 2018, le California Civil Code § 1798.100 *et suivants,* tel que modifié par la California Privacy Rights Act de 2020, et les règlements pris en application de celle-ci (collectivement, les « **lois américaines sur la protection des données personnelles** ») ; et (d) toute autre loi, règle, réglementation, directive d'autorégulation ou législation d'application applicable aux Services SaaS et au traitement des Données personnelles des Clients par Kyriba.
   d. « **Données personnelles du client** » : désigne les informations qui peuvent être fournies par le Client à Kyriba et qui comprennent les informations qui identifient, concernent, décrivent, sont susceptibles d'être associées ou pourraient r être liées, directement ou indirectement, à une personne concernée ou qui sont définies comme « informations personnelles identifiables », « informations personnelles », « données personnelles » ou tout autre terme similaire en vertu de la loi applicable en matière de protection des données personnelles.
   e. **Les termes « traitement »**, **« traité »** ou **« traiter »** ont la même signification que celle qui leur est donnée dans la Loi applicable en matière de protection des données personnelles.
   f. **Le terme** « **sous-traitant** » a la même signification que celle définie dans la Loi applicable en matière de protection des données personnelles et désigne tout sous-traitant (y compris tout tiers et toute filiale de Kyriba, à l'exclusion des employés de Kyriba) désigné par ou pour le compte de Kyriba afin de traiter les Données personnelles du Client.

g. Les mots et expressions utilisés dans le présent Addendum ont, dans la mesure du possible, le sens qui leur est donné dans la Loi applicable en matière de protection des données.
h. Tous les termes en majuscules non définis dans le présent document ont la signification qui leur est donnée dans le Contrat.
i. En cas d'incohérence entre les dispositions du Contrat et celles du présent Addendum, les Parties conviennent que les dispositions du présent Addendum prévaudront.

2. Relation entre les parties.

a. Le Client est le « responsable du traitement » (tel que défini dans la Loi applicable en matière de protection des données personnelles) ou l'entreprise qui détermine les finalités et les modalités du traitement des Données personnelles du Client par Kyriba. Le contrôle et la responsabilité des Données personnelles du Client restent à tout moment de la responsabilité du Client.
b. Kyriba est le « sous-traitant » soit le prestataire de services qui traite les Données personnelles du Client conformément aux instructions documentées du Client.

3. Obligations générales du sous-traitant.

a. Kyriba traitera les Données personnelles du Client conformément à la Loi applicable en matière de protection des données personnelles et uniquement dans le but de fournir les Services SaaS au Client. Kyriba s'engage à ne pas (i) traiter les Données personnelles du Client à des fins autres que celles énoncées dans le présent Addendum et conformément aux instructions documentées du Client ou à la loi applicable ; (ii) divulguer les Données personnelles du Client à des tiers autres que les sociétés affiliées ou filiales de Kyriba, aux fins susmentionnées ou conformément à la législation applicable ; (iii) vendre, louer, divulguer, diffuser, mettre à disposition, transférer ou communiquer de toute autre manière les Données personnelles du Client à un tiers en échange d'une contrepartie monétaire ou autre ; ou (iv) conserver, utiliser ou divulguer les Données personnelles du Client en dehors de la relation commerciale directe entre Kyriba et le Client.
b. Kyriba ne combinera pas les Données personnelles du Client qu'elle reçoit avec des informations personnelles qu'elle reçoit d'une autre personne ou entité, étant entendu que Kyriba peut combiner des informations personnelles afin de poursuivre tout objectif commercial tel que défini dans les Lois applicables en matière de protection des données personnelles.
c. Si Kyriba doit traiter les Données personnelles du Client conformément à une autre exigence légale applicable aux Services SaaS, Kyriba informera le Client de cette exigence légale avant de traiter les Données personnelles du Client, sauf si cette loi interdit une telle divulgation.
d. La finalité et la durée du traitement, sa nature, le type de Données personnelles du Client faisant l'objet du traitement et les catégories de personnes concernées sont précisés dans le présent Addendum, Annexe 1 joint aux présentes et intégré aux présentes (« Annexe 1 »).

4. Obligations générales du responsable du traitement.

a. Le Client est seul responsable de l'exactitude, de la qualité et de la légalité des Données personnelles du Client.
b. Le Client s'est conformé et continuera de se conformer à toutes les lois applicables en matière de protection des données personnelles.

c. Le Client dispose de l'autorité, de la licence ou du consentement nécessaire pour fournir les Données personnelles du Client et dispose d'une base légale (y compris toutes les notifications et tous les consentements légalement requis), s'est conformé (et continuera de se conformer) à toutes les Lois applicables en matière de protection des données personnelles, en particulier pour le partage, la transmission et le traitement des Données personnelles du Client avec, vers et par Kyriba aux fins des Services SaaS et du Contrat.
d. Le Client certifie que le traitement par Kyriba des Données personnelles du Client conformément aux instructions documentées du Client et au présent Addendum n'entraînera aucune violation par Kyriba des lois applicables en matière de protection des données.
e. Le Client a et continuera d'avoir le droit de transférer ou de donner accès aux Données personnelles du Client à Kyriba afin qu'elles soient reçues, transférées et traitées conformément au présent Addendum.
f. Le Client s'est engagé et continuera à s'engager, conformément à la Législation applicable en matière de protection des données personnelles, à réaliser toutes les évaluations d'impact sur la protection des données et/ou les évaluations de sécurité nécessaires pour faciliter le transfert des Données personnelles du Client à Kyriba (que ce soit à l'intérieur ou à l'extérieur du pays où les Données personnelles du Client ont été initialement collectées). Nonobstant ce qui précède et en tout état de cause, rien n'empêche Kyriba d'accéder, de recevoir, d'utiliser ou de traiter de toute autre manière les Données personnelles du Client en dehors du pays de réception, conformément aux conditions du présent Addendum.
g. Le Client informera immédiatement Kyriba de toute plainte, réclamation, enquête et/ou demande émanant d'une autorité réglementaire susceptible de concerner ou d'impliquer les Données personnelles du Client traitées par Kyriba.
h. Le cas échéant, le Client ne transférera ni ne divulguera aucune Donnée personnelle du client contenant des « secrets d'État » et/ou des « données importantes » tels que définis dans la Loi applicable en matière de protection des données personnelles, ou dont le transfert hors du pays de transfert est interdit en vertu de la Loi applicable en matière de protection des données.

5. **Conformité à l'article 28 du RGPD.**
a. Kyriba se conformera aux exigences énoncées à l'article 28 du RGPD ou du RGPD britannique, le cas échéant, et à la description du traitement figurant à l'annexe 1.
b. Kyriba (i) veillera à ce que les employés de Kyriba autorisés à traiter les Données personnelles du Client en vertu du présent Addendum soient liés par des clauses de confidentialité substantiellement similaires à celles du Contrat ou à l'obligation légale de confidentialité appropriée, (ii) compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, de maintenir des mesures de sécurité et des mesures techniques et organisationnelles conformes visées à l'article 32 du RGPD pour la protection, la confidentialité et l'intégrité des Données personnelles du Client, (iii) contrôler régulièrement le respect de ces mesures et ne pas réduire de manière significative la sécurité globale des Services SaaS pendant la fourniture des Services SaaS conformément au Contrat, (iv) dans la mesure où la loi le permet, informer rapidement le Client si Kyriba reçoit une demande d'un individu, d'un consommateur ou d'une personne concernée visant à exercer ses droits en vertu de la Loi applicable en matière de protection des données ou si elle reçoit une demande ou une plainte d'une autorité de contrôle ou d'un autre tiers (« **Demande** »), (v) compte tenu de la nature du traitement, mettre en place des mesures techniques

et organisationnelles appropriées, assister le Client dans son obligation de répondre aux demandes d'exercice des droits des personnes concernées, transférer au Client ses demandes dans un délai raisonnable apres en avoir pris connaissance, et ne pas répondre à ces Demandes directement, et (vi) sous réserve de la section 6.3 (Données du client) du Contrat, supprimer toutes les Données personnelles du Client du site live dans les soixante (60) jours suivant la résiliation du Contrat pour quelque raison que ce soit ou si les Données personnelles du Client ne sont plus nécessaires à l'exécution des Services SaaS ; toutefois, Kyriba peut conserver les Données personnelles du Client, se trouvant sur des sauvegardes («archives intermédiaires » telles que définies par le RGPD) que Kyriba a effectué au cours du déroulement normal de la relation commerciale établie entre les Parties et lorsque cela est nécessaire pour se conformer à la loi applicable ou à une obligation légale.

6. **Vérifications de conformité.**
   a. Kyriba mettra à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans le présent Addendum et permettra, dans la mesure requise par la loi, de contribuer aux audits, menés par le Client ou un autre auditeur, non concurrent de Kyriba, mandaté par le Client.
   b. Cet auditeur sera tenu de respecter des engagements de confidentialité au moins aussi stricts que ceux prévus dans le Contrat. En cas de demande d'audit, le Client informera Kyriba dans un délai raisonnable. Les audits seront effectués en dehors des locaux, conformément aux politiques de Kyriba, et ne perturberont pas de manière déraisonnable les activités commerciales de Kyriba. Les audits auront lieu pendant les heures normales de travail, sauf si l'audit doit être effectué en urgence à la demande d'une autorité réglementaire.
   c. Dans la mesure où la loi le permet, le Client sera responsable de tous les frais raisonnables et documentés, engagés par Kyriba, pour fournir une assistance qui va au-delà de ce qui est requis par la loi et conformément au présent paragraphe (c). Tous les rapports susmentionnés constituent des informations confidentielles des Parties.

7. **Transferts ultérieurs.**
   a. Le Client reconnaît et accepte que les Données personnelles du Client puissent être transférées en dehors de l'Espace Economique Européen, du Royaume-Uni ou d'autres juridictions dans lesquelles les Données personnelles du Client ont été collectées (« **Transfert ultérieur** »), vers des pays reconnus par la Commission européenne, ou l'Information Commissioner's Office UK (« **ICO** »), ou d'autres juridictions, le cas échéant, comme des pays offrant un niveau de protection adéquat, tel que mis à jour de temps à autre (« **Lieu autorisé** »).
   b. Pendant la durée du Contrat, les Parties, ou Kyriba et ses sous-traitants ultérieurs, le cas échéant, se conformeront aux conditions générales des Clauses contractuelles types applicables (Module 2 - Responsable du traitement à Sous-traitant) ou Module 3 - Sous-traitant à Sous-traitant) telles que définies dans la Décision de la Commission du 4 juin 2021 (2021/91), telle que modifiée, mise à jour, remplacée ou substituée de temps à autre (« **Clauses contractuelles types de l'UE** »), ou un formulaire équivalent aux Clauses contractuelles types, tel qu'approuvé par l'ICO, pour l'exportation des Données personnelles des clients britanniques, en dehors du Royaume-Uni (« **Addendum aux Clauses contractuelles types du Royaume-Uni** ») pour ces Transferts ultérieurs.

c. Si le Client accepte un Transfert ultérieur, celui-ci 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 la loi applicable en matière de protection des données personnelles, qui seront tous intégrés par référence et réputés exécutés en raison de la signature du Contrat par chacune des Parties. Les clauses applicables sont disponibles à l'adresse suivante : 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 requis concernant les Transferts ultérieurs, tels que requis par les clauses contractuelles types de l'UE et les clauses contractuelles types du Royaume-Uni, sont énoncés dans l'annexe 2 - Appendice aux clauses contractuelles types jointes aux présentes et intégrées aux présentes.

e. En outre, Kyriba Corp. se conforme au cadre de protection des données UE-États-Unis (EU-U.S. DPF), à l'extension britannique du cadre UE-États-Unis (UK Extension to the EU-U.S. DPF) et au cadre de protection des données Suisse-États-Unis (Swiss-U.S. DPF) tels que définis par le ministère américain du Commerce (collectivement, le « DPF »). Des informations sur la participation de Kyriba au DPF sont disponibles à l'adresse https://www.kyriba.com/legal-pages/data-privacy-framework-notice/

8. **Sous-traitants ultérieurs.**

a. Kyriba fait appel à des sous-traitants ultérieurs (tels que définis dans la législation applicable en matière de protection des données personnelles) pour effectuer des activités de traitement spécifiques, telles que l'hébergement, le support ou la maintenance. Les sous-traitants ultérieurs utilisés à la date du présent addendum sont spécifiés en annexe des présentes. En outre, le Client autorise par écrit Kyriba à faire appel à tout autre sous-traitant ultérieure pour les besoins 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 (« **Modification** »), conformément à ce qui suit :

i. Kyriba informera le Client à l'avance de toute modification proposée en rapport avec l'utilisation des Services SaaS par le Client, lui donnant ainsi la possibilité de s'opposer à cette Modification. Le Client dispose d'un délai maximal de sept (7) jours ouvrables à compter de la date de réception de cette information pour s'opposer expressément à la Modification pour des motifs valables en envoyant sa décision par écrit à Kyriba. Cet ecrit doit exposer les motifs de l'opposition. Si le Client envoie une notification s'opposant au nouveau sous-traitant ultérieur, les Parties s'efforceront de résoudre le problème par le biais d'un accord mutuel.

ii. Si, cinq (5) jours avant la date d'entrée en vigueur de la Modification, les Parties ne sont pas parvenues à un accord, le Client sera en droit de résilier le Contrat avec effet à la date d'entrée en vigueur de la Modification.

iii. Si le Client ne résilie pas le Contrat conformément à la présente section, il sera considéré comme ayant accepté la Modification. Ce droit de résiliation est le seul et unique recours du Client s'il s'oppose à un nouveau sous-traitant ultérieur.

iv. Kyriba signera un accord écrit avec tout sous-traitant ultérieur auquel elle fait appel afin de s'assurer que ce sous-traitant ultérieur respecte les dispositions de la présente section et satisfait aux exigences énoncées dans la loi applicable en matière de protection des données personnelles. Kyriba restera responsable du respect par ce sous-traitant ultérieur des conditions des présentes.

9. **Violation de la sécurité des informations.** Kyriba dispose de politiques et de procédures de gestion des incidents de sécurité et, en cas de violation effective de la sécurité affectant les Données personnelles du Client transmises, stockées ou traitées par Kyriba (la « **Violation de la sécurité des informations** »), Kyriba : informera le Client, après en avoir pris connaissance, et en tout état de cause dans les 48 heures, de 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 personnelles du Client concernées, lorsque ces informations sont disponibles. Kyriba décrira également, dans la mesure du possible, les conséquences probables de la Violation de la sécurité de l'information sur les données personnelles du client, ainsi que les mesures raisonnables que Kyriba juge nécessaires et raisonnables pour remédier à la cause de cette violation de la sécurité de l'information, dans la mesure où cette réparation est sous le contrôle de Kyriba, y compris, le cas échéant, pour atténuer ses effets négatifs; et agir dans les meilleurs délais (i) pour atténuer tout impact négatif ou autre préjudice causé au Client et à toute personne concernée, à la suite de cette Violation de la sécurité des informations ; et (ii) pour empêcher que d'autres violations similaires ne se produisent 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.

ANNEXE 1 - CALENDRIER DE TRAITEMENT DES DONNÉES

Le présent calendrier de traitement des données fait partie intégrante de l'avenant 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 de personnes, de consommateurs ou de personnes concernées	Finalité du traitement	Durée du traitement
Déterminée et contrôlée par le client, à sa discrétion ; 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, ainsi que les comptes financiers	Employés, représentants, sous-traitants, partenaires, fournisseurs, personnes d'intérêt et/ou clients du client	Fourniture des services SaaS dans le cadre du Contrat	La durée du traitement correspond à la durée du Contrat concernant les Données du client sur le site live. Les Données du client seront ensuite traitées en archives intermédiaires pour respecter la Loi applicable ou une obligation légale.

2. Sous-traitants ultérieurs

Veuillez vous reporter à l'annexe III de l'appendice 2 ci-dessous.

Il est entendu que Kyriba peut modifier, remplacer ou ajouter des sous-traitants ultérieurs conformément à la section 8 de l'Addendum.

ANNEXE 2 - APPENDICE AUX CLAUSES CONTRACTUELLES TYPE

ANNEXE I

A. LISTE DES PARTIES

MODULE DEUX : Transfert du responsable du traitement au sous-traitant
MODULE TROIS : Transfert entre responsables du traitement

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

- **Nom :** Le client identifié dans le contrat et/ou l'entité Kyriba applicable identifiée dans le contrat.

Importateur(s) de données : [*Identité et coordonnées de l'importateur ou des importateurs de données, y compris toute personne de contact responsable de la protection des données]*

- **Nom** : Kyriba SEMEA
- **Adresse** : Tour Eqho, 92400 Courbevoie, France
- **Nom, fonction et coordonnées de la personne à contacter** : Équipe chargée de la confidentialité des données de Kyriba : (privacy@kyriba.com)
- **Activités pertinentes pour les données transférées en vertu des présentes clauses** : Kyriba SEMEA est une filiale d'une société américaine, fournissant des solutions de gestion de trésorerie et de liquidité sous forme de logiciels en tant que service, ainsi que des services d'assistance, de maintenance, de mise en œuvre et de formation associés.

Importateur de données:
KYRIBA Corp (USA)
KYRIBA UK LIMITED
Kyriba Engineering Pologne sp. z.o.o.

- **Rôle (contrôleur/sous-traitant)** : sous-traitant

B. DESCRIPTION DU TRANSFERT

MODULE DEUX : Transfert du contrôleur au processeur
MODULE TROIS : Transfert du responsable du traitement au responsable du traitement

Catégories de personnes concernées dont les données à caractère personnel sont transférées

Employés, représentants, sous-traitants, partenaires, fournisseurs, personnes d'intérêt et/ou clients du client

Catégories de données à caractère personnel transférées

Déterminées et contrôlées par le client à sa discrétion ; elles peuvent 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, ainsi que 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, telles que, par exemple, une limitation stricte de la finalité, des restrictions d'accès (y compris l'accès réservé au personnel ayant suivi une formation spécialisée), la conservation d'un registre des accès aux données, des restrictions au transfert ultérieur 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 peut avoir lieu tout au long de la durée du contrat, selon les besoins.

Nature du traitement

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

Finalité(s) du transfert de données et du traitement ultérieur

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

Durée de conservation des données à caractère personnel ou, si cela n'est pas possible, critères utilisés pour déterminer cette durée

La durée du traitement correspond à la durée du Contrat concernant les Données du client sur son site Live. Kyriba conservera par la suite en archives intermédiaires les Données du client pour des raisons légales.

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

Lorsque des sous-traitants ultérieurs sont impliqués (voir liste fournie), le Transfert ultérieur est limité au transfert nécessaire à l'exécution du Contrat et à sa durée.

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

MODULE DEUX : Transfert du responsable du traitement au sous-traitant
MODULE TROIS : Transfert du responsable du traitement à un autre responsable du traitement

Autorité française chargée de la protection des données – CNIL

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

MODULE DEUX : Transfert du responsable du traitement au sous-traitant
MODULE TROIS : Transfert du sous-traitant à un autre sous-traitant

Description des mesures techniques et organisationnelles mises en œuvre par le responsable du transfert conformément aux clauses 4(d) et 5(c) (ou document/législation joint) :

La plateforme SaaS de Kyriba est auditée par un cabinet d'audit tiers réputé deux fois par an afin de garantir sa conformité à la déclaration d'engagement d'attestation n° 18 (SSAE 18)/Service Organization Control (SOC) 1 et une fois par an afin de garantir sa conformité aux normes SOC2. 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 d'un nombre croissant d'entreprises informatiques et de cloud computing. Elle permet à l'organisation auditée de démontrer qu'elle respecte et dépasse les normes reconnues par le 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 ISO/IEC 27001.

Kyriba dispose d'un cadre de gestion des risques basé sur les meilleures pratiques qui gère ses risques de sécurité en décrivant un cycle de vie de la gestion des risques de sécurité et définit les exigences pour comprendre, évaluer, répondre et surveiller les risques de sécurité chez Kyriba.

La méthodologie d'évaluation des risques de Kyriba repose sur :

- ISO/IEC 27001: 2022
- Afin d'ajouter des détails et une structure à la méthodologie, Kyriba a intégré une sélection de contrôles d'évaluation des risques du NIST faisant référence aux évaluations des risques, à la gestion des risques liés à la sécurité de l'information et au guide technique pour les tests de sécurité de l'information.

Afin de valider de manière indépendante la mise en œuvre des contrôles de sécurité, Kyriba fait régulièrement appel à des sociétés externes de renom pour effectuer des tests de pénétration sur ses applications web et des analyses de vulnérabilité. Kyriba a également mis en place un programme de sécurité logicielle qui aligne Kyriba sur les pratiques de développement logiciel sécurisé définies par l'OWASP et le SANS. Ce programme comprend une analyse statique du code effectuée sur la base de code Kyriba, une analyse dynamique automatisée du code et une formation au code sécurisé pour les développeurs et le personnel de sécurité de Kyriba.

Kyriba se soumet à une analyse d'impact sur les activités (BIA) et à une auto-évaluation SIG 7

(module cloud inclus) chaque année.

L'organisation chargée de la gestion des risques et de la conformité de Kyriba est très compétente et certifiée dans les domaines de la gestion des risques et de la conformité, avec des certifications telles que CISSP, CRISC, GIAC et PMP. L'équipe chargée de la gestion des risques et de la conformité possède une connaissance approfondie de divers 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 des utilisateurs finaux collectées pour le compte de ses clients via les applications d'entreprise Kyriba et les services associés. La politique de confidentialité des données clients est maintenue, appliquée et contrôlée par le bureau du directeur de la sécurité des systèmes d'information et est révisée au moins une fois par an afin d'en vérifier l'exactitude et l'applicabilité.

Conservation et destruction des données clients
Sauf disposition contraire expresse d'une loi ou d'un règlement, Kyriba ne conservera les données personnelles que pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Toutes les données personnelles stockées dans la base de données du serveur actif qui ne sont plus nécessaires seront rendues inaccessibles conformément aux normes de l'industrie dans un délai raisonnable après qu'il aura été déterminé qu'elles ne sont plus nécessaires. Pour les applications Kyriba Enterprise, des copies des 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, toute donnée contenant des données personnelles est protégée de la même manière et par les mêmes contrôles que ceux décrits plus en détail dans la Politique de confidentialité des données clients.

Divulgation à des tiers
Kyriba peut partager des données personnelles avec ses filiales et sociétés affiliées. Kyriba peut également partager des données personnelles avec des prestataires de services que nous avons engagés pour fournir des services pour le compte de Kyriba. Kyriba exige des prestataires de services auxquels elle divulgue des données personnelles et qui ne sont pas soumis aux lois basées sur la directive européenne sur la protection des données ou à la loi fédérale suisse sur la protection des données, selon le cas, qu'ils (i) concluent les clauses contractuelles types pour le transfert international de données personnelles adoptées par la Commission européenne ou (ii) soient soumis à une autre décision d'adéquation de la Commission européenne (par exemple, les entreprises situées au Canada).

Politique relative au système de gestion des clés de chiffrement :
L'accès aux clés de chiffrement stockées est enregistré à des fins d'audit et d'enquête en cas d'incident, si nécessaire. La gestion des clés de sécurité est conforme à l'esprit des normes fédérales américaines FIPS 140-2 (Federal Information Processing Standards). Des politiques sont en place pour fournir un environnement global qui s'efforce de maintenir :

- Sécurité : accès avec le moins de privilèges possible, supervision de la surveillance de la sécurité du système
- Disponibilité : garantie du respect des temps de fonctionnement minimaux
- Intégrité du traitement : supervision des interfaces/tâches
- Confidentialité : traitement des informations des clients comme des informations confidentielles

Classification des données
La classification des données est en place et sert à définir les exigences en matière de protection, les droits d'accès et les restrictions, ainsi que les exigences et les paramètres de conservation et de destruction. Les données clients restreintes seront rendues inaccessibles à la fin du contrat. À l'avenir, ces données pourraient être supprimées ou effacées conformément aux processus de suppression/effacement standard de l'industrie. Tous les disques stockant les données des clients sont cryptés au repos à l'aide d'un cryptage 256 bits.

Données personnelles
Kyriba prendra toutes les précautions raisonnables pour protéger les données personnelles en sa possession contre la perte, l'utilisation abusive, l'accès non autorisé, la divulgation, la modification et la destruction. Kyriba utilise des mesures de sécurité physiques, électroniques et administratives pour protéger les données personnelles. Kyriba limite l'accès aux données personnelles aux personnes de son organisation qui ont un objectif commercial spécifique pour la conservation et le traitement des données personnelles ou aux fournisseurs tiers agréés qui participent au traitement des données personnelles. Les personnes qui ont accès aux données à caractère personnel seront informées de leurs responsabilités spécifiques en matière de protection de la sécurité, de la confidentialité et de l'intégrité des données à caractère personnel. Kyriba réalise des audits périodiques tels que SOC1, SOC2, ISO 27001, des tests d'intrusion sur le réseau et/ou les applications, des audits du code source, d'autres audits récurrents et/ou programmés liés à l'architecture ou aux processus et 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 garantir le respect des engagements de Kyriba en matière de sécurité et d'intégrité des données des clients.

Gestion des incidents
Kyriba a mis en place une politique documentée de gestion des incidents afin de traiter les incidents. Une équipe d'action pour l'excellence du service (SEAT) est en place et intervient pour résoudre les incidents critiques susceptibles d'avoir un impact sur la sécurité, la disponibilité, l'intégrité et la confidentialité de la technologie et des données de Kyriba.
Kyriba a créé une documentation interne qui sert de guide pour la mise en place de l'équipe SEAT et la définition des membres de cette équipe. Cette documentation est considérée comme hautement sensible et confidentielle et n'est donc pas divulguée à l'extérieur de l'entreprise.

Reprise après sinistre
Kyriba dispose d'une documentation interne qui sert à guider les mécanismes de déclaration d'une catastrophe, la SEAT, la définition des membres de la SEAT, et qui est considérée comme hautement sensible et confidentielle et n'est donc pas divulguée en dehors de l'entreprise.

Des sauvegardes incrémentielles de l'application et des bases de données Kyriba sont effectuées quotidiennement sur un serveur de sauvegarde local. Des sauvegardes complètes sont effectuées chaque semaine. Les sauvegardes sont en outre répliquées sur un serveur de reprise après sinistre distant situé dans un centre de données alternatif. L'équipe des opérations techniques de Kyriba vérifie l'état des sauvegardes afin de s'assurer que la sauvegarde sur le serveur de sauvegarde local et la réplication sur le serveur de reprise après sinistre distant ont été effectuées avec succès.

Surveillance des services
Des accords de niveau de service (SLA) sont conclus entre Kyriba et ses clients. Des outils de

surveillance sont mis en place pour assurer une surveillance continue qui permet à Kyriba de mesurer son respect de ces engagements. L'équilibrage de charge est utilisé pour répartir la charge de travail entre plusieurs serveurs et machines virtuelles au sein de l'architecture de l'application Kyriba. Plusieurs équilibreurs de charge sont utilisés au sein du système afin d'optimiser l'évolutivité du système.

L'équipe technique interne de Kyriba est chargée de surveiller et de garantir la disponibilité de tous les systèmes qui font fonctionner les plateformes de production Kyriba à travers le monde.

Les systèmes de production maintiennent une haute disponibilité de 99,9 % (infrastructure redondante) 24 heures sur 24, 7 jours sur 7. Des politiques de pare-feu sont en place et 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 leur transfert, et pour garantir que les transferts sont sécurisés et enregistrés. Ces mesures comprennent :
● 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
● 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 autorités de surveillance et de sécurité.

ANNEXE III – LISTE DES SOUS-TRAITANTS

MODULE DEUX : Transfert du responsable du traitement au sous-traitant
MODULE TROIS : Transfert du responsable du traitement au sous-traitant

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants :

1. Les filiales de Kyriba (à des fins de mise en œuvre, d'assistance et de maintenance).

Entité Kyriba	**Entité Lieu**	**Finalité du traitement**
Kyriba Corp.	États-Unis	Mise en œuvre, assistance et maintenance
Kyriba UK LTD	Royaume-Uni	Mise en œuvre et assistance
Kyriba Engineering Pologne sp. z.o.o.	Pologne	Mise en œuvre, assistance et maintenance

2. Amazon Web Services, Inc. (aux fins de fournir l'infrastructure pour l'application Kyriba) : Europe
3. IGT I Outsourcing Lanka Limited (assistance et maintenance).
4. Si option modules IA/ML souscrite au niveau du Contrat : Databricks, Inc. et Qlick Cloud (qui alimentent les modèles d'intelligence artificielle et d'apprentissage automatique de Kyriba): UE.