This Data Processing Addendum ("**Addendum**") forms part of the agreement between the customer identified in an order form or agreement ("**Customer**") and Kyriba for the procurement of Kyriba's online solution and related services (the "**Agreement**") to reflect the parties' agreement with regard to the processing of Customer Personal Data and replaces and supersedes any existing provision regarding Customer Personal Data in the Agreement. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. The parties understand that personal information may be processed by Kyriba on behalf of Customer ("**Customer Personal Data**"). Customer Personal Data includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to, directly or indirectly, a particular individual, consumer, data subject, or household, or is defined as "personally identifiable information," "personal information," "personal data," or similar term under Applicable Data Protection Law. "**Applicable Data Protection Law**" means, if and to the extent applicable. (a) the UK Data Protection Act 2018; (b) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**"); (c) as of January 1, 2020, the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 *et seq*. ("**California Consumer Privacy Act**" or "**CCPA**"); and (d) any other data protection laws, rules, regulations, self-regulatory guidelines, or implementing legislation applicable to Kyriba's processing of Customer Personal Data. Words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in Applicable Data Protection Law. The parties acknowledge and agree that Customer is the controller or business that determines the purpose for and the manner in which Customer Personal Data is processed by Kyriba. The parties agree that control of and responsibility for such Customer Personal Data shall at all times remain with Customer, Kyriba is the processor or service provider that processes Customer Personal Data under this Addendum and according to Customer's instructions.

2. Kyriba will process Customer Personal Data in accordance with Applicable Data Protection Law and solely for the purpose of providing the SaaS Services to Customer. Kyriba will not otherwise (i) process Customer Personal Data for purposes other than those set forth in this Addendum or as instructed by Customer's documented written instruction; (ii) disclose Customer Personal Data to third parties other than Kyriba's affiliates or subsidiaries, for the aforementioned purposes or as required by law; (iii) sell Customer Personal Data; (iv) retain, use, or disclose Customer Personal Data outside of the direct business relationship between Kyriba and Customer. Kyriba certifies that it understands these restrictions and will comply with them. If Kyriba must process Customer Personal Data as otherwise required by applicable law, Kyriba shall inform Customer of that legal requirement before processing Customer Personal Data, unless that law prohibits such disclosure on important grounds of public interest. Notwithstanding the above, to the extent any Customer Personal Data becomes "deidentified" or in the "aggregate" as those terms are defined under Applicable Data Protection Law, Kyriba may use such information for any commercial purpose in accordance with Applicable Data Protection Law, including but not limited to developing analytics, and may retain, use and disclose such information for such purpose, without restriction. The purpose and duration of the processing, its nature, the type of Customer Personal Data subject to processing and the categories of data subjects are specified in the Data Protection Schedule attached hereto and incorporated by reference herein.

3. In the event Customer Personal Data relates to EU data subjects, Kyriba will comply with the requirements set forth in Article 28 of the GDPR and the description of processing in the Data Protection Schedule attached hereto. Accordingly, Kyriba shall (i) ensure that Kyriba employees authorized to process Customer Personal Data under this Addendum are bound by confidentiality terms substantially similar to those of the Agreement or the appropriate statutory obligation of confidentiality, (ii) taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, maintain reasonable security measures and appropriate technical and organizational measures referred to in Article 32 of the GDPR for the protection, confidentiality, and integrity of Customer Personal Data, (iii) regularly monitor compliance with these measures, and shall not materially decrease the overall security of the SaaS Services during its provision of the SaaS Services pursuant to the Agreement, (iv) to the extent legally permitted, promptly notify Customer if Kyriba receives a request from an individual, consumer, or data subject to exercise their rights under Applicable Data Protection Law or receives a request or complaint from a supervisory authority or other third party ("**Request**"), (v) taking into account the nature of the

processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the individual, consumer, or data subject's rights, and shall not respond to such Requests without written approval from Customer, except as necessary to comply with Applicable Data Protection Law, (vi) upon Customer's written request, and subject to Section 6.3 (Customer Data) of the Agreement, delete or return all Customer Personal Data to Customer within sixty (60) days after termination of the Agreement for any reason or if Customer Personal Data is no longer needed to perform the SaaS Services; however, Kyriba may retain Customer Personal Data where necessary for Kyriba to comply with applicable law or legal obligation, or its rights or those of a third party, and (vii) make available to Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in this Section and allow for, to the extent required by law, contribution to audits, including inspections, conducted by Customer or another auditor mandated by Customer. Such auditor will have to be bound by confidentiality undertakings at least as stringent as those set out in the Agreement. To the extent legally permitted, Customer shall be responsible for any costs arising from Kyriba's provision of assistance hereunder.

4. Kyriba uses sub-processors to carry out specific processing activities, such as hosting or maintenance. Sub-processors used as at the date of the present addendum are specified in the Data Protection Schedule attached hereto. In addition, Customer provides general written authorization to Kyriba to engage another sub-processor in connection with Customer's use of the SaaS Services. If Kyriba wishes to replace one of its existing sub-processors or hire a new sub-processor ("**Change**"), Kyriba will inform Customer in advance of any proposed changes in connection with Customer's use of the SaaS Services; thereby giving Customer the opportunity to object to such Change. Customer has a maximum period of two (2) business days from the date of receipt of this information to expressly object to the Change on reasonable grounds by sending a notice to Kyriba. Such notice shall set out the reasons for such objection. In the event Customer sends a notice objecting to the new sub-processor, the parties will seek to resolve the issue through a mutually agreeable understanding. Kyriba will use commercially reasonable efforts to make available to Customer a change in the SaaS Services or Customer's configuration thereof to avoid the processing of Customer Personal Data by the objected-to new sub-processor. If five (5) days before the effective date of the Change, the parties have failed to reach a common understanding, Customer will be entitled to terminate the Agreement with effect as at the effective date of the Change. If Customer does not terminate the Agreement pursuant to this Section, Customer will be considered as having agreed to the Change. This termination right is Customer's sole and exclusive remedy if Customer objects to any new sub-processor. Kyriba will sign a written agreement with any sub-processor it engages to ensure that such sub-processor complies with the provisions of this Section and meets the requirements laid down in the Applicable Data Protection Law. Kyriba will remain responsible and liable for the compliance by any such sub-processor with the terms of this Section.

5. Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data. Customer represents and warrants to Kyriba that, in respect of all Customer Personal Data, Customer has the necessary authority, license or consent to provide Customer Personal Data and has a lawful basis (including all legally required notices and consents), has complied (and will continue to comply) with all Applicable Data Protection Law, in particular for the sharing, transmission, and processing of Customer Personal Data with, to, and by Kyriba for the purposes of the SaaS Services and the Agreement, and Kyriba's processing of Customer Personal Data in accordance with Customer's instructions will not cause Kyriba to violate any Applicable Data Protection Law.

6. Customer acknowledges and agrees that Customer Personal Data may be transferred outside European Union countries to countries recognized by the European Commission as countries where there is an adequate level of protection as updated from time to time ("**Authorized Location**"). During the term of the Agreement, the parties shall comply with the terms and conditions of the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Commission as may be updated or otherwise amended ("Standard Contractual Clauses"), a current copy is attached hereto as Attachment 2, and the Standard Contractual Clauses are fully incorporated into this Addendum. In the event Customer agrees to a transfer of Customer Personal Data outside an Authorized Location, such transfer shall be subject to the execution between the Parties of the EU Standard Contractual Clauses or any other alternative mean validated by GDPR.

7. Kyriba maintains security incident management policies and procedures, and upon occurrence of any actual security breach affecting Customer Personal Data transmitted, stored, or otherwise processed by Kyriba, (the "**Information Security Breach**"), Kyriba shall:

(i) notify Customer, within 72 hours of confirmation of, and without undue delay, the Information Security Breach, and deliver to Customer a written report regarding the nature of the Information Security Breach, the categories and the approximate number of Customer Personal Data affected, if such information is available. Kyriba shall also describe the likely consequences of the Information Security Breach on Customer Personal Data as well as the reasonable measures Kyriba deems necessary and reasonable to remediate the cause of such Information Security Breach, to the extent the remediation is within Kyriba's reasonable control, including, where appropriate, to mitigate its possible adverse effects; and

(ii) Proceed as quickly as reasonably possible (a) to mitigate any adverse impact or other harm to Customer and any affected individuals, consumers, and data subjects resulting from such Information Security Breach; and (b) to prevent similar Information Security Breaches from occurring in the future. Kyriba will keep Customer fully informed of all stages of its investigation and all actions taken as a result thereof.

This Addendum shall be effective as of the effective date of the Agreement and shall remain effective for so long as the Agreement remains in effect. Only a written agreement signed by authorized representatives of both parties can modify this Addendum. In the event of inconsistency between the Agreement and the Addendum provisions, the parties agree that the provisions of this Addendum will prevail.

ATTACHMENT 1 TO THE ADDENDUM: DATA PROTECTION SCHEDULE

This Data Processing Schedule is part of the Addendum and of the Agreement and details the characteristics of processing Customer Personal Data.

1. Description of processing

Type of Customer Personal Data	Categories of individuals, consumers, or data subject	Purpose of processing	Duration of processing
Determined and controlled by Customer, in Customer's discretion; and may include, without limitation, name, email address, phone number, IP address, Ad ID, username and password, government issued identification, and financial accounts	Customer's employees, representatives, contractors, partners, vendors, persons of interest, and/or customers	Provision of SaaS Services under the Agreement	Duration of the processing shall correspond to the duration of the Agreement except where otherwise required by applicable law or legal obligation, or for Kyriba to protects its rights or those of a third party.

2. Subprocessors

Affiliates of Kyriba (for purposes of implementation, support and maintenance)

FireEye, Inc. DBA Mandiant (if the event of a data breach, for purposes of data breach investigation and remediation)

Amazon Web Services, Inc. (for purposes of providing infrastructure for Kyriba's application)

Iron Mountain Incorporated (for purposes of providing infrastructure for Kyriba's application)

Equinix (France) SAS (for purposes of providing infrastructure for Kyriba's application)

Sage Intacct, Inc. (for purposes of invoice generation and management)

Salesforce.com, Inc. (for administration of contract)

Salesforce.com EMEA Limited (for administration of contract)

Digital Guardian, Inc. (for data loss prevention and monitoring)

Netskope, Inc. (in the event of data breach, provides data loss prevention solution)

Mimecast North America, Inc. (provides email security tool to protect Kyriba against spam, viruses and malware)

Splunk, Inc. (provides security analytics tool to identify anomalous activity within Kyriba's environment)

SIA S.P.A. (provides connection to Italian banking protocol)

Fujitsu FIP Corporation (provides connection to Japanese banking protocol)

ServiceNow, Inc. (provides tool to ticket, track and process customer support requests)

It is understood that Kyriba may change, substitute or add subprocessors in accordance with Section 4 of the Addendum.

ATTACHMENT 2 TO THE ADDENDUM: EU STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: ……

Entity that has entered into the Agreement, which this Addendum forms a part of and its EU affiliates

(the data **exporter**)

And

The names of the data importing organisations are set forth in the table below:

Data Importer:
KYRIBA CORP.
KYRIBA SEA PTE LTD
KYRIBA SOFTWARE TECHNOLOGY (SHANGHAI) LIMITED
KYRIBA ENGINEERING LIMITED LIABILITY COMPANY
KYRIBA JAPAN CO., LTD
Kyriba UK LTD
RIM TEC, INC.

(each a "data importer" and together the "data importers") each a "party"; together "the parties",

WHEREAS, pursuant to an agreement between the data exporter and data importer or data importer's affiliate, data importer provides to data exporter online treasury management and liquidity software as a service, and related support, maintenance, implementation and training services, and in connection with such services, data importer may process personal data;

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same

conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely by the laws of France.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely by the laws of France.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer: KYRIBA CORP.

Name (written out in full):

Position:

Signature…….

On behalf of the data importer: KYRIBA UK LTD
Name (written out in full):
Position:

Signature…….

On behalf of the data importer: KYRIBA SEA PTE LTD

Name (written out in full):
Position:

Signature…….

On behalf of the data importer: KYRIBA SOFTWARE TECHNOLOGY (SHANGHAI) LIMITED

Name (written out in full):
Position:

Signature…….

On behalf of the data importer: KYRIBA ENGINEERING LIMITED LIABILITY COMPANY

Name (written out in full):
Position:

Signature…….

On behalf of the data importer: KYRIBA JAPAN CO., LTD

Name (written out in full):
Position:

Signature…….

On behalf of the data importer: RIM TEC, INC.

Name (written out in full):
Position:

Signature…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

To receive services related to the activities of the data importer

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

A US company and its affiliates, providing treasury management and liquidity solution on a software as a service basis and associated support, maintenance, implementation and training services

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees, independent contractors, customers, suppliers and payees of data exporter and its subsidiaries

Categories of data

The personal data transferred concern the following categories of data (please specify):

First name, last name, title, contact details (telephone number, mobile phone number, email address, fax number, mailing address), system access/usage, authorization data, bank account, financial information, and government issued identification.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Collecting, storing, deleting, altering, transferring and other processing as set forth in the agreement between the data exporter and data importer or data importer's affiliate for the provision of data importer's online treasury management and liquidity software as a service, and related support, maintenance, implementation and training services.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER: Kyriba Corp.

Name:

Authorised Signature ……

DATA IMPORTER: KYRIBA SEA PTE LTD.

Name:

Authorised Signature ……

DATA IMPORTER: KYRIBA SOFTWARE TECHNOLOGY (SHANGHAI) LIMITED
Name:

Authorised Signature ……

DATA IMPORTER: KYRIBA ENGINEERING LIMITED LIABILITY COMPANY
Name:

Authorised Signature ……

DATA IMPORTER: KYRIBA JAPAN CO., LTD
Name:

Authorised Signature ……

DATA IMPORTER: KYRIBA UK LTD
Name:

Authorised Signature ……

DATA IMPORTER: RIM TEC, INC.
Name:

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Kyriba's SaaS platform is audited by a reputable third-party accounting firm on a semi-annual basis to ensure it meets the Statement for Attestation Engagement No. 18 (SSAE 18)/Service Organization Control (SOC) 1 and on an annual basis to ensure it meets SOC2 standards. The SOC 2 Type II certification, defined by the American Institute of Certified Public Accountants (AICPA), is recognized worldwide as one of the strictest audit standards for service providers. This certification has been designed to meet the needs of the growing number of IT and cloud computing companies. It allows the audited organization to demonstrate that it meets and exceeds the industry's accepted standards governing controls and protection of all hosted and processed data, on behalf of Kyriba's clients.

Kyriba has a best practice Risk Management Framework which manages its security risks by depicting a security risk management life-cycle, and sets the requirements for understanding, assessing, responding, and monitoring security risks at Kyriba.

Kyriba's risk assessment methodology is based on:

- ISO/IEC 27001:2018
- ISO/IEC 31000 and 31010 Risk Management

To add additional detail and structure to the methodology, Kyriba incorporated selected NIST risk assessment controls referencing risk assessments, the management of information security risk and technical guide to information security testing.

For an independent validation of the implementation of security controls, Kyriba hires highly reputable outside firms on an-going basis to perform penetration testing against its web application as well as vulnerability scanning. Kyriba has also implemented a software security program that aligns Kyriba with secure software development practices as outlined by OWASP and SANS. This program includes static code analysis that is conducted on the Kyriba codebase, automated dynamic code analysis, and secure code training for Kyriba developers and security personnel.

Kyriba undergoes an annual Business Impact Analysis (BIA) and an annual SIG 7 self-assessment (cloud module included).

Kyriba's Risk and Compliance organization is well versed and certified in the areas of Risk and Compliance with certifications ranging from CISSP, CRISC, GIAC and PMP. The Risk and Compliance team has a deep understanding of various security frameworks such as ISO, PCI, FedRAMP, DOD and NIST; as well as SOC Compliance.

Customer Data Privacy Policy

Kyriba manages a Customer Data Privacy Policy which summarizes the procedures of Kyriba Corp. in regard to end user data collected on behalf of its customers via the Kyriba enterprise applications and related services. The Customer Data Privacy Policy is maintained, enforced and monitored by the Office of the Chief Information Security Officer and is reviewed at least annually as to its accuracy and applicability.

Retention & Disposal of Customer Data

Unless a law or regulation specifically requires otherwise, Kyriba will retain personal data only for as long as it has a reasonable need for such personal data. All personal data residing on the active-server database that is no longer needed shall be rendered inaccessible in accordance with industry standards within a reasonable timeframe once it has been determined that such personal data is no longer needed. For the Kyriba Enterprise Applications, copies of production data may be used in external testing environments; however, any such data that contains personal data is protected in the same manner and by the same controls as further described in the Customer Data Privacy Policy.

Disclosure to Third Parties
Kyriba may share personal data with Kyriba's subsidiaries and affiliates. Kyriba may also share personal data with service providers we have retained to perform services on Kyriba's behalf. Kyriba requires service providers to whom it discloses personal data and who are not subject to either the laws based on the European Union Data Protection Directive or the Swiss Federal Act on Data Protection, as applicable, to either (i) enter into the standard contractual clauses for the international transfer of personal data adopted by the European Commission or (ii) be subject to another European Commission adequacy finding (e.g., companies located in Canada).

In case where Kyriba would be requested to share personal data with law enforcement authorities or State security bodies, Kyriba will inform the controller of any legally binding request, unless otherwise prohibited. The request for disclosure will be put on hold and the competent supervisory authorities will be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).

If in specific cases the suspension and/or notification are prohibited, Kyriba will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

In any case, transfers of personal data by Kyriba to any public authority will not be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Security System requirements
Production systems maintain a high availability of 99.9% (redundant infrastructure) 24 hours/7 days a week. Firewall policies are in place and are managed by Kyriba's technical operations team.

Security zones are protected by firewalls. Modifications to firewall rules are executed according to policy and are logged and auditable.

Encryption Key Management System policy:
Access to stored Encryption Keys are recorded for audit and incident investigation if needed. Security Key Management follows the intent of Federal Information Processing Standards (FIPS 140-2). Policies are in place to provide an overall environment that strives to maintain:

- Security: least privilege access, overseeing security monitoring of the system
- Availability: ensuring that minimum uptimes are met
- Processing Integrity: overseeing interfaces / jobs
- Confidentiality: treating client information as confidential

Data classification
Data classification is in place and is used to define protection requirements, access rights and restrictions, and retention and destruction requirements and parameters. Restricted client data will be rendered inaccessible at the end of the contract at this time. In the future, this data could be deleted or otherwise erased in accordance with industry standard deletion/wiping processes. Disks storing client data are encrypted at rest at the Kyriba SAN hardware level and these disks become unreadable if removed from the Kyriba SAN array.

Personal Data
Kyriba will take reasonable precautions to protect personal data in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction. Kyriba uses physical, electronic and administrative security measures to protect personal data. Kyriba limits access to personal data to those persons in Kyriba's organization that have a specific business purpose for maintaining and processing the personal data or approved third party vendors that are involved in the processing of the personal data. Individuals who have been granted access to personal data will be made aware of their specific responsibilities to protect the security, confidentiality, and integrity of the personal data. Kyriba conducts periodical audits such as SOC1, SOC2, network and/or application intrusion testing, source code audit, other recurring and/or scheduled audits related to architecture or processes and procedures. Audits are run by reputable third parties. The Office of the Chief Information Security Officer is in charge to order all audits necessary to be compliant with Kyriba's commitments related to the client data security and integrity.

Incident Management
Kyriba has a documented Incident Management Policy in place for addressing incidents. A Special Work Actions Team (SWAT Team) is in place and utilized to solve critical incidents that may arise with potential impact to the security, availability, integrity, and confidentiality of Kyriba technology and data.
Kyriba has created internal documentation used to guide through the mechanics of how to initiate the SWAT team, definition of SWAT team members, and is considered highly sensitive and confidential and therefore not released outside the company.

Disaster Recovery
"Management Crisis Governance - SWAT", current version, is the Kyriba guideline to strictly apply a disaster recovery plan. Kyriba has internal documentation used to guide through the mechanics of how to initiate the SWAT team, definition of SWAT team members, and is considered highly sensitive and confidential and therefore not released outside the company.

Incremental backups of the Kyriba application and databases are performed to a local backup server on a daily basis. Full backups are performed on a bi-weekly basis. Backups are additionally replicated to a remote disaster recovery server located at the alternate data center. Kyriba Technical Operations team reviews the status of the backups to ensure successful completion of the backup to the local backup server and the replication to the remote Disaster Recovery server.

Services monitoring
Service Level Agreements (SLAs) are normally in place between Kyriba and its clients. Monitoring tools are in place for ongoing monitoring which is performed in order for Kyriba to measure itself against these commitments. Load balancing is used to distribute the workload across multiple servers and virtual machines within the Kyriba application architecture. Multiple load balancers are used within the system to help maximize system scalability.

The internal Kyriba Technical Operations team is tasked with monitoring and assuring the availability of all systems that run the Kyriba production platforms around the globe.

Disclosure Control
Measures are taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that transfers are secure and are logged. These measures shall include:
● Encryption using a VPN for remote access
● Encryption and other secure methods (e.g. sFTP) for transport and communication of data
● Creation of an audit trail of data transfers related to the services

Internal Documentation
Kyriba shall implement internal documentation in order to assess the exposition of personal data processed by Kyriba to requests and controls by surveillance and security authorities.