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 and UK General Data Protection Regulation 2021 ("UK GDPR"); (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 (Controller to Processor) as set out in the Commission Decision of June 4, 2021 (2021/91)as may be amended, updated, substituted or replaced from time to time ("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, 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. 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) : USA

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

Iron Mountain Incorporated (for purposes of providing infrastructure for Kyriba's application) : N/A for EU clients

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

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

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

Salesforce.com EMEA Limited (for administration of contract) : EU

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

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

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

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

Carbon Black, Inc. (anti-malware used on Kyriba's solution for endpoint detection and response) : US

Society for Worldwide Interbank Financial Telecommunication SCRL (provides access and use to SWIFT messaging platform) : US

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

Fujitsu FIP Corporation (provides connection to Japanese banking protocol) : Japan

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

OwnBackup Inc. (provides backup of Salesforces solution) US

Planview Delaware, LLC (provides project management tool to facilitate client implementation projects) : US

3CLogic Inc. (provides tool for customer support and call center management) : EU except phone number in US

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

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.
b. The Parties:
   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

   have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix

to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified

in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

MODULE TWO: Transfer controller to processor

a. OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least seven (7) business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.
e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

MODULE TWO: Transfer controller to processor

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   ii. refer the dispute to the competent courts within the meaning of Clause 18.
d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority
b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[12];
   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the

data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
ii. the data importer is in substantial or persistent breach of these Clauses; or
iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18
Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
b. The Parties agree that those shall be the courts of France.
c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
d. The Parties agree to submit themselves to the jurisdiction of such courts.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

[6] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

[7] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

[11] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

EXPLANATORY NOTE:
It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can [be] achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. The Client or Customer identified in the SaaS Agreement.

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: KYRIBA SEMEA

Address: …247 Bureaux de la Colline 92210 SAINT-CLOUD FRANCE

Contact person's name, position and contact details: DPO : privacy@kyriba.com

Activities relevant to the data transferred under these Clauses: Kyriba is a US and international 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 Importer:
KYRIBA CORP.
KYRIBA SEA PTE LTD
KYRIBA SOFTWARE TECHNOLOGY (SHANGHAI) LIMITED
KYRIBA ENGINEERING LIMITED LIABILITY COMPANY
KYRIBA ENGINEERING POLAND SP Z.O.O.
KYRIBA JAPAN CO., LTD
KYRIBA UK LTD
RIM TEC, INC.

1. Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

Client's employees, representatives, contractors, partners, vendors, persons of interest, and/or customers

Categories of personal data transferred

Determined and controlled by Client, 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

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfer is continuous.

Nature of the processing

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.

Purpose(s) of the data transfer and further processing

Provision of data importer's online treasury management and liquidity software as a service, and related support, maintenance, implementation and training services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

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.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

When sub-processors are involved (see list provided), transfer is limited to transfer necessary for the performance of the agreement, and for its duration.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

French Data Authority - CNIL

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:
The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

- *Measures of pseudonymisation and encryption of personal data*
- *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*
- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*
- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*
- *Measures for user identification and authorisation*
- *Measures for the protection of data during transmission*
- *Measures for the protection of data during storage*
- *Measures for ensuring physical security of locations at which personal data are processed*
- *Measures for ensuring events logging*
- *Measures for ensuring system configuration, including default configuration*
- *Measures for internal IT and IT security governance and management*
- *Measures for certification/assurance of processes and products*
- *Measures for ensuring data minimisation*
- *Measures for ensuring data quality*
- *Measures for ensuring limited data retention*
- *Measures for ensuring accountability*
- *Measures for allowing data portability and ensuring erasure]*

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

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, for all services provided except FireApps. 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 is also ISO27001 certified.

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 but no customer data is used in test or development environment unless it has been anonymized ; 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).

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. All disks storing client data are encrypted at rest using 256 bit encryption.

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, ISO 27001, 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 Service Excellence Action Team (SEAT) 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 SEAT team, definition of SEAT team members, and is considered highly sensitive and confidential and therefore not released outside the company.

Disaster Recovery
Kyriba has internal documentation used to guide through the mechanics of how to declare a Disaster, the SEAT team, definition of SEAT 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 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.

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.

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.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:
This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

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) : USA

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

Iron Mountain Incorporated (for purposes of providing infrastructure for Kyriba's application) : N/A for EU clients

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

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

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

Salesforce.com EMEA Limited (for administration of contract) : EU

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

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

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

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

Carbon Black, Inc. (anti-malware used on Kyriba's solution for endpoint detection and response) : US

Society for Worldwide Interbank Financial Telecommunication SCRL (provides access and use to SWIFT messaging platform) : US

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

Fujitsu FIP Corporation (provides connection to Japanese banking protocol) : Japan

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

OwnBackup Inc. (provides backup of Salesforces solution) US

Planview Delaware, LLC (provides project management tool to facilitate client implementation projects) : US

3CLogic Inc. (provides tool for customer support and call center management) : EU except phone number in US