kyriba

Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is effective as of the Addendum Effective Date and forms part of the agreement (the "**Agreement**") between the Customer and Kyriba (each a "**Party**" or collectively the "**Parties**") for the provision of the SaaS Services. This Addendum sets forth the Parties understanding with regard to the Processing of Customer Personal Data and replaces and supersedes any existing provision regarding Customer Personal Data in the Agreement or otherwise.

1. Definitions.

a. **"Addendum Effective Date"** means the effective date of the Agreement and shall remain effective for so long as the Agreement remains in effect.
b. **"Anonymized"** means the stripping and masking of Customer Personal Data, using obfuscation and non-reversible hashing cryptographic algorithms, such that the data in no way identifies or is connected to any person. "Anonymized" shall also mean making it impossible to identify individuals within data sets and is an irreversible process. When this anonymization is effective, the data is no longer considered as personal data and the requirements of the GDPR are no longer applicable.
c. "**Applicable Data Protection Law**" means, if and to the extent applicable, (a) the UK Data Protection Act 2018 and the EU GDPR, as it forms part of retained EU law in the United Kingdom ("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**"); data protection laws in the U.S., including but not limited to the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 *et seq*, as amended by the California Privacy Rights Act of 2020, and regulations issued thereunder (collectively "**US Data Protection Laws**"); and (d) any other data protection laws, rules, regulations, self-regulatory guidelines, or implementing legislation applicable to the SaaS Services and Kyriba's processing of Customer Personal Data.
d. **"Customer Personal Data"**- mean the personal information that may be provided by Customer to Kyriba that 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.
e. "**Processing"**, **"processed"** or **"process"** has the same meaning as set forth in the Applicable Data Protection Law.
f. "**Subprocessor**" has the same meaning as set out in the Applicable Data Protection Law and means any Processor (including any third party and any Kyriba affiliate, but excluding an employee of Kyriba) appointed by or on behalf of Kyriba or to process Customer Personal Data.
g. Words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in Applicable Data Protection Law.
h. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.
i. In the event of inconsistency between the Agreement and the Addendum provisions, the Parties agree that the provisions of this Addendum will prevail.

2. Parties' Relationship.

a. Customer is the "controller" (as set out in the Applicable Data Protection Law) or business that determines the purpose for and the manner in which Customer Personal Data is processed by Kyriba. The control of and responsibility for the Customer Personal Data shall remain with Customer at all times.
b. Kyriba is the "processor" or service provider that processes Customer Personal Data according to Customer's documented instructions.

3. Processor General Obligations.

a. 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 (i) process Customer Personal Data for purposes other than those set forth in this Addendum, as required by Customer's documented instructions, or as required by applicable law; (ii) disclose Customer Personal Data to third parties other than Kyriba's affiliates or subsidiaries, for the aforementioned purposes or as

required by applicable law; (iii) sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Customer Personal Data to any third party for monetary or other valuable consideration; or (iv) retain, use, or disclose Customer Personal Data outside of the direct business relationship between Kyriba and Customer.

b. Kyriba shall not combine Customer Personal Data that Kyriba receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person, or collects from its own interaction with an individual, provided that Kyriba may combine personal information to perform any business purpose as defined under Applicable Data Protection Laws.
c. If Kyriba must process Customer Personal Data as otherwise required by applicable law to the SaaS Services, Kyriba will inform Customer of that legal requirement before processing Customer Personal Data, unless that law prohibits such disclosure.
d. 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 this Addendum, Attachment 1 – Data Processing Schedule attached hereto and incorporated herein ("Attachment 1").
e. Kyriba certifies that it understands and will comply with the processing obligations set forth in this Addendum.

4. Controller General Obligations.

a. Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data.
b. Customer has complied and will continue to comply with all Applicable Data Protection Law.
c. 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.
d. Customer certifies that Kyriba's processing of Customer Personal Data in accordance with Customer's documented instructions and this Addendum will not cause Kyriba to violate any Applicable Data Protection Law.
e. Customer has, and will continue to have, the right to transfer, or provide access to, the Customer Personal Data to Kyriba for receiving, transferring and processing in accordance with this Addendum.
f. Customer has undertaken, and shall continue to undertake as required under Applicable Data Protection Law, all such data protection impact assessments and/or security assessments to facilitate the transfer of the Customer Personal Data to Kyriba (whether within or outside the country the Customer Personal Data was first collected). Notwithstanding the foregoing and in any event, nothing shall prohibit Kyriba from accessing, receiving, storing, using, or otherwise processing the Customer Personal Data outside of the receiving country in accordance with the terms of this Addendum.
g. Customer shall immediately notify Kyriba of any and all complaints, claims, investigations, and/or enquiries from any regulatory authorities that may pertain to or involve the Customer Personal Data that Kyriba is processing.
h. Where applicable, Customer shall not transfer or disclose any Customer Personal Data containing "state secrets" and/or "important data" as defined under Applicable Data Protection Law, or which is otherwise prohibited from leaving the transferring country under Applicable Data Protection Law.

5. Compliance with GDPR Article 28.

a. In the event Customer Personal Data relates to EU or UK data subjects, as applicable, Kyriba will comply with the requirements set forth in Article 28 of the GDPR or UK GDPR, where applicable, and the description of processing outlined in Attachment 1.
b. Kyriba will (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, except as necessary to comply with Applicable Data Protection Law, and (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 Kyriba's rights.

6. **Compliance Verifications.**
   a. Kyriba will make available to Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in this Addendum to Customer and allow for, to the extent required by law, contribution to audits, including inspections, conducted by Customer or another auditor, not competitor to Kyriba, mandated by Customer.
   b. Such auditor will have to be bound by confidentiality undertakings at least as stringent as those set out in the Agreement. In the event of any requested review, Customer shall give Kyriba reasonable notice of the reviews shall be conducted off premises, subject to Kyriba policies, and shall not unreasonably interfere with or disrupt Kyriba's business activities. Audits shall take place within normal business hours unless the review is required to be carried out on an emergency basis by a regulatory authority.
   c. To the extent legally permitted, Customer shall be responsible for any reasonable and demonstrable costs arising from Kyriba's provision of assistance that are over and beyond those required by law and pursuant to this subsection (c). Any of the above reports shall constitute confidential information of the Parties.

7. **Onward Transfers.**
   a. Customer acknowledges and agrees that Customer Personal Data may be transferred outside the European Economic Area, the United Kingdom, or other jurisdictions in which Customer Personal Data originated from ("**Onward Transfer**"), to countries recognized by the European Commission, or the Information Commissioner's Office UK ("**ICO**"), or other jurisdictions where applicable, as countries where there is an adequate level of protection as updated from time to time ("**Authorized Location**").
   b. During the term of the Agreement, the Parties, or Kyriba and its Sub-processors, where applicable, shall comply with the terms and conditions of the applicable Standard Contractual Clauses ((Module 2 – Controller to Processor) or Module 3 - Processor to Sub-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 ("**EU Standard Contractual Clauses**"), or a form equivalent to the Standard Contractual Clauses, as approved by the ICO, from time to time, for the export of Customer Personal Data of UK data subjects, outside of the UK ("**UK Standard Contractual Clauses Addendum**") for such Onward Transfers.
   c. In the event Customer agrees to an Onward Transfer, such Onward Transfer shall be subject, where applicable, to the EU Standard Contractual Clauses, the UK Standard Contractual Clauses Addendum, or any other alternative mean validated by Applicable Data Protection Law, all of which shall be incorporated by reference and deemed executed by reason of each Parties' signature on the Agreement. The applicable clauses are available at: EU Standard Contractual Clauses [[English] www.kyriba.com/contracts/eusccs] / [[French]www.kyriba.com/contracts/uecct] and UK Standard Contractual Clause Addendum [www.kyriba.com/contracts/dpa/uksccs].
   d. The required details of the Onward Transfers as required by the EU Standard Contractual Clauses and the UK Standard Contractual Clauses are as set forth in Attachment 2 – Appendix to the Standard Contractual Clauses attached hereto and incorporated herein.

8. **Subprocessors.**
   a. Kyriba uses Subprocessors (as set out in the Applicable Data Protection Law) 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.

b. Subprocessor Changes. If Kyriba wishes to replace one of its existing sub-processors or hire a new sub-processor ("**Change**"), pursuant to the following:
   i. 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 seven (7) 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.
   ii. 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.
   iii. 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.
   iv. 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.
   v. 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.

9. **Information Security Breach.** 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 will: notify Customer, without undue delay after becoming aware of it, 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, where possible, 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 Proceed as quickly as reasonably possible (i) 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 (ii) 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.

10. **Data Aggregation.** Notwithstanding anything to the contrary and to the extent any Customer Personal Data becomes Anonymized, Kyriba may monitor, collect and 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.

kyriba

ATTACHMENT 1 - DATA PROCESSING SCHEDULE

This Data Processing Schedule is part of the Addendum 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, 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.

2. Subprocessors

Please see Attachment 2, Annex III below.

It is understood that Kyriba may change, substitute or add subprocessors in accordance with Section 8 of the Addendum.

ATTACHMENT 2 - APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

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.

kyriba

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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]*

- **Name:** The Customer identified in the Agreement and/or the applicable Kyriba entity identified in the Agreement.

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

- **Name**: Kyriba Corp.
- **Address**: 4435 Eastgate Mall, Suite 200, San Diego, California 92121
- **Contact person's name, position and contact details**: Kyriba Data Privacy Team: (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 SEMEA
KYRIBA SEA PTE LTD
KYRIBA SOFTWARE TECHNOLOGY (SHANGHAI) LIMITED
KYRIBA (CHONGQING) SOFTWARE DEVELOPMENT CO.
KYRIBA HK LIMITED
KYRIBA JAPAN CO., LTD
RIM TEC, INC.

- **Role (controller/processor)**: processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

Customer's employees, representatives, contractors, partners, vendors, persons of interest, and/or clients

Categories of personal data transferred

Determined and controlled by Customer at Customer's discretion; and may include, without limitation, name, email address, phone number, IP address, Ad ID, username and password, 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.

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 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

kyriba

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

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:

1. Affiliates of Kyriba (for purposes of implementation, support and maintenance).
2. Amazon Web Services, Inc. (for purposes of providing infrastructure for Kyriba's application): EU, Canada, and US (where applicable).