Gurock Data Processing Agreement
as Data Processors

This Data Processing Agreement ("**DPA**") amends and is incorporated into the terms of any existing and currently agreement between Gurock Software GmbH ("**Gurock**") and the counterparty agreeing to these terms ("**Customer**"), which, as a result, Gurock accesses, collects, acquires, receives, transfers, processes, and/or uses Personal Data (defined below) from or on behalf of Customer or its Affiliates ("**Agreement**").

All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement. If there is any inconsistency or conflict between this DPA and any Agreement in effect between Gurock and Customer, then as it relates to data protection or processing, the terms of this DPA shall govern and control and shall survive any termination or expiration of the previous Agreement. This DPA only applies to the extent Gurock processes Personal Data on behalf of Customer. If you are accepting these terms, you warrant that: (a) you have full legal authority to bind Customer to these data processing terms; (b) you have read and understand these data processing terms; and (c) you agree, on behalf of Customer, to these data processing terms. If you do not have the legal authority to bind Customer, please do not accept these data processing terms. Gurock and Customer agrees as follows:

1. Definitions

(a) "**Affiliate**" means an entity that a party controls or is controlled by, or with which a party is under common control. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or equivalent ownership interest in an entity.

(b) "**Applicable Laws**" means all applicable laws, rules, regulations, order, ordinances, regulations, guidance, and industry self-regulations.

(c) "**Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR, as well as, to the extent applicable, the data protection or privacy laws of any other country.

(d) "**GDPR**" means the EU "**General Data Protection Regulation**", Regulation 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, and repealing Directive 95/46/EC, as may be amended, modified, supplemented, restated, or superseded from time to time.

(e) "**Privacy Incident**" means any incident involving the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of, or access to, Personal Data.

(f) "**Services**" means the services Gurock is obligated to perform pursuant to the Agreements.

(g) "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**", and "**Processing**" shall have the meaning given to them in Chapter 1, Article 4 of the GDPR and their cognate terms shall be construed accordingly.

2. Processing of Personal Data

To the extent Gurock Processes any Personal Data on behalf of Customer and of its Affiliate(s) pursuant to an Agreement, Gurock represents and warrants that it shall (and shall ensure that all of its subcontractors shall) comply with the following obligations set forth in this Section 2:

(a) General Obligations. Gurock will process Personal Data in compliance with Applicable Law at all times. Subject to Applicable Law, Gurock will not disclose Personal Data to any third party without first obtaining Customer's written consent, unless otherwise required by Applicable Law. Gurock shall ensure that, at all relevant times during the Term of the Agreement, all Gurock personnel engaged in the Processing of Personal Data are aware of, and subject to, enforceable obligations to maintain the confidentiality of the Personal Data and to comply with the other relevant obligations and restrictions of this Agreement.

(b) Processing Only on Instructions from Customer. Gurock will process Personal Data solely for the purpose of performing the Services and in accordance with Customer's instructions as issued from time to time in writing. Gurock acknowledges that, with respect to any Personal Data subject to this Agreement, Gurock will act only as a Data Processor. Gurock will collect only such Personal Data during the course of performing the Services as is strictly necessary for Gurock to perform the Services. If Applicable Law (or any subcontractor) requires Gurock to conduct Processing that is or could be construed as inconsistent with Customer's instructions, then Gurock shall notify Customer promptly and prior to commencing the Processing. If Gurock believes that any instruction from Customer is in violation of, or would result in Processing in violation of Applicable Law, then Gurock shall notify Customer immediately.

(c) Details Related to the Processing of Personal Data. Details regarding the Processing of Personal Data are set forth on Appendix A. Customer may make reasonable amendments to Appendix A by written notice to Gurock from time to time as Customer reasonably considers necessary to meet the requirements of Applicable Law. Gurock agrees to reasonably notify Customer in writing if it believes that Appendix A is not accurate or otherwise does not meet the requirements of Applicable Law.

(d) Subcontractors. Gurock may subcontract the Processing of Personal Data when this is authorized by the Customer. By signing this DPA, Customer authorizes Gurock to use the subprocessors listed in Gurock's website. All Processing by subcontractors must be subject to a written agreement between Gurock and the subcontractor that (i) requires the subcontractor to comply with the same obligations and restrictions as provided in this Agreement; (ii) meets the requirements of Article 28(3) of the GDPR; and (iii) includes express guarantees by the subcontractor to implement technical and organizational measures to ensure that Processing satisfies all requirements of Applicable Law. When any new subprocessor is engaged during the term of this DPA, Gurock will, at least 30 days before the new subprocessor processes any Personal Data, inform Customer of the engagement, including the activities it will perform. Customer may object to any new subprocessor by terminating the Agreement immediately upon written notice to Gurock, on condition that Customer provides such notice within 90 days of being informed of the engagement of the new subprocessor as described in this section. This termination right is Customer's sole and exclusive remedy if Customer objects to any new subprocessor. Gurock shall remain responsible for the Processing of the Personal Data.

(e) Personnel. Gurock shall, and shall cause each subcontractor to, take reasonable steps to ensure the reliability of all personnel who may have access to the Personal Data. Furthermore, Vendor shall ensure in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and comply with Applicable Law in the context of that individual's duties to Vendor.

(f) Cooperation to Facilitate Responses. Gurock will, at no additional cost to Customer taking into account the nature of the Processing, assist the Customer:

i. by appropriate technical and organizational measures and in so far as it is possible, in fulfilling the Customer's obligations to respond to requests from data subjects exercising their rights; and

ii. in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation;

(g) Cross-Border Transfers. Gurock may only Process, access or transfer Personal Data across national borders in compliance with Applicable Law.

i. If Gurock collects, stores or otherwise Processes Personal Data in the European Economic Area or Switzerland, then Gurock will follow adequate safeguards for the privacy of all relevant Data Subjects and require any applicable subcontractors to do the same. Without limiting the generality of the foregoing, transfers by Gurock (if any) of Personal Data from the European Economic Area or Switzerland to another location must be: (A) to a country providing adequate protection of privacy rights (as deemed by the European Commission from time to time); (B) pursuant to the Standard Contractual Clauses set forth in Appendix B, as amended from time to time, issued by the European Commission, provided Gurock has secured all necessary approvals for the transfer from applicable governmental authorities; (C) authorized by all applicable governmental authorities in the European Economic Area or Switzerland, as the case may be, such as through Binding Corporate Rules approved by all applicable governmental authorities; or (D) to an entity or group of entities that has self-certified under the EU-U.S. Privacy Shield mechanism and which, at the

time of the transfer, is listed on the United States Department of Commerce Privacy Shield List as a current participant in the EU-U.S. Privacy Shield program in good standing.

(h) Retention and Deletion. Gurock may retain Personal Data only for the period of time required for Gurock to perform the Services, or such longer period required by Applicable Law, required pursuant to the Agreement or requested in writing by Customer. Gurock will permanently delete all copies of Personal Data in its possession or control at the expiration of such time period.

3. Technical and Organizational Security Measures

To the extent Gurock Processes any Personal Data on behalf of Customer or its Affiliate(s) pursuant to the Agreement, Gurock represents and warrants that it shall (and shall ensure that all of its subcontractors shall) comply with the following obligations set forth in this Section 3:

(a) Measures to be Implemented. Gurock will implement and maintain appropriate technical and organisational measures to protect the Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the personal data which is to be protected. Gurock, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural person, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

(b) Compliance. Gurock will observe and to the extent that it will not cause undue burden on Gurock, comply with all security and privacy policies, rules, and standards provided to Gurock by Customer form time-to-time.

(c) Technology Changes. Gurock will advise Customer of all changes in technology implemented from time to time which may be relevant to ensuring that an appropriate level of security is in place with respect to Personal Data.

(d) Privacy Incidents. If Gurock becomes aware of any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to the personal data that Gurock processes in the course of providing the Services (a "**Security Breach**"), Gurock will notify Customer without undue delay after having become aware of it and:

(i. provide Customer (as soon as possible) with a detailed description of the Security Breach; the type of data that was the subject of the Security Breach; and the identity of each affected person, as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Customer may reasonably request relating to the Security Breach);

(ii. take action immediately, at Gurock's own expense, to investigate the Security Breach and to identify, prevent and mitigate the effects of the Security Breach and to carry out any recovery or other action necessary to remedy the Security Breach; and

(iii. not release or publish any filing, communication, notice, press release, or report concerning the Security Breach without Customer's prior written approval except where Gurock is required by Applicable Law to make such disclosure prior to obtaining Customer’s written consent.

4. Audits

(a) Gurock will provide Customer, its auditors, and other representatives, at Customer’s cost and expense, once per calendar year, at a time mutually agreed upon by Gurock and Customer, access to Gurock’s security policies, practices and procedures, data flow diagrams, business continuity facilities, and records relating to the Services for the purpose of verify Gurock’s compliance with this Agreement.

(b) Documentation and Requests for Information. Gurock will upon request provide Customer with the following information:

i. Copies of all records of Personal Data Processing activities processed under this Agreement required to be maintained under Applicable Law;

ii. Copy of Gurock's then-most recent audit report or review conducted by Gurock's external auditors that relates to any Processing of Personal Data processed under this Agreement; and

iii. Copies of the reports resulting from any audits performed by Gurock's internal personnel that include Processing of Personal Data within their scope.

5. Indemnification

Gurock shall indemnify, defend, and hold Customer, its Affiliates, and their respective directors, officers, employees, independent contractors and agents (each an "**Indemnified Party**") harmless, to the fullest extent permitted by law, from and against all losses, judgments, liabilities, costs, expenses, fines, penalties and awards that an Indemnified Party suffers or incurs as a result of any claims, demands, suits, causes of action or enforcement proceedings (each, a "**Claim**") arising from, relating to or alleging any breach of this Agreement or violation of Applicable Law by Gurock but solely to the extent that Gurock fails to act or acts outside or against the instructions of Customer. Gurock's liability under this Agreement shall be limited to three times the amount paid by Customer to Gurock in the previous year.

6. Miscellaneous

(a) Conflicts. In the event of any conflict or inconsistency between the provisions of this DPA and the Agreement, the provisions of this DPA shall control with respect to the subject matter set forth herein. All the terms, provisions and requirements contained in the Agreement shall remain in full force and effect except to the extent they conflict with and are superseded by this Agreement.

(b) Governing Law and Jurisdiction. This Agreement shall be governed by and construed in accordance with the internal laws of the State of Texas, without giving effect to any principles of conflicts of law. The parties irrevocably agree with the exclusive jurisdiction of the courts of Travis county, Texas.

(c) Term. This DPA shall enter into force on the date of signing and shall remain in force for as long as Gurock processes Personal Data on behalf of Customer. Upon termination of the Agreement, this DPA will be terminated accordingly.

(d) Binding Effect. The terms, provisions and conditions of this Agreement shall be binding upon and inure to the benefit of each respective party and their respective legal representatives, successors and assigns.

(e) Notices; Change of Address. Any notices, consents or approvals required or permitted to be given hereunder shall be deemed to be given and sufficient (a) three (3) days after deposit in the United States mails, if sent via certified or registered letter, return receipt requested; or (b) one (1) day after deposit with a reputable overnight delivery or courier service, in each case, to the respective addresses set forth in the signature block or such other address provided by either Party in accordance with this section.

Appendix A
Details of Processing of Personal Data

Subject matter and duration

The subject matter and duration of the Processing of Personal Data are set forth in the Agreement and all amendments, exhibits, schedules, task orders, addenda, SOW's, purchase orders and other documents associated therewith and incorporated therein.

Nature and purpose

The nature and purpose of the Processing of Personal Data are set forth in the Agreement and all amendments, exhibits, schedules, task orders, addenda, SOW's, purchase orders and other documents associated therewith and incorporated therein.

Categories of Data Subjects

Data subjects may include Customer's representatives and end users, such as employees, contractors, collaborators, partners, customers and users of the Customer. Data subject may also include individuals attempting to communicate or transfer Personal Data to users of the Services. Gurock's customers have the ability to store data about any Data Subject. As such, Gurock does not have visibility of the Data Subject category the Customer will input in Gurock's system. For example, if the Gurock customer add a user named John Smith, Gurock will not know if John Smith is a Customer employee or a client of Gurock's customer. The same is true for any other category of data subject collected by the Customer.

Types of Personal Data

In order to execute the Agreement, and in particular to perform the Services, Customer authorizes and requests that Gurock process the following personal data. Personal Data may include, among other information, personal contact information such as full name, home address, mobile number, email address; details including employer name, job title and function, identification numbers and business contact details; goods or services provided; IP addresses and interest data.

Processing operations

The Personal Data transferred will be subject to the following basic processing activities: Gurock will use Customer email address to validate the login username and to send any notifications about the application the user has chosen to be notified.

Appendix B
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection

Gurock's Customer (the **data exporters**)

Gurock Software GmbH (the **data importer**)

HAVE AGREED on the following Contractual Clauses (the 'Clauses') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1 to the Clauses, such transfer arising from the processing of personal data from data exporters as permitted pursuant to the Agreement between Customer and Gurock.

Clause 1
Definitions

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

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

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

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

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

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

Clause 2
Details of the transfer

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

Clause 3
Third-party beneficiary clause

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

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

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

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

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

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

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

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in *Appendix 1* to the Clauses;

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

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

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

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

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

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

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

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorized access; and

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

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

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by

a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

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

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

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

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

Clause 6
Liability

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

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

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

Clause 7
Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

Clause 9

Governing law

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

Clause 10

Variation of the Clauses

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

Clause 11

Sub-processing

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

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

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

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

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the

confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES
DESCRIPTION OF THE TRANSFERS

Data Subjects:

The Personal Data transferred concern some or all of the following categories of Data Subjects: customer name, email address, account information.

Purposes of the Transfer(s):

The transfers are made for the following purposes: financial accounting and reporting and planning; Gurock is part of the US based Idera group. Department heads are based in the US and therefore need access to certain information to be able to work together with their European teams. In addition, the sales team of the whole group works closely together, e.g. renewals are managed in total by the United States division.

Categories of Data:

The Personal Data transferred fall within the following categories of data: Gurock customer name and email address.

Recipients:

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients, on a need to know basis: Idera, Inc., and its subsidiaries.

Sensitive Data (If Appropriate):

Not applicable.

Data Protection Registration Information of Data Exporter: The Data Exporters have registered and/or will register their data processing operations as required by law.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Technical and Organizational Security Measures
The data importer is committed to maintaining the privacy, confidentiality and security of personal data of the data exporter's personal data. The data importer uses industry best practices, technology and security measures to protect any and all personal data that is transferred to it and to secure its networks, data centers and servers. The security measures adopted by the data importer (and its subcontractors) include, without limitation:

> The maintenance of physical, electronic and procedural measures to safeguard the confidentiality of personal data in compliance with applicable data protection, privacy and data security laws and regulations. These include, without limitation, restricting access by the data importer's personnel and subcontractors on a role-based, need to know basis, background checks on data importer personnel; The implementation and enforcement of corporate policies and standards relating to the protection of information and security, which are strictly enforced. Failure to adhere to these policies and the standards will result in disciplinary action, which can include dismissal; Adopting a multi-layered approach to information security controls, which enable the data importer to protect against security breach; Compliance with applicable laws, regulations and security standards applicable to information security; The employment of highly trained staff who have relevant and up to date knowledge of data protection and data security risk management practices; and Regular reviews and controls against compliance with the above mentioned technical and organizational security measures.

1. Amazon Web Services for all data storage and processing

The data importer uses Amazon Web Services ("AWS") exclusively for the processing and storage of all data. No data leaves the AWS environment unless requested by the data exporter under their own control. All AWS security and data privacy compliance can be reviewed at https://aws.amazon.com/compliance/programs/. The use of AWS provides the data importer with an industry leading environment for the protection of its customers data.

2. Access Control

Data processing systems shall be prevented from being used without authorization. All systems are protected by the use of personally identifiable access keys that are expired on employee change of role or departure from the organization.

3. Change Control

Persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording.

4. Data Forwarding

Personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities. As the systems are located in Amazon Web Services, the data importer has no direct access to any of the physical media on which the personal data is stored. AWS compliance with physical media protection standards can be viewed at https://aws.amazon.com/compliance/programs/.

5. Order Control

Personal data processed on behalf of a data exporter are processed strictly in compliance with the data exporter's instructions. Data importer shall encrypt all personal data that it possesses, including electronic messages and attachments, strictly in compliance with the data exporter's instructions.

6. Availability control

Data must be protected against accidental destruction or loss.

7. Separation control

Data collected for different purposes can be processed separately.

8. Personnel of data importer

Any personnel of data importer entrusted with processing data exporter's personal data have undertaken to comply with the principle of confidentiality in accordance with statutory law. The undertaking to confidentiality shall continue after the termination of the above-entitled activities. Prior to providing access to personal data, the data processor shall train its personnel concerning the implementation of, compliance with and enforcement of, the data processor's security program and the handling of the personal data.

9. Adequate alternative measures

The technical and organizational security measures are subject to technical progress and development, and data importer may implement adequate alternative measures. Any material changes to technical and organizational measures must be documented. Data importer must provide data exporter with reasonable information in order to support data exporter's reporting upon written request by the data exporter. Data importer will provide to data exporter any security assessments/certifications previously performed (and if data importer has not previously performed security assessments/certifications, it shall perform and provide such assessments/certifications at data exporter's request).