Alchemy Systems, LP

Data Processing Addendum

This Data Processing Addendum (the "**DPA**") is made between [ ] [a corporation with its principal place of business at] (hereinafter referred to as "Customer") and [Alchemy Systems, LP], [an **Texas** corporation with its principal place of business at **Texas**] (hereinafter referred to as "**Data Processor**"). Customer and Data Processor (each a "**Party**" and together the "**Parties**") hereby enter into the following DPA effective as of [ ], 2021.

WHEREAS:

(A) Data Processor provides Services (as defined below) to Customer pursuant to the Parties' General Terms and Conditions ("Agreement").

(B) This DPA is entered into to provide adequate safeguards with respect to the protection of privacy and security of Personal Data passed from Customer to Data Processor for Processing or accessed by Data Processor on the authority of Customer for Processing or otherwise received by Data Processor for Processing on Customer's behalf.

(C) By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Data Processor processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

(D) This DPA further defines certain service levels to be applied to all Personal Data related Services (as defined below) provided by Data Processor to Customer.

(E) All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

IT IS AGREED THAT:

1. DEFINITIONS

1.1 In this DPA, the following expressions shall have the following meanings unless the context otherwise requires:

"Authorized Affiliate"	means Affiliates, which (a) are subject to the data protection laws and regulations of any member of the EU or European Economic Area or the UK and (b) are permitted to use the Services pursuant to the Agreement between Customer and Data Processor or on whose behalf Data Processor Processes Personal Data.
"Business"	means a legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects Data Subjects' Personal Data, or on behalf of whom such Personal Data is collected and that alone, or jointly with others, determines the purposes and means of the Processing of Data Subjects' Personal Data, as defined by the California Consumer Privacy Act ("CCPA") as amended from time to

	time, and is Customer as set forth in this Addendum;
"Business Purpose"	means the use of Personal Data for the Business's or Service Provider's operational purposes, or other notified purposes, provided that the use of Personal Data is reasonably necessary and proportionate to achieve the operational purpose for which Personal Data was collected or processed or for another operational purpose that is compatible with the context in which Personal Data was collected, as defined by the CCPA as amended from time to time;
"CCPA"	means the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 to 1798.199), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 999.300 to 999.337), and any related regulations or guidance provided by the California Attorney General, as each of these titles may be amended from time to time;
"Commercial Purpose"	means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction, as defined by the CCPA as amended from time to time;
"Data Controller"	means the entity which determines the purposes and means of the Processing of Personal Data;
"Data Processor"	means the entity which Processes Personal Data on behalf of the Data Controller;
"Data Protection Laws and Regulations"	means (a) the GDPR; and (b) United Kingdom Data Protection Act of 2018, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and (c) all laws, regulations or requirements or regulatory guidance, in any jurisdiction, relating to data protection, privacy and confidentiality of Personal Data, in each case to the extent applicable to a Party.
"Data Subject"	means an identified or identifiable natural person who is the subject of Personal Data;
"Instruction"	means the written instruction, submitted by the Data Controller to Data Processor, and directing the same to perform a specific action with regard to Personal Data (including depersonalizing, blocking, deleting, making available, etc.);
"Personal Data"	means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic,

cultural or social identity;

"Personal Data Breach"	shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
"Process"/"Processing"	means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
"Schedule"	means the schedule annexed to and forming part of this DPA;
"Services"	means Processing of the Personal Data by the Data Processor in connection with and for the purposes of the provision of the services to be provided by the Data Processor to the Data Controller relating to General Terms and Conditions including as described in Schedule 1 to this DPA; and
"Sale"/"Selling"	means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data by a Party to a third party for monetary or other valuable consideration;
"Standard Contractual Clauses"	means the agreement executed by the Data Controller as data exporter and Data Processor as data importer, attached hereto as Schedule 2; and
"Subprocessor"	means any processor engaged by the Data Processor (or by any other Subprocessor of the Data Processor) who agrees to receive from the Data Processor (or from any other Subprocessor of the Data Processor) Personal Data exclusively intended for Processing such Personal Data on behalf of the Data Controller after the transfer in accordance with its Instructions and the terms of the written subcontract.

1.2 Terms used in this DPA and not otherwise defined shall have the meaning given by Data Protection Laws and Regulations.

2. SCOPE AND APPLICATION OF THIS DPA

2.1 The scope, manner, purpose, categories of Personal Data, and the Data Subjects affected are set out in Schedule 1 to this DPA.

2.2 This DPA applies, in relation to the Services, to:

2.2.1 all Personal Data sent by or on behalf of Customer to Data Processor for Processing;

2.2.2 all Personal Data accessed by Data Processor on the authority of Customer for Processing; and

2.2.3 all Personal Data otherwise received by Data Processor for Processing on Customer's behalf.

3. DATA PROCESSING

Data Processor agrees to Process the Personal Data to which this DPA applies by reason of clause 2 in accordance with the terms and conditions set out in this DPA, and in particular Data Processor agrees:

3.1 to Process the Personal Data only on behalf of Customer and at all times in compliance with Customer's Instructions based on this DPA, and all applicable data protection laws and solely for the purposes (connected with provision of the Services by Data Processor) and in the manner specified from time to time by Customer in writing and for no other purpose or in any manner except with the express prior written consent of Customer. Instructions orally given shall be promptly confirmed in writing. If Data Processor cannot provide such compliance for whatever reasons, it agrees to promptly notify Customer of its inability to comply, in which case Customer is entitled to suspend the transfer of Data and/or terminate this DPA. Where Data Processor believes that compliance with any instructions by Customer would result in a violation of any applicable law on data protection, Data Processor shall notify Customer thereof in writing within a reasonable period of time;

3.2 that it has no reason to believe that any applicable law prevents it from fulfilling the Instructions received from Customer and its obligations under this DPA and that in the event of a change of any applicable law which is likely to have a substantial adverse effect on the obligations provided under this DPA, it will promptly notify Customer of the change as soon as it is aware of such change, in which case Customer is entitled to suspend the transfer of Personal Data and/or terminate this DPA;

3.3 that within Data Processor's area of responsibility, Data Processor will structure its internal corporate organization to comply with the specific requirements of the protection of Personal Data. Data Processor will incorporate technical and organizational measures to adequately protect Customer's Personal Data against misuse and loss. An overview of the technical and organizational measures has been attached as Schedule 2 (Description of Technical and Organizational Measures) to this DPA. Data Processor regularly monitors compliance with these measures and will not materially decrease the overall security of the Services during the Agreement;

3.4 inform each of its employees, agents and Subprocessors of its obligations under this DPA with regard to the security and protection of the Personal Data and require that they enter into binding obligations with Data Processor to maintain the levels of security and protection provided for in this DPA;

3.5 require personnel entrusted with the Processing of Customer's Personal Data to themselves to confidentiality. The obligation to maintain data secrecy shall survive the termination of the respective employment relationship;

3.6 not to divulge the Personal Data whether directly or indirectly to any person, firm or company or otherwise without the express prior written consent of Customer except to those of its employees, agents and Subprocessors who are engaged in the Processing of the Personal Data and are subject to the binding obligations referred to in clause 3.4 or 3.5 or except as may be required by any law or regulation;

3.7 promptly notify Customer about:

3.7.1 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;

3.7.2 any substantial disruption of the Services or serious interruptions of the operations, any infringements by Data Processor or its employees, of applicable data protection laws or of this DPA, or any material irregularity in relation to the Processing of the Personal Data belonging to Customer;

3.7.3 any Personal Data Breach of which it becomes aware. Such notification shall include, taking into account the nature of the Processing and the information available to Data Processor, any information relevant to assist Customer with its own notification obligations under applicable law:

3.7.4 any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorized to do so in writing by Customer;

3.8 in the event of the exercise by Data Subjects of any of their rights under applicable law in relation to the Personal Data (including rights to access, rectification, erasure, blocking, objection, restriction, data portability, and the right not to be subject to a decision based solely on automated Processing, including profiling), to inform Customer as soon as possible, and Data Processor further agrees to assist Customer with all Data Subject requests which may be received from any Data Subject in relation to any Personal Data;

3.9 taking into account the nature of the Processing, to assist Customer by appropriate technical and organisational measures, insofar this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the Data Subject's rights laid down by applicable law;

3.10 to deal promptly and properly with all inquiries from Customer relating to its Processing of the Personal Data, including making available to Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA or information necessary for Customer to apply with applicable laws;

3.11 that any Processing services carried out by a Subprocessor will be carried out in accordance with clause 6;

3.12 that Data Processor has appointed a data protection officer to the extent this is required by applicable law. Data Processor will provide the contact details of the appointed person; and

3.13 to assist Customer in ensuring compliance with applicable law, including the obligation to carry out data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of the Processing and the information available to Data Processor.

4. OBLIGATIONS OF CUSTOMER

4.1 Within and restricted to the scope of this DPA, Customer agrees that it shall ensure that any disclosure of Personal Data made by it to Data Processor is made with the Data Subject's consent or is otherwise lawful.

4.2 Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the Customer's use of Data Processor.

4.3 Customer is solely responsible for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

5. DURATION; TERMINATION; RETURN OR DELETION OF PERSONAL DATA

5.1 This DPA will become effective when the Parties' Agreement enters into effect. This DPA will automatically terminate upon the later of (a) termination or expiry of Data Processor's obligations in relation to the Services and (b) at the choice of Customer to terminate the DPA. On termination of this DPA, Data Processor shall deliver to Customer or destroy, at Customer's sole option, all Customer's Personal Data in its possession or under its control. Upon the request of Customer, Data Processor shall confirm compliance with such obligations in writing and delete all existing copies, unless applicable law requires storage of the Personal Data.

5.2 Customer shall be entitled to terminate this DPA by notice in writing to Data Processor if Customer receives notice from Data Processor in accordance with clause 3.1 or 3.2 of this DPA.

6. AUDITS AND INFORMATION REQUESTS

6.1 Data Processor has obtained the third-party certifications and audits set forth in the Technical and Organizational Measures. Upon Customer's written request at reasonable intervals, and subject to confidentiality provisions set forth in the Parties' Agreement, Data Processor (or Customer's independent, third-party auditor that is not a competitor of Data Processor) shall provide Customer with a copy of Data Processor's then most recent third-party audits or certifications, in the form of the applicable ISO 27001 certifications, SOC 1, or SOC 2 reports, or other applicable certifications or reports.

6.2 To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Laws and Regulations cannot reasonably be satisfied through audit reports set forth in Section 6.1 above, Customer may during regular business hours, without unreasonably interfering with Data Processor's business operations, and after a reasonable prior notice, personally audit Data Processor, or appoint a third-party auditor being subject to confidentiality obligations, and who is not a competitor of Data Processor, to carry out such audit up to once per year.

6.3 Before the commencement of any such on-site audit, Customer and Data Processor shall mutually agree upon the scope, timing, and duration of the audit. Data Processor shall, upon request and within a reasonable time, provide to Customer all information which is necessary to carry out an audit of the Processing. Neither Customer nor the auditor shall have access to any data from Data Processor's other customers or to Data Processor's systems or facilities not involved in the Services. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer agrees to share such audit report with Data Processor and Data Processor will promptly address any material non-compliance.

6.4 Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Data Processor expends for any such audit. Customer will reimburse Data Processor for the costs incurred with respect to responding to information requests and assisting with audits at the then current professional service rates.

6.5 The Parties further agree that the Customer's audit under this Section shall serve as the audit for its Authorized Affiliates.

7. APPOINTMENT OF SUBPROCESSORS

7.1 Customer hereby consents to and generally authorizes the engagement of Subprocessors set out in Schedule 4 to this DPA by Data Processor.

7.2 Upon request of Customer, Data Processor will make available to Customer a list of the then current Subprocessors for the Services.

7.3 Data Processor may only authorize a new Subprocessor to Process any Personal Data with Customer's prior written approval. In order to exercise its right to object to Data Processor's use of a new Subprocessor, the Customer shall notify Data Processor promptly in writing within twenty (20) calendar days after receipt of Data Processor's notice. In the event Customer objects to a new Subprocessor, and that objection is not unreasonable, Data Processor will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected to new Subprocessor without unreasonably burdening Customer. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the relevant portion(s) of the Services which cannot be provided by Data Processor without the use of the objected-to new Subprocessor by providing written notice to Data Processor. Data Processor will refund Customer any prepaid fees for the terminated portion(s) of the Services that were to be provided after the effective date of termination.

7.4 Any such Processing by a Subprocessor shall be done pursuant to a signed DPA that is no less restrictive than this DPA.

7.5 No Processing by a Subprocessor will release Data Processor from its responsibility for its obligations under this DPA, and Data Processor will be fully liable for the work and activities of each of its Subprocessors.

8. STANDARD CONTRACTUAL CLAUSES

8.1 In the course of the provision of Services by Data Processor to Customer, it will be necessary to transfer Personal Data of Customer to Data Processor located in the United States.

8.2 With regard to the data transfers referred to in clause 8.1, the Standard Contractual Clauses executed by Customer as data exporter and Data Processor as data importer apply as further set out in the following clauses 8.3 to 8.6.

8.3 Subprocessors shall be appointed pursuant to Clause 9 of the Standard Contractual Clauses as further specified in clause 7 of this DPA. Copies of the Subprocessor agreements that must be provided by Data Processor to Customer pursuant to Clause 5 (j) of the Standard Contractual Clauses may have all commercial information or other clauses unrelated to the Standard Contractual Clauses removed by Data Processor beforehand. Such copies will be provided by Data Processor only upon Data Controller's request.

8.4 The audits pursuant to Clause 8.9 of the Standard Contractual Clauses shall be carried out as further specified in clause 6 of this DPA.

8.5 The certification of the deletion of Personal Data pursuant to Clause 16 of the Standard Contractual Clauses shall be provided by Data Processor only upon Data Controller's request.

8.6 In the event of any conflict between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the provision protecting the rights and freedoms of Data Subjects to a greater extent shall prevail.

9. LIMITATION OF LIABILITY

9.1 Each Party's and all of its Authorized Affiliate's liability, taken together in the aggregate, arising out of or related to this DPA (including the SCC in Schedule 3), whether in contract, tort or under any other theory of liability, is subject to the General Terms and Conditions, and any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement.

9.2 The total liability of Data Processor for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement shall apply in the aggregate for all claims under both the Agreement and the DPA (including the SCC in Schedule 3), by Customer and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

10. California Consumer Data Protection

10.1 In addition to the provisions set forth in this DPA, with respect to the Processing of Personal Data of California residents, the Parties acknowledge and agree:

10.1.1 Customer is and shall be a Business and Data Processor shall be a Service Provider;

10.1.2 When Data Processor Processes Personal Data on behalf of Customer, Data Processor represents and warrants that it shall not:

(a) retain, use, or disclose Personal Data it collects or Processes in connection with the Services for any purpose other than for performing the Services set out in the Agreement and/or its exhibits and in accordance with the terms of this DPA, the Parties' Agreement, and Customer's instruction;

(b) retain, use, or disclose Personal Data for a Commercial Purpose other than providing the Services set out in the Agreement and/or its exhibits;

(c) sell or promote the Sale of Personal Data;

(d) combine Customer's Personal Data with Personal Data received from other entities except to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity; and

(e) disclose or transfer Personal Data to unauthorized personnel or parties, outside the direct business relationship between Customer and Data Processor.

10.1.3 Data Processor will reasonably cooperate with and assist Customer with its CCPA compliance obligations. Upon written request from Customer, Data Processor will make reasonable efforts to assist Customer with its obligation to respond to Data Subject requests to exercise rights under the CCPA in a manner that allows Customer to respond to such requests within the timeframes set under the CCPA. If a Data Subject makes a request to exercise a right under the CCPA directly with Data Processor, Data Processor will promptly notify Customer and will not

respond to Data Subject except to direct such Data Subject to contact Customer; and

10.1.4 Data Processor must notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates to either Party's compliance with the CCPA.

10.2 Customer acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA

10.3 Data Processor shall immediately notify Customer in writing if it determines or reasonably suspects its inability to comply with its obligations set forth in Section 10 above. Upon any such notice to Customer, Data Processor shall immediately cease all use of Personal Data hereunder, and Customer is entitled to suspend or terminate this DPA with cause;

10.4 Notwithstanding this Section 10, above, the Parties agree to adhere to all provisions and accompanying schedules set forth in this DPA with respect to Processing Personal Data of California residents.

10.5 Data Processor hereby certifies, and will certify throughout the term of the Agreement that Data Processor acknowledges and agrees to the provisions set forth in Section 10, above, and will comply with them and all applicable obligations under the CCPA.

11. MISCELLANEOUS PROVISIONS

11.1 Amendments or additions to this DPA must be made in writing to be effective. This shall also apply to amendments of this written form requirement. The written form requirement in this clause does not include faxes or any non-transitory form of visible reproduction of words (like emails).

11.2 Should any provision of this DPA be or become invalid, this shall not affect the validity of the remaining terms. The Parties shall in such an event be obliged to cooperate in the creation of terms which achieve such legally valid result as comes closest commercially to that of the invalid provision. The above shall apply accordingly to the closing of any gaps in the DPA.

11.3 Any Customer obligations arising from statutory provisions or according to a judicial or regulatory decision shall remain unaffected by this DPA.

11.4 This DPA shall be governed by the same law that is governing the Services Agreement, to which this DPA has been attached.

AS WITNESS the hands of the Parties the day and year first above written:

SIGNED by _____

duly authorised for and on behalf

of _____

SIGNED by _____

duly authorised for and on behalf

of _____

SCHEDULE 1

DESCRIPTION OF THE PROCESSING

Subject-Matter

The subject-matter of the Processing:

Alchemy Systems provision of the Services as defined in Section 1.1 of the Data Processing Agreement.

Duration

Data will not be kept for any longer than is necessary for achieving the purposes for which it was collected, processed or used, or as it is established in the applicable laws related to data retention periods.

The Term plus the period from the expiry of the Term until deletion of all Personal Data by Alchemy Systems in accordance with the Terms, in accordance with Section 5.1 of the Data Processing Agreement.

Extent, Type and Purpose of the Processing

The extent, type and purpose of the Processing is as follows:

Alchemy Systems will process Personal Data for the purposes of providing the Services.

Data Subjects

The Personal Data Processed concern the following categories of Data Subjects:

The Data Processor may process the Personal Data of the customers of the Data Controller's subsidiary, Customer. The Data Processor also may process the Personal Data provided by the end users of the Services, which may include the Personal Data of current employees, former employees, and end users

Categories of Data

The Personal Data Processed concern the following categories of data:

Data relating to individuals provided by Alchemy Systems via the Services, by (or at the direction of) Customer or by Customer End Users.

Contact data, Employment status, Location Data

SCHEDULE 2

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES

General Security Measures

Alchemy Systems will comply with industry standard security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, and incident response measures necessary to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer's personal information provided by Customer to Alchemy Systems), as well as with all applicable data privacy and security laws, regulations and standards.

Contact Information

security.office@alchemysystems.com

Compliance

Alchemy Systems policies, procedures, and standards are based on the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 and follows the NIST SP 800-30 Risk Management Framework to identify cybersecurity threats.

Information Security Program

We are committed to information security and privacy. The objective of our Information Security Program is to maintain the confidentiality, integrity and availability of its computer and data communication systems. We have the appropriate technical and organizational measures designed to protect our customer data against unauthorized access, modification or deletion.

- Personnel Security
    - Alchemy Systems employee competence is a key element of the control environment. Alchemy Systems is committed to training and developing its employees.
    - Alchemy Systems ensures that personnel have the knowledge and training needed to perform their duties. New employees go through initial Security training during the New Hire Process.
    - Alchemy Systems personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.
    - Alchemy Systems conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
    - Alchemy Systems Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Alchemy Systems confidentiality and privacy policies. Personnel are provided with security training yearly. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (eg., certifications). Alchemy Systems personnel will not process Customer Data without authorization.

- Data Classification & Protection
    - Alchemy Systems maintains policies and procedures for data classification and protection, along with requirements for classification of data containing personally identifiable information (PII) in consideration of applicable laws, regulations and contractual obligations. Alchemy Systems shall also maintain requirements on data encryption, rules for transmission of data and requirements for removable media, along with requirements on how access to these data should be governed.
- Network Security
    - Alchemy Systems maintains policies and procedures on the network infrastructure used to process Customer data, establish and enforce safe network practices, and define service level agreements with internal and external network services.
- Physical and Environmental Security
    - Alchemy Systems maintains policies and procedures for physical and environmental security, define requirements to protect areas that contain sensitive information and ensure that critical information services be protected from interception, interference or damage.
    - The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.
- Business Continuity and Disaster Recovery
    - Alchemy Systems has developed and maintains a process to address its business continuity plan throughout the organization. This plan addresses the information security requirements needed for the company's continuity in a disaster scenario. It plans for the maintenance and/or restoration of operations to ensure availability of information and continuity of critical business processes.
- Secure Software Development
    - Alchemy Systems maintains policies and procedures to ensure that system, device, application and infrastructure development is performed in a secure manner. This includes review and test of all Alchemy Systems applications, products and services for common security vulnerabilities and defects, employing defense-in-depth strategy through the use of multiple layers of security boundaries and technologies, periodic penetration testing and security assessment of these services, defining baseline configurations and requirements for patching of third party systems.

Access Control

Alchemy Systems shall maintain access control measures designed to limit access to Alchemy Systems facilities, and systems to a limited number of personnel who have a business need for such access. Alchemy Systems shall ensure such access is removed when no longer required and shall conduct access reviews periodically.

- Preventing Unauthorized Access
    - We maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.
    - We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.
    - Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the

appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

- Preventing Unauthorized Use
    - We implement industry standard access controls and detection capabilities for the internal networks that support its products.
    - Network access control devices are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.
    - Security reviews of code stored in our source code repositories is performed, checking for coding best practices and identifiable software flaws through static code analysis and vulnerability assessment.
    - We maintain relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Transmission Encryption

Alchemy Systems makes HTTPS encryption (also referred to as SSL or TLS connection) available. To reinforce our objective to secure data, the company's Secure File Transfer and Physical Media Handling Standards define mandatory security measures for when full encryption of removable media is required. Alchemy Systems will encrypt all sensitive information in transit across public networks depending on Customer's ability to support encryption. Highly sensitive data is also encrypted at rest, including passwords as applicable.

Risk Assessments

Alchemy Systems has a documented cybersecurity risk management program that follows the NIST SP 800-30 Risk Management Framework to identify cybersecurity threats, assign a rating to the associated risks, and monitor each threat and risk profile. Alchemy Systems conducts risk assessments on its products and infrastructure frequently, including data classification reviews and highly sensitive data flows. Alchemy Systems performs on a regular basis application and infrastructure level testing as well as periodic reassessments of its network. Alchemy Systems forces access control, peer code review, static code analysis, vulnerability assessment, manual penetration testing and automated tools.

Third-Party Risk Assessments

Alchemy Systems performs security due diligence on third-party service providers to assess and monitor risk. This assessment includes a review of scope of confidential information and personal data transferred to or processed by the service provider and the purpose of the work. Alchemy Systems will also conduct a risk assessment which may include the service provider's organization and technical security measures, the sensitivity of any information processed by the service provider, storage limitations, and data deletion procedures and timelines.

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES PURSUANT TO REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

between

Customer

and

Alchemy Systems, LP

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) for the transfer of personal data to a third country.

The Parties:

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

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").

These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(b) 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:

Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

Clause 8.1(b), 8.9(a), (c), (d) and (e);

Clause 9(a), (c), (d) and (e);

Clause 12(a), (d) and (f);

Clause 13;

Clause 15.1(c), (d) and (e);

Clause 16(e);

Clause 18(a) and (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.

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 (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

(a) PRIOR AUTHORISATION FOR CURRENT USE OF SUB-PROCESSORS. The list of sub-processors used by data importer to carry out any of its processing activities performed on behalf of the data exporter under these Clauses and who are already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s). The data importer shall specifically inform the data exporter in writing of any intended new sub-processor at least 20 calendar days in advance, thereby giving the data exporter sufficient time to be able to object to such changesprior 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. 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

(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. The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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

(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

(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

(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;

(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

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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

(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 Germany.

(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.

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 achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name:

   Address:

   Contact person's name, position and contact details:

   Contact person:

   Data Protection Officer:

   Activities relevant to the data transferred under these Clauses: *Transfer of data for the purposes of performing the services.*

   Signature and date:

   Role: Controller

Data importer(s):

1. Name: Alchemy Systems, LP

   Address: 5301 Riata Park Ct, Building F Austin, TX 78727

   Contact person: Aaron Rapoport

   Data Protection Officer: Philip Edge

   Activities relevant to the data transferred under these Clauses: *Transfer of data for the purposes of performing the services.*

   Signature and date:

   Role: Processor

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The Data Processor may process the Personal Data of the customers of the Data Controller's subsidiary, Customer. The Data Processor also may process the Personal Data provided by the end users of the Services, which may include the Personal Data of current employees, former employees, and end users.

Categories of personal data transferred

Contact data, Employment status, Location Data

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.

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.

See Schedule 2 Above

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

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

Continuous while the services agreement is in affect

Nature of the processing

Alchemy and/or its Sub-processors are providing Services or fulfilling contractual obligations to Customer as described in the Agreement. These Services may include the processing of Personal Data by Alchemy and/or its Sub-processors on systems that may contain Personal Data.

Purpose(s) of the data transfer and further processing

Alchemy Systems will process Personal Data for the purposes of providing the Services.

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

See GTCs

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

See Annex III Below

B.COMPETENT SUPERVISORY AUTHORITY

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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.

See Schedule 2 Above

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

ANNEX III – LIST OF SUB-PROCESSORS

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:

Entity Name	Subprocessing Activities	Description	Entity Country
Rackspace	Private Cloud Data Center	Primary and Secondary Data Centers	United States
Amazon Web Services, Inc.	Private Cloud Service Provider	Cloud Compute, Services and Storage	United States
Google, Inc.	Cloud Service Provider	Website Analytics	United States
Snowflake, Inc.	Cloud Service Provider	Data Warehouse	United States
Pendo.io, Inc.	Cloud Service Provider	Product Experience	United States
ETL Works	Cloud Service Provider	Data Transformation for Data Warehouse	United States