Data Processing Agreement

between

THE CLIENT

(as “Data Controller”)

AND

ALCHEMY SYSTEMS, LP

(as “Data Processor”)

TABLE OF CONTENTS

1. DEFINITIONS 1
2. SCOPE AND APPLICATION OF THIS AGREEMENT 3
3. DATA PROCESSING 3
4. OBLIGATIONS OF THE DATA CONTROLLER 5
5. TERMINATION 6
6. APPOINTMENT OF SUBPROCESSORS 6
7. STANDARD CONTRACTUAL CLAUSES 6
8. MISCELLANEOUS PROVISIONS 7

BETWEEN:

(1) **THE CLIENT** (the "**Data Controller**"); and

(2) **Alchemy Systems, LP** (the "**Data Processor**"),

(each a "**Party**", and together the "**Parties**").

WHEREAS:

(A) The Data Processor is to provide Services to the Data Controller pursuant to this Agreement.

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

(C) This Agreement further defines certain service levels to be applied to all Personal Data related Services (as defined below) provided by the Data Processor to the Data Controller.

IT IS AGREED THAT:

1. DEFINITIONS

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

"Data Protection Laws"	shall mean worldwide data protection and privacy laws and regulations applicable to the personal data in question, it shall include, but not limited to: a) the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations; b) Regulation (EU) 2016/679 (EU GDPR); or c) the Data Protection Act 2018 (DPA);
"Data Controller"	shall have the meanings given in applicable Data Protection Laws;
"Data Processor"	shall have the meanings given in applicable Data Protection Laws;
"Data Subject"	have the meanings given in applicable Data Protection Laws;
"Instruction"	shall mean the written instruction, submitted by the Data Controller to the 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”	shall mean any information relating to an identified or identifiable natural person and shall include, without limitation, any and all “personal information” as that term is defined in applicable Data Protection Laws; 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”	shall mean 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 Agreement;
“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 the Master Services Agreement between Alchemy Systems and CLIENT, including as described in Schedule 1 to this Agreement;
“Standard Contractual Clauses”	means (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on 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 ("EU SCCs") as incorporated into this Agreement in Annex D; and (ii) where the DPA applies, the Standard Contractual Clauses as modified by the "International Data Transfer Addendum" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("UK

	Addendum") as incorporated into this Agreement in Annex E ;
"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;
"Term"	means the Term of SOW as defined in the Statement of Work pursuant to the Master Services Agreement between Alchemy Systems and CLIENT.

2. SCOPE AND APPLICATION OF THIS AGREEMENT

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

2.2 This Agreement shall apply, in relation to the Services, to:

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

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

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

3. DATA PROCESSING

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

3.1 to Process the Personal Data only on behalf of the Data Controller and at all times in compliance with the Data Controller's Instructions based on this Agreement, and all applicable Data Protection Laws , and solely for the purposes (connected with provision of the Services by the Data Processor) and in the manner specified from time to time by the Data Controller in writing and for no other purpose or in any manner except with the express prior written consent of the Data Controller. Data Processor shall not Process Personal Data for its own "commercial purposes," as that term may be defined in the applicable Data Protection Laws. Instructions orally given shall be promptly confirmed in writing. If the Data Processor cannot provide such compliance for whatever reasons, it agrees to promptly notify the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer of Data and/or terminate this Agreement. Where the Data Processor believes that compliance with any instructions by the Data Controller would result in a violation of any

applicable law on data protection, the Data Processor shall notify the Data Controller 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 the Data Controller and its obligations under this Agreement 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 Agreement, it will promptly notify the Data Controller of the change as soon as it is aware of such change, in which case the Data Controller is entitled to suspend the transfer of Personal Data and/or terminate this Agreement;

3.3 that within the Data Processor's area of responsibility, the Data Processor shall structure its internal corporate organization to ensure compliance with the specific requirements of the protection of Personal Data. The Data Processor shall take the technical and organizational measures to adequately protect the Data Controller'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 Agreement. The Data Processor regularly monitors compliance with these measures;

3.4 to ensure that each of its employees, agents and Subprocessors are made aware of its obligations under this Agreement with regard to the security and protection of the Personal Data and shall require that they enter into binding obligations with the Data Processor in order to maintain the levels of security and protection provided for in this Agreement;

3.5 to ensure that any personnel entrusted with the Processing of the Data Controller's Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of 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, including without limitation in a manner that would constitute a "sale" of Personal Data under the appliable Data Protection Laws, without the express prior written consent of the Data Controller 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 that it will promptly notify the Data Controller 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 the Data Processor or its employees, of applicable data protection laws or of this Agreement, or any material

irregularity in relation to the Processing of the Personal Data belonging to the Data Controller;

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 the Data Processor, any information relevant to assist the Data Controller 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 the Data Controller;

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 the Data Controller as soon as possible, and the Data Processor further agrees to assist the Data Controller 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 the Data Controller by appropriate technical and organisational measures, insofar this is possible, for the fulfilment of the Data Controller'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 the Data Controller relating to its Processing of the Personal Data, including making available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement or information necessary for the Data Controller 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 the Data Processor has appointed a data protection officer to the extent this is required by applicable law. The Data Processor will provide the contact details of the appointed person; and

3.13 to assist the Data Controller 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 the Data Processor.

4. OBLIGATIONS OF THE DATA CONTROLLER

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

5. TERMINATION

5.1 This Agreement shall terminate automatically upon the later of (a) termination or expiry of the Data Processor's obligations in relation to the Services and (b) at the choice of the Data Controller to terminate the Agreement. On termination of this Agreement, the Data Processor shall forthwith deliver to the Data Controller or destroy, at the Data Controller's sole option, all the Data Controller's Personal Data in its possession or under its control. Upon the request of the Data Controller, the 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 The Data Controller shall be entitled to terminate this Agreement forthwith by notice in writing to the Data Processor if the Data Controller receives notice from the Data Processor in accordance with clause 3.1 or 3.2 of this Agreement.

6. APPOINTMENT OF SUBPROCESSORS

6.1 The Data Processor may only authorize a Subprocessor to Process any Personal Data with Data Controller's prior written approval. In the case of a general written authorization, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other Subprocessors, thereby giving the Data Controller the opportunity to object to such changes.

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

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

7. STANDARD CONTRACTUAL CLAUSES

7.1 In the course of the provision of Services by the Data Processor to the Data Controller, it may be necessary to transfer Personal Data of the Data Controller to the Data Processor located outside of the Data Subject's location.

7.2 With regard to the data transfers referred to in clause **Error! Reference source not found.**, the Standard Contractual Clauses executed by the Data Controller as data exporter and the Data Processor as data importer as set out in Schedule 3.

7.3 Subprocessors shall be appointed pursuant to Clause 5(h) of the Standard Contractual Clauses as further specified in clause *6* of this Agreement.

7.4 In the event of any conflict between the body of this Agreement 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.

7.5 In the event Data Processor transfers its assets to a third party as part of a merger, acquisition, bankruptcy, or other transaction in which a third party assumes control of all or part of Data Processor's assets, Data Processor shall provide Data Controller with

prior written notice and any such Personal Data shall be excluded from Data Processor's assets for the purpose of the merger, acquisition, bankruptcy, or other transaction.

8. MISCELLANEOUS PROVISIONS

8.1 Amendments or additions to this Agreement 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).

8.2 Should any provision of this Agreement 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 Agreement.

8.3 Any Data Controller obligations arising from statutory provisions or according to a judicial or regulatory decision shall remain unaffected by this Agreement.

8.4 This Agreement shall be subject to all the general terms and conditions found in the service agreement between Alchemy and Client

AS WITNESS the hands of the Parties:

SIGNED by

_____

duly authorised for and on behalf
of

SIGNED by

_____

duly authorised for and on behalf
of Alchemy Systems

SCHEDULE 1

DESCRIPTION OF THE PROCESSING

Subject-Matter

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

Duration of the Processing

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.

This is 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

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

Data Subjects

The Data Processor may process the Personal Data of the customers of the Data Controller's subsidiary, CLIENT. 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

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

As the Data Processor, the following types of data are provided by the Data Controller:

- First name, last name, worksite, location, user ID, employee ID, and date of hire and termination

The Data Controller will inform the Data Processor in writing in advance if any additional Personal Data is provided.

SCHEDULE 2

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES

As from the Terms Effective Date, Alchemy Systems will implement and maintain the Technical and Organizational Measures set out in this Schedule 2. Alchemy Systems may update or modify such Technical and Organizational Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Subprocessor Security

Before onboarding Subprocessors, Alchemy Systems conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Alchemy Systems has assessed the risks presented by the Subprocessor, then subject to the requirements of the Data Controller's Requirements for Subprocessor Engagement, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms, in accordance with Section 6 of the Data Processing Agreement.

UK Internation Data Transfer Addendum

1.1 Mandatory Clauses

1.1.1 Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses;

1.2.3 Part three: Commercial Clauses; and

1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section **Error! Reference source not found.**.

2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.

3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

4.1 The Parties may choose to each sign (or execute):

4.1.1 the same copy of this IDTA;

4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so

that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

1.1.2 How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

8.2 The Exporter must:

8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

1.1.3 The Exporter

11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at

any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

1.1.4 The Importer

12. General Importer obligations

12.1 The Importer must:

12.1.1 only Process the Transferred Data for the Purpose;

12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or

delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.2.1.1 a description of the nature of the Importer Personal Data Breach;

15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.2.1.3 likely consequences of the Importer Personal Data Breach;

15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.2.1.5 contact point for more information; and

15.2.1.6 any other information reasonably requested by the Exporter,

15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.3.1 a description of the nature of the Importer Personal Data Breach;

15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.3.3 likely consequences of the Importer Personal Data Breach;

15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.3.5 contact point for more information; and

15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those

Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request. This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

- 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or
- 16.1.2 the third party has been added to this IDTA as a Party; or
- 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
- 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
- 16.1.5 the transfer is to the UK or an Adequate Country.

16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer's responsibility if it authorises others to perform its obligations

17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).

17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

1.1.5 What rights do individuals have?

18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

- 18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;
- 18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;
- 18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and

20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or

20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant

protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor

21.1 Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section** Error! Reference source not found. (Legal Glossary).

32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a

Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The parties may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

For all parts to Appendix 1, see description contained in Schedule 1 of the Data Processing Agreement.

Data Controller

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

- Client is the Data Controller who is receiving Services under the Terms of Service.

Data Processor

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

- Alchemy Systems is a provider of enterprise cloud computing solutions which processes personal data upon the instruction of the controller in accordance with the terms of the Agreement.

Data subjects

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

- Prospective and existing customers of the controller

Categories of data

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

- Data relating to individuals provided to Alchemy Systems via the Services, by (or at the direction of) Client or by Client End Users.
    - First name, last name, worksite, location, user ID, employee ID, and date of hire and termination
- Customer will inform Alchemy Systems in writing in advance if any additional Personal Data is provided.

Special categories of data (if appropriate)

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

- None

Processing operations

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

- Personal data is used for filtering training content and operational tasks as well as reporting around those elements.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organisational security measures implemented by the data processor in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See description contained in Schedule 2 of the Data Processing Agreement.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

Alchemy Systems may use the following Subprocessors to host Customer Data or provide other infrastructure that helps with delivery of our Services:

Entity Name	**Subprocessing Activities**	**Entity Country**
Amazon Web Services, Inc.	Cloud Service Provider (Data Centers, Cloud Compute, Services and Storage)	United States
Google, Inc.	Website Analytics	United States
Netsuite	Business software suite	United States
HubSpot	Inbound Marketing, Sales, and Service Software	United States
Snowflake, Inc	Data Warehouse	United States
Pendo.io, Inc.	Product Experience Analytics	United States
ETL Works / Amazon Kinesis Data Firehose	Data transformation for Data Warehouse	United States
Power BI	Data Analytics	United States