Data Processing Agreement

This Data Processing Agreement, (the "***DPA***") is made by and between **SaaS Consulting Group, LLC**, a Texas limited liability company, having a principal place of business at 3345 Bee Caves Road, Suite 206, West Lake Hills, Texas 78747 USA ("**Data Processor**") and the Customer, as defined in the Master Services Agreement and/or Subscription Services Agreement ("**Data Controller**"), (each a "**Party**", and collectively the "**Parties**"). This DPA is effective and shall remain in force for the term of the Master Services Agreement and/or Subscription Services Agreement.

1. **Purpose of the DPA.** The Parties have executed an agreement for the provision, performance and/or delivery of services by the Data Processor to the Data Controller whereby the Data Processor may process Personal Data, as defined in Section 2 (c) of this DPA, obtained by and on behalf of the Data Controller, which may be a Master Services Agreement, a Subscription Services Agreement, and/or a Statement of Work (individually or collectively, the "**Agreement**").

2. **Definitions.** The following defined terms are used in this DPA, together with other terms defined herein.

    a) "**Data Protection Laws and Regulations**" means the following data protection laws: (i) EU Regulation 2016/679 ("GDPR"), where the Controller is established in a European Economic Area ("EEA") member state or is otherwise subject to GDPR; (ii) the UK Data Protection Act 2018 and any data protection laws substantially amending, replacing or superseding the GDPR following the United Kingdom's exit from the European Union, and (iii) any and all other applicable data privacy laws including, without limitation, the California Consumer Privacy Act of 2018.

    b) "**Data Subject**" means the individual to whom Personal Data relates.

    c) "**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, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

    d) "**Processing (or Process)**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure or destruction.

    e) **"Service" or "Services"** means the services requested by the Customer and Data Controller to be performed or delivered by Data Processor, having the same meaning as in the Master Services Agreement – services pertaining to or related to the implementation, configuration, customization, optimization, integrations and/or ongoing support of Salesforce and/or NetSuite business applications, as more fully described in one or more Statements of Work.

3. **Processing of Data.**

    a) Data Controller's Processing of Personal Data. Data Controller will Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Data Controller's instructions for the Processing of Personal Data will comply with Data Protection Laws and Regulations. Data Controller is solely responsible for the accuracy, quality, and legality of Personal Data and the means by which Data Controller acquired Personal Data.

    b) Data Processor's Processing of Personal Data. Data Processor will only Process Personal Data on behalf of and in accordance with Data Controller's instructions and in relation to the Agreement and its purpose

(the "Purpose"), and will treat Personal Data as Confidential Information. By entering into this DPA, Data Controller instructs Data Processor to Process Personal Data in accordance with the Purpose. Data Controller may issue additional instructions to Data Processor, and Data Processor shall promptly comply with all such additional instructions, as long as such instructions (i) comply with applicable Data Protection Laws and Regulations, (ii) are issued by Data Controller to Data Processor in writing and with sufficient advance notice for Data Processor to review, consider and act on such instructions, do not provide Data Processor with additional sensitive or special Personal Data that imposes additional data security or data protection obligations on Data Processor beyond those which are already contemplated in the Agreement (iii) and (iv) Data Processor has the means and authority to so act. To the extent that Data Processor expects to incur additional charges or fees not contemplated or covered by the Agreement and with respect to any additional instructions, the Parties shall, without prejudice, negotiate in good faith as to which Party or Parties bear the cost of the additional instructions.

c) <u>Subprocessing of Personal Data</u>. Data Controller permits Data Processor to use subprocessors to Process Personal Data; provided, that Data Processor enters into an agreement with each subprocessor that contains terms no less restrictive than this DPA and that complies with the Data Protection Laws and Regulations. Data Processor will provide Data Controller with sixty (60) calendar days advance notice prior to using a new subprocessor to Process Personal Data for the Purpose. Data Controller may terminate this DPA if the new subprocessor is unacceptable to Data Controller.

4. **Rights of Data Subjects.**

a) <u>Correction, Blocking and Deletion</u>. To the extent Data Controller does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws and Regulations, Data Processor will comply with any commercially reasonable written request by Data Controller to facilitate such actions to the extent Data Processor is legally permitted to do so. Data Controller is responsible for any costs arising from Data Processor's assistance.

b) <u>Data Subject Requests</u>. Data Processor will, to the extent legally permitted, promptly notify Data Controller if it receives a request from a Data Subject for access to, correction, amendment or deletion of that person's Personal Data. Data Processor will not respond to any such Data Subject request without Data Controller's prior written consent except to confirm that the request relates to Data Controller. Data Processor will provide Data Controller with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Data Controller does not have access to such Personal Data. Data Controller is responsible for any costs arising from Data Processor's assistance.

5. **Data Processor Personnel.**

a) <u>Confidentiality</u>. Data Processor will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Data Processor will ensure that such confidentiality obligations survive the termination of the personnel engagement.

b) <u>Reliability</u>. Data Processor will take commercially reasonable steps to ensure the reliability of any Data Processor personnel engaged in the Processing of Personal Data.

c) <u>Limitation of Access</u>. Data Processor will ensure that access to Personal Data is limited to those personnel performing services or related oversight of such services in accordance with the Agreement.

d) <u>Data Protection Officer</u>. Data Processor has appointed a corporate officer to oversee and otherwise manage its data protection responsibilities and obligations. The appointed person may be reached at legal@saascg.com.

6. **Security.** Data Processor maintains adequate administrative, physical, and technical safeguards for protection of the security (including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage), confidentiality, and integrity of Personal Data.

7. **Security Breach Management and Notification.** Data Processor maintains security incident management policies and procedures, and will, to the extent permitted by law, promptly notify Data Controller of any actual or reasonably suspected unauthorized disclosure of Personal Data, of which Data Processor becomes aware (a "**Security Breach**"). To the extent such Security Breach is caused by a violation of the requirements of this DPA, Data Processor will make reasonable efforts to identify and remediate the cause of such Security Breach.

8. **International Data Exports.** Where Controller has expressly agreed that Processor and/or its approved Sub-processors may process Personal Data outside of the EEA, the United Kingdom, and/or Switzerland as is necessary to provide support-related or other services requested by Controller, the following terms shall apply:

    (a) In the event Personal Data is transferred to the Data Processor outside the EEA and/or Switzerland such transfers shall be subject to the Standard Contractual Clauses set forth in <u>Appendix 1</u> and as revised below, or any future data transfer mechanism as approved by the European Commission and agreed to by Controller to provide adequate levels of protection determined according to Applicable Data Protection Laws:

        i. Where expressly approved by Controller in writing and in advance of such appointment, Sub-processors shall be appointed pursuant to Clause 5 (h) of the Standard Contractual Clauses as further specified in the Parties' Amendment.

        ii. The audits pursuant to Clause 5 (f) and Clause 12 (2) of the Standard Contractual Clauses shall be carried out as further specified in the Amendment.

    (b) In the event of any conflict between this Exhibit and the Standard Contractual Clauses, the provision protecting the rights and freedoms of Data Subjects to a greater extent shall prevail.

    (c) Processor shall assess whether the domestic laws in any jurisdiction in which Processing is performed by Processor outside the EEA, Switzerland or the United Kingdom offer an adequate level of protection essentially equivalent to that ensured within the European Union ("Required Level of Protection" and "Assessment" respectively). Processor shall cooperate with Controller and provide any data reasonably necessary for Processor and Controller to identify the Required Level of Protection resulting from the Assessment.

    (d) If (a) Controller reasonably believes in good faith and in accordance with Data Protection Law that the Required Level of Protection is not being met, or (b) a court of competent jurisdiction should determine that the Required Level of Protection is not being met, Controller and Processor shall identify and mutually agree on supplementary measures, including but not limited to additional technical-organizational safeguards, enforceable data subjects rights and effective legal remedies, including use of end-to-end encryption to provide the Required Level of Protection including with respect to any Onward Transfers.

    (e) Processor shall comply with such supplementary measures mutually agreed and the Amendment shall be deemed amended accordingly.

    (f) If (a) Controller reasonably determines in good faith and in accordance on Data Protection Law (b) or a regulatory organization or court of competent jurisdiction should determine that the supplementary measures offered by Processor do not provide the Required Level of Protection and Processor is unable to provide supplementary measures consistent with the Required Level of Protection:

    (y) Controller may suspend the transfer of Personal Data and Processor shall cease all processing of Personal Data; and/or

    (z) Controller may by notice terminate the Agreement and all Services without penalty or further payment, except for payment due for Services rendered prior to the effective date of termination.

    (g) For the avoidance of doubt, this Section 7.1 shall apply to any processing of Personal Data by a Subprocessor.

9. **Audits.**

    a) <u>Data Processor</u>. Data Processor allows for, cooperates with, and contributes to audits, including inspections, conducted by Data Controller or an external auditor engaged by Data Controller. Audits may be conducted: (i) from time to time on reasonable notice, but no more frequently than once per

calendar year; (ii) during normal business hours and so as not to unreasonably interfere with Data Processor's performance of the services or unreasonably interfere with Data Processor's business; and (iii) during the term of this DPA. The notice requirement in clause 9(a)(i) and the restrictions stated in 9(a)(ii) shall not apply to the extent the audit is initiated by a regulator. Data Processor shall provide to Data Controller and its auditors and regulators reasonable assistance as they require for the purpose of performing an audit, including access to the following: the place, premises and facilities from which the services will be performed; the systems (including software, networks, firewalls and servers) used to perform the service; and data, records, manuals and other information relating to the services. Each Party shall bear its own costs in relation to the audit. If an audit results in Data Processor being notified that it, or its Processing of Personal Data, is not in compliance with Data Protection Laws and Regulations, the Parties shall discuss such finding and, with respect to any such non-compliance, Data Processor shall promptly take all corrective actions necessary to achieve compliance to the satisfaction of Data Controller. Where any audit report prepared by Data Processor's internal or external auditors contains information relating to the Personal Data, Data Processor shall promptly disclose such information to Data Controller.

b) <u>Subprocessor.</u> Data Processor will facilitate, cooperate, and assist with Data Controller's audit of any subprocessor. If an audit results in Data Processor being notified that the subprocessor, or its Processing of Personal Data, is not in compliance with Data Protection Laws and Regulations, the Parties shall discuss such finding and, with respect to any such non-compliance, Data Processor shall promptly take all corrective actions necessary to achieve compliance to the satisfaction of Data Controller including, but not limited to, replacing the subprocessor with a new subprocessor acceptable to Data Controller. If Data Processor breaches its obligations under this Section, Data Controller may terminate the Agreement.

10. Updates. This DPA may be amended from time to time as necessary by the Data Processor. Data Processor shall maintain version documentation for each DPA, and shall provide at least thirty (30) days written notice to Customers of any updates to the DPA.

11. **Miscellaneous**. This DPA constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior understandings regarding such subject matter, whether written or oral. To the extent a conflict exists between this DPA and the Agreement regarding the subject matter of this DPA, the terms of this DPA will govern. This DPA will be binding upon and inure to the benefit of the Parties, their successors and permitted assigns. Data Controller may assign this DPA to an affiliate or in connection with a merger of Data Controller or the sale of substantially all of Data Controller's assets. If this DPA is translated into languages other than English, the English version will control. If for any reason, a court of competent jurisdiction or duly appointed arbitrator finds any provision or portion of this DPA to be unenforceable, the remainder of this DPA will continue in full force and effect. No amendment or modification of this DPA will be binding unless in writing and signed by Data Controller. Any waiver by a Party of a breach of any provision of this DPA will not operate as or be construed as a waiver of any further or subsequent breach. Provisions of this DPA that by their nature are to be performed or enforced following any termination of this DPA shall survive such termination.

12. **Authority of Signatories**. Each person signing the Agreement represents and warrants that he or she is duly authorized and has legal capacity to execute this DPA.

Appendix 1
Standard Contractual Clauses
Controller-to-Processor Transfers

<u>SECTION I</u>

Clause 1
Purpose and scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b)   The Parties:

    (i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

    (ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

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

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

(d)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

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

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

Clause 3
Third-party beneficiaries

(a)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

    (i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

---

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

(ii)   Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii)   Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv)   Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v)   Clause 13;

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

(vii)   Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b)   Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a)   Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b)   These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)   These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7 - Optional
Docking clause

(a)   An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b)   Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)   The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

MODULE TWO: Transfer controller to processor

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

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

8.3   Transparency
On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

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

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

8.6   Security of processing
(a)   The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional

information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7   Sensitive data

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

8.8   Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (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

---

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

(a)   The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)   The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)   The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)   The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)   The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

MODULE TWO: Transfer controller to processor

(a)   OPTION 1: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*THIRTY DAYS (30)*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)   Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)   The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d)   The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e)   The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

MODULE TWO: Transfer controller to processor

(a)   The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

---

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

(b)   The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)   In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

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

MODULE TWO: Transfer controller to processor

(b)   In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)   Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  (i)   lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  (ii)   refer the dispute to the competent courts within the meaning of Clause 18.

(d)   The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)   The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)   The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

MODULE TWO: Transfer controller to processor

(a)   Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)   The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

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

(d)   The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)   Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)   The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

MODULE TWO: Transfer controller to processor

(a)   [Where the data exporter is established in an EU Member State:] 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.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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.

Clause 14
Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(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[4];

   (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

---

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

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.

<div align="center">

Clause 15
Obligations of the data importer in case of access by public authorities

</div>

MODULE TWO: Transfer controller to processor

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.

<div align="center">

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

</div>

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

    (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

    (ii)   the data importer is in substantial or persistent breach of these Clauses; or

    (iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17
Governing law

MODULE TWO: Transfer controller to processor

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 **IRELAND**.

Clause 18
Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)   The Parties agree that those shall be the courts of **IRELAND**.

(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

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter:
The Data Controller, as defined at the beginning of the Agreement, having the same contact information as provided in the Master Services Agreement.

Data importer:
The Data Processor, as defined at the beginning of the Agreement, having the same contact information as provided in the Master Services Agreement.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred (or may be transferred), according to Data Controller instructions and the nature of Services performed or delivered:
Natural persons who are the Customer's:
- *Employees*
- *Directors or Officers*
- *Shareholders*
- *Suppliers, Vendors or Contractors*
- *Leads, Prospects or Customers*
- *End Users (software, website, etc.)*

………………………..

Categories of personal data transferred*: The Data Controller determines the categories of personal data that may be included in business applications that are in scope for the Services performed or delivered by the Data Processor.*

………………………..

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.
The Data Controller is solely responsible for disclosing to Data Processor any existence of Sensitive Data as part of the Services performed or delivered by Data Processor to Customer. For the sake of clarity, such sensitive data, is Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

………………………..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
As needed for completion of the Services during the duration of the Services agreement(s).

………………………….

Nature of the processing*: Access, visibility, data migration consultation, data transformation consultation, and data validation consultation.*

………………………….

Purpose(s) of the data transfer and further processing*: For Data Processor to perform or deliver 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: *Duration necessary to perform or complete the Services.*

……………………..

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: *Same as above.*

…………………..

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13:
For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; (ii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established; or (iii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).

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

MODULE TWO: Transfer controller to processor

The Data Processor shall, at all times, deploy and maintain appropriate control measures designed to (1) prevent and/or detect data privacy or information security breaches or violations with potential to compromise a Customer's Personal Data by any of its employees, contractors, or agents performing or delivering the Services to Customer, either directly or indirectly, or with/without intent, (2) prevent and/or detect data privacy or information security breaches or violations with potential to compromise a Customer's Personal Data from external 3rd party threats gaining access via a computer or similar device used by its employees, contractors, or agents performing or delivering the Services to Customer. Included among these are the following as it relates to all employees, contractors, or agents performing or delivery Services to Customer:

- Criminal background checks as condition of employment or contract agreement
- Confidentiality clauses and agreements as condition of employment or contract agreement
- Ongoing monthly information security and cybersecurity threat awareness training (employees only)
- Access to Personal Data is controlled and provisioned by the Customer, and Data Processor will only share such access on a need-to-know basis and only as it relates to the performance or delivery of the Services, including oversight and management
- Sign-on credentials to systems and applications containing Personal Data shall be stored/shared via encrypted and secure password vaults with complex passwords
- Acknowledgement and adherence to the Data Processor's Acceptable Use Policy, which includes hard drive encryption enabled on all computer devices
- All computer devices must contain threat detection sensors deployed on each monitored endpoint to gather system events and to execute proactive detection and prevention actions as a part of the Company's subscription to the Crowdstrike Falcon Platform – a software-as-a-service threat detection and response solution that combines anti-virus capabilities with Cloud-based analysis and threat detection (the "EDR Software"). The EDR Software may detect and report vulnerabilities, which are further investigated to determine whether they represent and Incident or some other action or response
- For sharing of files that may include Personal Data, Data Processor requires Customer to share/store those in a secured Cloud environment whereby the Customer solely controls access, and Data Processor access is to be removed upon performance or delivery of the Services.

In addition, Management of the Data Processor has established incident response policies and procedures, and regularly evaluates its overall information and cyber security posture for continuous improvement and/or enhancement opportunities.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The controller has authorised the use of the following sub-processors:
None.

Appendix 2

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Controller-to-Processor Transfers

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

1.1. Part 1: Tables

1.1.1.   Table 1: Parties

Start date	As set forth in the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	As set forth in the Agreement	As set forth in the Agreement
Key Contact	As set forth in the Agreement	As set forth in the Agreement
Signature (if required for the purposes of Section 2)	N/A	N/A

1.1.2.   Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	As set forth in Appendix 1 to the DPA attached to the Agreement

1.1.3.   Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As stated in the Agreement

Annex 1B: Description of Transfer: As stated in the Agreement

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As stated in the Agreement

Annex III: List of Sub processors (Modules 2 and 3 only): None

1.1.4. Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

1.2. Part 2: Mandatory Clauses

1.2.1. Entering into this Addendum

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

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

1.2.2. Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum 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.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

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

8. Any references to 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 Addendum has been entered into.

1.2.3. Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

1.2.4. Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

   a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

   b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

   c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

   a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

   b. In Clause 2, delete the words:

   > "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";

   c. Clause 6 (Description of the transfer(s)) is replaced with:

   > "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

   d. Clause 8.7(i) of Module 1 is replaced with:

   > "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

   e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

   > "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

   f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of

"Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

1.2.5. Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

   a   its direct costs of performing its obligations under the Addendum; and/or

   b   its risk under the Addendum,

   and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum 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 Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.