GLOBAL DATA PROCESSING AGREEMENT

This Global Data Processing Agreement ("**DPA**") is effective as of the effective date of the Principal Agreement (as defined below). "**Heath**" means Heath Consultants Incorporated. This DPA is subject to, and part of, the Principal Agreement. By entering into a Principal Agreement that references this DPA, Customer agrees to and enters into this DPA with Heath. This DPA applies solely to the Processing of Personal Data where, and to the extent, an agreement for the Processing of Personal Data is required by Data Protection Law.

1. DEFINITIONS.

"**Controller**" means a "controller" or "business" as applicable under Data Protection Law.

"**Customer**" means the organization to which Heath provides services under the Principal Agreement.

"**Data Processing Exhibit**" is the Exhibit hereto that describes Heath's Processing activities. If EU Standard Contractual Clauses or the UK Addendum is incorporated into this DPA, then **Part 1: Table 3 - Annex I** to such UK Addendum and **Annex I** to such EU Standard Contractual Clauses shall be deemed to be the same as the Data Processing Exhibit.

"**Data Protection Law**" means all applicable laws or regulations relating to the privacy or protection of Personal Data, including without limitation: **(a)** EU Regulation 2016/679 (together with any related laws adopted by any EEA member states and together with any related regulations, "**GDPR**"); **(b)** the retained EU law version of EU Regulation 2016/679 as enacted into UK law ("**UK GDPR**"); **(c)** the California Consumer Privacy Act of 2018 and the California Privacy Rights Act (together with any related regulations, the "**CPRA**"); and **(d)** any amendments, updates, or replacements to any of the foregoing.

"**Data Regulator"** means any governmental body responsible for administering Data Protection Laws, including without limitation any "Supervisory Authority" as defined in GDPR or UK GDPR.

"**Data Subject**" means any Natural Person to whom Personal Data relates.

"**EEA**" means the European Economic Area and Switzerland.

"**Natural Person**" means any person who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier or device identifier, or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that person.

"**Permitted Sub-Processors**" means the sub-processors authorized by Customer pursuant to **Section 3.1**. The list of Permitted Sub-Processors in Part 1: Table 3 - Annex III of the UK Addendum shall be deemed to be the same as the list of Permitted Sub-Processors in the Data Processing Exhibit.

"**Personal Data**" means information provided to or Processed by Heath by or on behalf of Customer that **(a)** identifies, relates to, describes, is capable of being associated with, or could be linked directly or indirectly to a Natural Person; **(b)** constitutes "personal data," "personal information," "personally identifying information" or an equivalent designation under Data Protection Law; or **(c)** is regulated under Data Protection Law, including without limitation "personal information" as defined in the CPRA.

"**Principal Agreement**" means the agreement, including a License Agreement for Software, and any order forms, exhibits, addendums, and ancillary documents or agreements, between Heath and Customer under which Heath provides Services to Customer and that references this DPA.

"**Processing**" means **(a)** processing, as defined in an applicable Data Protection Law; or **(b)** any other creation, access, modification, disclosure, transfer, storage, deletion, destruction, or other use of Personal Data. "**Process**" and "**Processed**" shall be construed in accordance with this definition.

"**Processor**" means a "processor" or "service provider" as applicable under Data Protection Law.

"**Relevant Country**" means all countries other than those within the European Union, EEA, United Kingdom, or Switzerland and countries in respect of which an adequacy finding under Article 25(6) of the European Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("European Data Protection Directive"), or Article 45 of the GDPR, or UK GDPR, has been given.

"**Security Breach**" means with respect to Personal Data in Heath's possession or control a breach of security of Personal Data, security incident, or an equivalent incident under any other Data Protection Law.

"**Security Exhibit**" is the Exhibit hereto that describes Heath's technical and organizational measures for securing Personal Data. If the UK Addendum is incorporated into this DPA, then **Part 1: Table 3 - Annex II** to such UK Addendum shall be deemed to be the same as the Security Exhibit. If EU Standard Contractual Clauses are incorporated into this DPA, then **Annex II** to such EU Standard Contractual Clauses shall be deemed to be the same as the Security Exhibit.

"**Services**" means services or technology provided by Heath to Customer under the Principal Agreement.

"**EU Standard Contractual Clauses**" means the Standard Contractual Clauses set out in the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 (as may be amended, updated or superseded from time to time), as set out in the EU Standard Contractual Clauses Exhibit.

"**UK Addendum**" means the Addendum issued by the UK Information Commissioner's Office in accordance with the Data Protection Act 2018 on 2 February 2022 (as may be amended, updated or superseded from time to time by the UK Government or the Information Commissioner's Office) and as currently set out in the UK Addendum Exhibit.

"**User**" means any person authorized to use the Services by Customer.

2. PROCESSING OF PERSONAL DATA

2.1 The parties agree that Customer is the Controller under Data Protection Law and Heath is the Processor under applicable Data Protection Law. Each party will comply with the requirements applicable to it under Data Protection Law.

2.2 Customer shall notify Heath in writing of all jurisdictions from which Personal Data will be made available to Heath in connection with the Services. Customer shall ensure that it has obtained all permissions, provided all notices, and documented a valid legal basis necessary to provide the Personal Data to Heath for the purposes contemplated by the Principal Agreement. Customer shall, in its use of the

Services, Process Personal Data in accordance with the requirements of Data Protection Law. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data provided to Heath and the means by which Customer acquired Personal Data.

2.3 Heath shall treat Personal Data as confidential information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions, so long as such instructions comply with applicable Data Protection Laws and reasonable commercial practices, for the following purposes: (i) Processing in accordance with the Principal Agreement; (ii) Processing initiated by Users in their use of the Services; (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; and (iv) Processing necessary to comply with applicable law.

2.4 Where required by Data Protection Law, Heath shall not (1) retain, use, disclose or otherwise Process Personal Data for any purpose (including any commercial purpose) except for the business purpose as provided in the Principal Agreement and this DPA; (2) sell, share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic means, any Personal Data to any third-party for monetary or other valuable consideration; or (3) retain, use, or disclose any Personal Data outside of the direct business relationship between Heath and Customer. Except as permitted by Data Protection Law, Heath shall not combine the Personal Data it receives from Customer with personal information it receives from or on behalf of any other third party or that Heath collects from its own interaction with a Data Subject. Heath shall promptly notify Customer if Heath determines it can no longer meet its obligations under Data Protection Law, in which event Customer may take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data.

2.5 Heath shall 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 are subject to appropriate obligations of confidentiality. Heath shall take commercially reasonable steps to ensure the reliability of any Heath personnel engaged in the Processing of Personal Data.

3. SUB-PROCESSING OF PERSONAL DATA

3.1 Customer hereby authorizes Heath to engage (a) the entities listed in the Data Processing Exhibit as Permitted Sub-Processors to Process Personal Data in compliance with this DPA; and (b) any additional entity ("**Proposed Sub-Processor**") retained by Heath to Process Personal Data in compliance with this DPA. Heath shall provide Customer with prior written notice (email sufficing) before permitting a Proposed Sub-Processor to Process Personal Data. Customer may object to a Proposed Sub-Processor only for legitimate data protection reasons. If Customer does not object to the Proposed Sub-Processor in writing within 30 days after receiving such notice, then the Proposed Sub-Processor shall be deemed to be a Permitted Sub-Processor.

3.2 Heath shall impose on each Permitted Sub-Processor, by way of contract, data protection obligations substantially the same as those set out in this DPA.

4. DATA SUBJECT RIGHTS.

4.1 Taking into account the nature of the Services, Heath shall, with respect to Personal Data in Heath's possession or control, assist Customer in fulfilling requests received by Customer from Data Subjects to exercise rights provided to Data Subjects under Data Protection Law (such rights, "Data Subject Rights"). Data Subject Rights include, without limitation (a) deleting Personal Data; (b) providing access to Personal Data; (c) providing a copy of Personal Data; (d) correcting Personal Data; (e) restricting Processing of Personal Data; (f) providing Personal Data in a portable format; (g) providing information about the use or disclosure of Personal Data; or (h) prohibiting or limiting certain uses or disclosures under Data Protection Law.

4.2 If Heath receives a request to exercise any Data Subject Rights, Heath shall (a) forward a copy of such request to Customer; and (b) assist Customer in fulfilling any Data Subject Rights requests as provided in Section 4.1 above.

5. SECURITY; SECURITY BREACHES

5.1 Heath shall maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data (collectively, "**Security Controls**"), as further set forth in the Security Exhibit. Such Security Controls shall include protection against (i) unauthorized or unlawful Processing of Personal Data, (ii) accidental or unlawful destruction, loss or alteration or damage to Personal Data, and (iii) unauthorized disclosure of, or access to, Personal Data. Heath will not materially decrease the overall security of the Services during a subscription term.

5.2 Heath shall (i) promptly investigate each Security Breach; and (ii) take reasonable technical steps to remedy any Security Breach.

5.3 Heath shall notify Customer in writing of a Security Breach affecting Personal Data in Heath's possession or control promptly and without undue delay after Heath first becomes aware of a Security Breach. Heath shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Heath deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Heath's reasonable control. Unless required by Data Protection Law, Heath shall not make any notification of a Security Breach to Data Subjects.

6. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION. If requested, Heath shall provide assistance to Customer with data protection impact assessments and prior consultations with a Data Regulator required under Data Protection Law, taking into account the nature of the Processing and information available to Heath.

7. DELETION OR RETURN OF PERSONAL DATA. Promptly after the expiration or termination of the Principal Agreement, Heath shall, unless otherwise required by applicable law, delete all Personal Data in its possession or control. Prior to the expiration or termination of the Principal Agreement, Customer may, except for Personal Data required to be retained by applicable law, delete Personal Data using the Services.

8. INFORMATION; AUDITS

8.1 Heath shall permit Customer to monitor Heath's compliance with this DPA as further provided in this Section 8. If requested by a Customer, Heath shall, not more than once in any twelve (12) month period, provide information to Customer about Heath's compliance with this DPA in the form or Customer's reasonable information security questionnaire. In the event that Heath elects to have an audit or test performed by a third party on its information systems or security controls, Heath may make the results of such audit or test available to Customer instead of responding to Customer's security questionnaire.

8.2 Additionally, in the event that Customer reasonably believes Heath has materially breached its obligations under this DPA or at the request of a Data Regulator, Heath shall permit Customer or a Data Regulator to conduct an Audit with reasonable advance notice, which shall be no less than thirty (30) days' written notice to Heath. **"Audit**" means an audit and inspection of Heath's procedures and security controls necessary to determine Heath's compliance with this DPA. The Audit shall be conducted at Heath's place of business, during Heath's normal business hours, and without unreasonably interrupting Heath's business operations.

8.3 All information disclosed by Heath under this Section 8 shall be the confidential information of Heath and may only be used to determine Heath's compliance with this DPA.

9. Transfers. This Section 9 shall apply solely if Customer provides Personal Data to Heath that is subject to the Data Protection Laws of the EEA, United Kingdom, or Switzerland (collectively, "**EU Personal Data**"). In the event that Heath transfers EU Personal Data to a Relevant Country, Heath shall transfer such EU Personal Data in accordance with the EU Standard Contractual Clauses and/or UK Addendum. In the event that Heath is certified under the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, or the Swiss-US Data Privacy Framework and Heath transfers EU Personal Data to a Relevant Country, then instead Heath shall transfer such EU Personal Data in accordance with the EU-US Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, or the Swiss-US Data Privacy Framework, as applicable.

10 GENERAL TERMS

10.1 This DPA includes all exhibits, schedules or other attachments hereto. In the event of any conflict or inconsistency between the terms of this DPA and the Principal Agreement (including any exhibits, schedules or other attachments thereto), then the provision providing for greater compliance with applicable law or security and confidentiality of personal data shall control.

10.2 This DPA shall remain in effect until terminated in accordance with the terms of this DPA. This DPA shall automatically terminate upon the expiration or termination of the Principal Agreement.

10.3 Customer shall indemnify, defend and hold harmless Heath and its affiliates and its and their respective officers, directors, shareholders, members, managers, employees and agents from all out-of-pocket costs, damages, losses, judgements, fines, penalties, and expenses (including reasonable attorneys' fees) arising from any third-party demand, claim or proceeding arising from Heath's receipt, storage, use, modification, deletion, or disclosure of Personal Data in accordance with this DPA. Notwithstanding anything to the contrary in the Principal Agreement or otherwise, Customer's indemnity

obligations under this DPA shall not be limited to by any limitation of liability in the Principal Agreement. All other liability of the parties under this DPA shall be subject to the limitation of liability in the Principal Agreement.

[DATA PROCESSING EXHIBIT FOLLOWS]

DATA PROCESSING EXHIBIT

This **Data Processing Exhibit** is incorporated into the DPA to which this Exhibit is attached.

If the EU Standard Contractual Clauses or UK Addendum apply to the Personal Data Processed under this DPA, then this Data Processing Exhibit shall be deemed to be Part 1, Table 3, Annex 1A and 1B to the UK Addendum and Annex I to the EU Standard Contractual Clauses respectively.

The details of the Processing taking place under this DPA are set out below.

EU Standard Contractual Clauses Annex I.A - List of Parties

(1) Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]
Name: Customer
Address: as set forth in the Principal Agreement
Contact person's name, position and contact details: as specified in the Principal Agreement or notified in writing to Heath
Activities relevant to the data transferred under these Clauses: Data exporter utilizes Heath's Services pursuant to the Principal Agreement.
Role (controller/processor): Controller

(2) Data importer(s): [Identity and contact details of the data importer(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: Heath Consultants Incorporated
Address: as set forth in the Principal Agreement
Contact person's name, position and contact details: Abraham Oyewale, Manager, Information Security, abraham.oyewale@heathus.com; 713-844-1207
Data Protection Officer's name, position and contact details: Carolina Hodgson, VP, IT, c.hodgson@heathus.com ; 713-844-1275

Activities relevant to the data transferred under these Clauses: Data importer provides Services to the data exporter pursuant to the Principal Agreement.
Role (controller/processor): Processor

EU Standard Contractual Clauses Annex I.B - Description of Transfer

(3) Categories of data subjects whose personal data is transferred:

Heath employees, distributors, contractors and third party project vendors. Customer employees and contractors

(4) Categories of personal data transferred:

Name (first and last)
Business email address

Business street address
Business City
Business State or province
Business postal code
Business phone number
Other unique identifiers that include any of the foregoing

Log data and data resulting from the use of data importer's Services

Username
Password
Account verification details
Automatically generated geolocation
IP Address
Device ID
MAC address

(5) 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

None

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

Continuous

(7) Nature of the processing:

Processing in cloud and networked computing environments.

(8) Purpose(s) of the data transfer and further processing:

The data exporter utilizes the data importer's Services pursuant to the Principal Agreement, including software-as-a-service in connection with the data importer's devices.

Except as limited by applicable law or the other agreements between data importer and data exporters, data importer's system and services may be used to process Personal Data for purposes of conducting testing (for example, to ensure that Personal Data intended to be used in the system or by the services is used accurately), development (for example, to determine more efficient ways to process Personal Data within data importer's system or services), and training (for example, to train internal users of data exporters how to use Personal Data within data importer's system or with data importer's services).

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

Personal Data will be deleted or destroyed upon the expiration or termination of the Principal Agreement; provided that this DPA shall survive until all Personal Data has been deleted or destroyed in accordance with this DPA and the Principal Agreement.

For purposes of Clause 8.5 of the EU Standard Contractual Clauses (and for any data subject to the UK Addendum), data exporters choose the option of deletion.

(10) Permitted Sub-Processors. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Permitted Sub-Processor: Full Legal Name and street address, including contact details of data protection officer or EU representative, as applicable	Permitted Sub-Processor: Location of data processing activities, including Country	Permitted Sub-Processor: Subject matter and nature of data processing activities
None	not applicable	not applicable

EU Standard Contractual Clauses Annex I.C - Competent Supervisory Authority

(11) Identify the competent supervisory authority/ies for purposes of GDPR or UK GDPR:

Data Protection Commission, Republic of Ireland

SECURITY EXHIBIT

(and, if applicable, Annex II to the EU Standard Contractual Clauses and Part 1, Table 3, Annex II of the UK Addendum)

This **Security Exhibit (and, if applicable, Annex II to the EU Standard Contractual Clauses and Appendix 2 to the UK Standard Contractual Clauses)** is incorporated into the DPA to which this Exhibit is attached. This Exhibit is included in the term "Security Controls", as defined in the DPA.

The following are Security Controls that Heath has implemented and that Heath will maintain to protect Personal Data and Systems for so long as Heath is Processing Personal Data on behalf of Customer. "Systems" means applications and other systems used by Heath to Process Personal Data of Customer.

1. Heath has implemented, and will comply with, a written information security program consistent with established industry standards and including administrative, technical, and physical safeguards appropriate to the nature of the Personal Data and designed to protect such Personal Data and Systems from: unauthorized access, destruction, use, modification, or disclosure; unauthorized access to or use that could result in substantial harm or inconvenience to Customer; and any anticipated threats or hazards to the security or integrity of such Personal Data and Systems;

2. Heath has adopted, implemented, and is maintaining reasonable policies and standards related to security of Personal Data and Systems;

3. Heath has assigned responsibility for information security management and data protection with respect to Personal Data and Systems to a lead resource and other dedicated resources at Heath, and Heath will provide Customer with the contact details of Heath's lead resource if requested by Customer;

4. Heath is devoting, and will continue to devote, adequate personnel and other resources to information security;

5. Heath carries out background and verification checks on employees and contractors who will have access to Personal Data and Systems to the extent permitted under applicable law;

6. Heath requires employees, vendors and others with access to Personal Data and Systems to enter into written confidentiality agreements;

7. Heath conducts annual training to make employees and others with access to Personal Data and Systems aware of information security risks and to enhance compliance with Heath’s policies and standards related to data protection, as well as requiring such employees and other to keep all such data and systems secure and confidential during their assignment and thereafter;

8. Heath has adopted disciplinary procedures that are applied by Heath if there is misuse of Personal Data or Systems by Heath's employees or others with access to Personal Data or Systems;

9. Sub-Processing will be limited to Permitted Sub-Processors in compliance with the DPA, and Heath will ensure that Permitted Sub-Processors are required to implement security controls no less stringent than the Security Controls set forth herein;

10. Heath prevents unauthorized access to Systems and Personal Data through the use of physical and logical entry controls, secure areas for data processing, procedures for monitoring the use of data processing facilities, built-in system audit trails, use of secure passwords, network intrusion detection technology, encryption, pseudonymization and authentication technology, secure log-on procedures, and virus protection, monitoring compliance with its policies and standards related to data protection on an ongoing basis. Without limiting the foregoing, Heath has implemented and complies with the following with respect to Personal Data and Systems:

a. Physical access control measures to prevent unauthorized access to data processing systems such as entry controls including the legitimization of authorized persons (e.g., access ID cards, card readers, alarm systems, burglar alarms, video surveillance and exterior security);

b. Denial-of-use control measures to prevent unauthorized use of data protection systems by technical (keyword/password protection) and organizational measures concerning user identification and authentication (e.g., automatically enforced password complexity, automatic disabling and change requirements, firewalls);

c. Requirements-driven authorization scheme and access rights, and monitoring and logging of system access to permit access to data processing systems to only persons with appropriate access rights and to further limit such access to the only data needed by persons to perform services for Customer;

d. Data transmission control measures to restrict data from being read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and transfer and receipt records. In particular, Heath's information security program shall be designed to facilitate the encryption "in transit" of data over public networks to protect the security of the transmission;

e. Security tests conducted on the Services or Systems;

f. When subcontracting Services involving the processing of sensitive data, shall execute formal agreements with each subcontractor that requires the subcontractor to implement security controls no less stringent than those set forth here;

g. Measures to protect data from accidental destruction or loss including without limitation: data backup, retention and secure destruction policies, secure offsite storage of data sufficient for disaster recovery, uninterrupted power supply, and disaster recovery and emergency programs;

h. Measures to ensure that information collected for different purposes can be processed separately including without limitation adequate logical separation of data (e.g., "internal client capability"/purpose limitation, separation of functions as production and test);

i. Return or secure destruction of the Personal Data as set forth in the DPA.

j. Copies of Personal Data are not made except to the extent necessary to provide Services to Customer;

k. Appropriate technical and organizational measures to ensure availability and resilience of processing systems and services and a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;

l. A patching and vulnerability management program, consistent with the generally accepted best practices of Heath's industry, that requires prompt patching of Systems; and

m. A reasonable plan to prevent and, if necessary, recover from a ransomware attack within a commercially reasonable timeframe and in accordance with applicable laws.

11. Heath will implement and maintain the following controls for Accounts. With respect to this Section 11, "Accounts" means Heath's accounts and accounts or applications Heath provides to its customers.

a. Heath shall implement and maintain password authentication and other controls that meet either (A) or (B) below:

(A) Password authentication will comply with Security Assertion Markup Language 2.0 (or such other standard that Customer may agree to in writing) and will require multifactor authentication.

(B) (1) passwords are forced to change at least every 90 days; (2) passwords that are changed may not re-use the last 5 passwords; and (3) passwords must have at least an 8 character length and have at least three of the following: lowercase letter, upper case letter, numerical digit, special character

EU STANDARD CONTRACTUAL CLAUSES EXHIBIT

This **EU Standard Contractual Clauses Exhibit**, including the EU Standard Contractual Clauses included in this **Exhibit**, is incorporated into the DPA. If there is any conflict between any provision of the EU Standard Contractual Clauses and any provision of the DPA or any other agreement (including without limitation any other exhibit, schedule, or other attachment thereto), then the provision of the EU Standard Contractual Clauses will control to the extent of such conflict with respect to the Personal Data that is subject to the EU Standard Contractual Clauses. Any personal data described in the EU Standard Contractual Clauses is included in the definition of Personal Data.

STANDARD CONTRACTUAL CLAUSES

(controller to processor)

SECTION I

Clause 1
Purpose and scope

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

(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

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such

instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a)The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to

the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's

request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9

Use of sub-processors

(a) 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 30 days 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. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason

to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not

disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

(d) 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.

(e) 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.

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

Clause 17

Governing law

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

that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State of a data exporter with respect to the Personal Data of such data exporter (specify Member State).

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the Member States of the data exporter that is subject to the dispute, and if Personal Data of more than one data exporter is subject to a dispute, then data exporter and data importer shall agree on the court of a Member State to hear such dispute (specify Member State).

(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.

[end of exhibit]

UK ADDENDUM EXHIBIT

This **UK Addendum Exhibit** is incorporated into the DPA. If there is any conflict between any provision of the UK Addendum and any provision of the DPA or any other agreement (including without limitation any other exhibit, schedule, or other attachment thereto), then the provision of the UK Addendum will control to the extent of such conflict with respect to the Personal Data that is subject to the UK Addendum. Any personal data described in the UK Addendum is included in the definition of Personal Data. Part 1: Table 2 should be interpreted as referencing the EU Standard Contractual Clauses (module Controller to Processor) as completed in the EU Standard Contractual Clauses Exhibit. Part 1: Table 4 is deemed to be completed as indicating the data exporter.

Part 2: Mandatory Clauses

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.

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.

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.

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.

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.

[END OF EXHIBIT]