DATA SHARING AGREEMENT FOR CEGA SECONDARY PROVIDER CONTRACTS – CONTROLLER TO CONTROLLER

This Data Sharing Agreement ("DSA") forms an agreement between CEGA Group Services Limited ("CEGA") and you ("You"), the Supplier or Third-Party Provider accepting this DSA by either:

a) electronically signing it;
b) completing it and returning it to us; or
c) signing an Order Form which includes a link to this DSA; or
d) providing services to a patient who is a policyholder whose claim is administered by CEGA ("Policyholder"). In the event that You provide services to a Policyholder, You are deemed to accept the terms of the DSA and Standard Contractual Clauses.

In the event of any conflict between the provisions of any existing agreement between You and CEGA and this DSA, the provisions of this DSA shall control. In the event of any conflict between this DSA and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall control.

EXECUTING THIS DATA SHARING AGREEMENT

This DSA has been pre-signed on behalf of CEGA and is incorporated by reference into any existing agreement between You and CEGA or is incorporated by reference to govern the provision of services by You to any Policyholder or to CEGA.

To execute this DSA, please complete the details for the Data Importer in Annex 1A, ensuring that you include:

a. the full legal entity name that is providing services to a Policyholder or has signed an existing Services Agreement with CEGA;
b. the registered address of this legal entity;
c. the date of your existing Services Agreement with CEGA; and
d. your reference number and our reference number as set out on the relevant documentation.

Please complete the information in the signature box and sign on the next page.

Please insert details of any processors appointed by You in Annex III.

Send the signed DSA to sccremediationproject@charlestaylor.com, indicating your reference and our reference numbers.

This DSA has been pre-signed on behalf of CEGA. For the avoidance of doubt, signature of this DSA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including Schedule 2.

This DSA shall be deemed effective from the date on which this DSA is provided to You in connection with the provision of services to any Policyholder or to CEGA.

For and on behalf of CEGA Group Services Limited

Signature: _____
Jody Baker, CEO

For and on behalf of [Third Party Provider full legal name]
Signature: _____
Name: _____
Title: _____
Date: _____

This Data Sharing Agreement ("the **Agreement** ") is made on [DATE] (the '**Effective Date'**) between:

CEGA Group Services Limited trading as Charles Taylor Assistance, a company incorporated in England and Wales (Company Number. 1303318), with its registered address at The Minster Building, 21 Mincing Lane, London, EC3R 7AG, United Kingdom ("**CT ASSISTANCE**" or "**the Client**").

and

You, the organisation accepting this Agreement (referred to below as "the **Third Party Provider**"),

each a "**party**" and together the "**parties**".

IT IS AGREED as follows:

1. Definitions and Interpretation

1.1. In preparing this , the parties have taken into account the specific tasks and responsibilities of the Third Party Provider in performing the Medical treatment and any risks to the rights and freedoms of any Data Subjects that may be affected.

1.2. In this Agreement the following words and expressions shall have the following meanings:

"Affiliate"	means, with respect to a party, an entity that (directly or indirectly) controls, is controlled by or is under common control with, such party, where control refers to the power to direct or cause the direction of the management policies of another entity, whether through ownership of voting securities, by contract or otherwise;
"Applicable Laws"	means: (i) all applicable laws, statutes, statutory instruments, orders, rules, regulations and codes of practice (whether or not having the force of law) in force from time to time in each part of the United Kingdom of Great Britain and Northern Ireland (the "UK") and as applicable in the European Union or in one of the Member States of the European Union; and (ii) in relation to Public Authority Access only, the laws of the relevant Restricted Country of destination;
"Appropriate Safeguard"	means a safeguard which CT Assistance deems to be necessary to ensure that the Restricted Transfer may occur in accordance with the Data Protection Legislation, including: (a) procuring that any third party provider involved in the Restricted Transfer enters into a data processing agreement or data sharing agreement (as applicable) with the Third Party Provider on terms which are equivalent to those agreed between CT ASSISTANCE and the Third Party Provider relating to the Restricted Transfer (save that the third party provider shall have no right to transfer Personal Data to any other third party or otherwise transfer Personal Data outside of the recipient country except for transfers back CT ASSISTANCE or the Third Party Provider in the originating country);

	and any one of the following: (b) the execution by the Third Party Provider of a Data Transfer Agreement; (c) where the third party provider is a member of the Third Party Provider's Group, relying on a valid set of binding corporate rules that have been approved by a Data Protection Supervisory Authority ("**Binding Corporate Rules**"); (d) promptly replacing the Standard Contractual Clauses with any amended or updated version of those clauses approved from time to time under the Data Protection Legislation; (e) replacing any Appropriate Safeguard with another data transfer mechanism which is or may become available (including any standard clauses forming part of an applicable code of conduct or certification scheme); or (f) such additional requirements as are set out in this Agreement (including the Addendum) in relation to the transfers of data to a third party provider;
"Consent" of the Data Subject	means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
"Data Importer"	means a third party provider that Processes Personal Data in a Restricted Country, which it receives from, or is granted access to by, the Third Party Provider (whether directly from the Third Party Provider or indirectly from another party);
"Data Protection Legislation"	means data protection laws applicable to the parties' Processing of Personal Data under the Agreement, including (as applicable) the GDPR, the UK GDPR and all other mandatory laws and regulations of the European Union, the European Economic Area and the United Kingdom;
"Data Transfer Agreement "	means an agreement between the Third Party Provider and a Data Importer (or between a third party provider and a Data Importer, as applicable) which incorporates the Standard Contractual Clauses;
"Data Transfer Risk Assessment"	(a) means an assessment of the transfer of Personal Data to a Restricted Country, which shall set out: (b) Personal Data which will be transferred and/ or Processed; (c) the country or countries in which and/ or to which Personal Data will be transferred and/or Processed; (d) any third party provider who will be Processing and/or receiving Personal Data in such countries; (e) details of the proposed transfer, including duration, scale and regularity of the transfer, the length of any onward Processing chain and the number of actors involved and the transmission channels; (f) details of any Public Authority Access made to each Data Importer or those third parties with whom each Data Importer may/shall onward share Personal Data; (g) confirmation of the implementation of the appropriate safeguards as are necessary under Data Protection Legislation, including the Appropriate Safeguards;

	(h) without limiting paragraph (d), how each Data Importer will ensure that the Data Subjects have enforcement rights and effective legal remedies; (i) the results of a data protection impact assessment required under Article 35 of the GDPR (where applicable); (j) the local country assessment undertaken to record the Third Party Provider's assessment of legal sufficiency of the recipient country (including whether in the Third Party Provider's reasonable opinion, having regard to Data Protection Legislation), anything in that country's law or practice impinges on the effectiveness of the Appropriate Safeguards, including respecting the essence of the fundamental rights and freedoms and that such laws and practices do not exceed what is necessary and proportionate in a democratic society to safeguard the objectives set out in Article 23(1) of the GDPR and are not otherwise in contradiction with the Data Protection Legislation ("**Local Equivalency**"); (k) what supplementary measures (including relevant technical measures such as encryption of Personal Data, contractual measures and organisational measures) have been adopted by the Third Party Provider as between itself (or a third party, as applicable) and each Data Importer in cases that the local country assessment (referred to in (i) above) has identified any impingement on the effectiveness of the Appropriate Safeguards as a consequence of the laws or practices therein; and (l) that it has regard to and complies with current government, European Data Protection Board, or other Data Protection Supervisory Authority recommendations, policies, procedures, guidance and codes of practice on, and any approval processes in connection with the Restricted Transfer;
"EEA"	means European Economic Area;
"GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), as amended from time to time and **"UK GDPR"** means the GDPR as incorporated into domestic laws of the United Kingdom;
"Good Industry Practice"	means in relation to any activity and under any circumstances exercising the same skill, expertise and judgment and using facilities and resources of a similar or superior quality as would be expected from a person who: (a) is skilled and experienced in providing the medical treatment in question, seeking in good faith to comply with his contractual obligations and seeking to avoid liability arising under any duty of care that might reasonably apply; (b) takes all proper and reasonable care and is diligent in performing his obligations; and (c) complies with all applicable law;
"Group"	means, in relation to any company, that company, its subsidiaries, its holding companies and every subsidiary of each such holding company from time to time;
"Incident Management Plan"	means a plan agreed between CT Assistance and the Third Party Provider for managing incidences of Security Breach;
"Personal Data"	means any information processed under this Agreement which relates to an identified or identifiable natural person and shall include, without

	limitation, all payment card data regulated by the most up to date version (from time to time) of the Payment Card Industry Data Security Standard ("PCI DSS), to the extent processed by or on behalf of the Third Party Provider;
"Processor"	means any person that is receiving and processing Personal Data on behalf of a data controller;
"Public Authority Access Request"	means a request for disclosure of, or direct access to, Personal Data by any government or public authority (or any body with delegated authority for any of them) under the laws of the relevant Restricted Country to which the Data Importer is subject
"**Request"**	means a subject access request or other data subject right request under Articles 15-22 of the GDPR;
"Security Breach"	means any loss, unauthorised or unlawful destruction, alteration, or unauthorised disclosure of, or access to the Personal Data (accidental or otherwise);
"Special Category Personal Data"	means personal data that specifically reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, 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;
"Standard Contractual Clauses"	means the appropriate set of standard contractual clauses approved by the European Commission or the UK government to legitimise the transfer of personal data to a Third Country Recipient;
"Processor"	has the meaning set out in the GDPR and UK GDPR;
"Public Authority Access Request"	means a request for disclosure of, or direct access to, Personal Data by any government or public authority (or any body with delegated authority for any of them) under the laws of the relevant Restricted Country to which the Data Importer is subject;
"Restricted Country"	means a country, territory or jurisdiction that is outside the UK or the European Economic Area which is not the subject of an adequacy determination by the UK Secretary of State or the European Commission (as applicable);
"Restricted Transfer"	means the transfer, storing or Processing of Personal Data or storing Personal Data in a Restricted Country, either through: (a) direct transfer or remotely (e.g. via outsourcing, as part of business continuity arrangements, cloud arrangements, offshore models etc.); (b) remotely accessing, or allowing remote access to, CT ASSISTANCE's information systems; (c) an onward transfer of Personal Data from a receiving party under a. or b. above, to a further member of its Group or any third party; and/or (d) any other means;
"Sub-Processor"	in the event that the Third Party Provider processes Personal Data on behalf of CT Assistance as its Processor, Sub-processor means any party to which the Third Party Provider has sub-contracted any of its Processor obligations and, in performing such obligations the sub-contractor will receive and process Personal Data;
"Third Party Provider Personnel"	means the Third Party Provider and/or each of its sub-processors and the officers, employees, agents, consultants, representatives and other personnel of the Third Party Provider and each sub-processor;

"UK Restricted Transfer"	means a transfer of Personal Data to, or access to Personal Data from, a jurisdiction outside of the UK and any further onward transfer of that Personal Data to (or access to such Personal Data from) another jurisdiction outside the UK where such transfer or access is not covered by: (i) a positive finding of adequacy by the UK Government (or the relevant UK authority) under UK Data Protection Laws; or (ii) binding corporate rules which have been approved by the relevant authority under UK Data Protection Laws,
"**Working Days**"	means Monday to Friday excluding bank holidays in England and Wales.

1.3. This Agreement supersedes and extinguishes all other contracts, agreements, arrangements and understandings between the Parties, whether written or oral, pertaining to the processing of Personal Data for the purposes of providing the medical treatment agreed between the parties with the exception of where the Third Party Provider and CT Assistance have in place Standard Contractual Clauses and specified IT security requirements.

1.4. Where there is any inconsistency between the terms of this Agreement and any other term of any other contract, the terms of this Agreement shall take precedence.

1.5. References to "include", "includes" and "including" shall be read as being followed by "without limitation" so as to provide a non-exhaustive list of examples.

2. PURPOSE OF PROCESSING

Any Personal Data processed under this Agreement shall be processed only to the extent, and in such manner, as is necessary for

(a) the provision of the medical treatment; or

(b) the proper performance of obligations under this Agreement; or

(c) as authorised by law or any regulatory body.

3. CONTROLLER – CONTROLLER PROVISIONS

3.1. The parties acknowledge that in most circumstances, each party processing Personal Data in connection with this Agreement shall be a controller in relation to such processing. In respect of such processing each Party shall comply with its obligations as a controller under the Data Protection Legislation and shall:

(a) implement appropriate technical and organisational measures to maintain the security of the Personal Data and prevent unauthorised or unlawful access to, or processing of, or any accidental loss, destruction or damage to the Personal Data;

(b) unless otherwise agreed between the relevant Parties, notify the other Party without undue delay:

(i) upon receiving a subject access or other request from a Data Subject of the Personal Data, or if it receives any other claim, complaint or allegation relating to the processing of the Personal Data by the first Party; and

(ii) upon becoming aware of any breach of security leading to the destruction, loss or unlawful disclosure of the Personal Data in the first Party's possession or control,

and in each case the Parties shall cooperate with each other in handling such event and provide all reasonable assistance to the other Party in the discharging of its duties under Data Protection Legislation.

(c) Upon the reasonable request by either Party, the other Party shall provide such information relating to its processing of Personal Data as reasonably required in order to satisfy the requesting Party's obligations under Data Protection Legislation.

4. PROCESSOR OBLIGATIONS

4.1. In the event that the Third Party Provider processes Personal Data as a Processor, on behalf of CT Assistance, this clause 4 shall apply.

4.2. The Third Party Provider warrants that it has provided, or will provide, information to all affected Data Subjects as to how their Personal Data is to be processed.

4.3. The Third Party Provider shall immediately notify CT Assistance in the event that it becomes aware of any issues relating to the accuracy of the Personal Data.

4.4. The Third Party Provider shall process the Personal Data only in accordance with the documented instructions of CT Assistance (which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise notified by CT Assistance to the Third Party Provider during the term of this Agreement).

4.5. If the Third Party Provider is required to process the Personal Data for any other purpose by any United Kingdom, European Union or Member State law, the Third Party Provider will inform CT Assistance of this legal requirement to the extent permitted to do so by applicable law.

4.6. The Third Party Provider shall ensure that Personal Data is only processed by Third Party Provider Personnel Third Party Provider who are reasonably required to do so in order to enable the Third Party Provider to comply with its obligations under this Agreement. The Third Party Provider shall further ensure that all Third Party Provider Personnel who have access to any Personal Data provided under this Agreement:

(a) are informed of the confidential nature of the Personal Data provided;

(b) have received, and will continue to receive, appropriate training to ensure that they are aware of the requirements of Data Protection Legislation and their obligations under this Agreement;

(c) undertake contractually to comply with the obligations of the Third Party Provider as set out in this Agreement and respect the confidentiality of the Personal Data; and

(d) shall not use, publish, disclose or divulge any of the Personal Data other than in the provision of the medical treatment agreed between the parties or proper performance of this Agreement.

4.7. Subject to clause 4.9 below, the Third Party Provider shall not engage a Sub-Processor without the prior specific written authorisation of CT Assistance.

4.8. Where a sub-processor is instructed by the Third Party Provider pursuant to a specific written authorisation provided in accordance with this clause 4.8, such written instructions shall include a requirement that the

Sub-Processor shall be instructed pursuant to a contract containing equivalent data protection obligations as provided for in this Agreement.

4.9. CT Assistance grants the Third Party Provider a general authorisation to engage Sub-Processors for the purposes of providing local or direct assistance to any Data Subject in the management of any claim for medical assistance made by such Data Subject. The Third Party Provider shall inform CT Assistance of any intended changes concerning the addition or replacement of any Sub-Processor, in order that CT Assistance may object to such changes. Any Sub-Processor engaged pursuant to this general authorisation will be subject to a contract providing equivalent data protection obligations as provided for in this Agreement.

4.10. Where the Sub Processor fails to meet its data protection obligations, the Third Party Provider shall remain fully liable to CT Assistance for the performance of those obligations.

5. JOINT CONTROLLERS

5.1. The parties agree that in the event that, on the facts, the Parties are Joint Controllers, each Party shall comply with its obligations under the Data Protection Legislation as a Joint Controller and the provisions of this clause 5 shall apply.

5.2. The Parties agree that CT Assistance shall be the lead Joint Controller for the purposes of this Basic Joint Controller Agreement and shall:

(i) be the exclusive point of contact for Data Subjects and be responsible for all steps necessary to comply with the Data Protection Legislation regarding the exercise by Data Subjects of their rights under the Data Protection Legislation; and

(ii) direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy.

Notwithstanding the terms of clause5.2(i) and (ii), the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation against either Party as Controller.

5.3. Each Party shall:

(i) be solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under the Data Protection Legislation (including but not limited to Articles 13 and 14 of the GDPR and UK GDPR); and

(ii) be responsible for obtaining the informed consent of Data Subjects for the processing where consent is the relevant legal basis for that, in accordance with the Data Protection Legislation;

5.4. The Third Party Provider may only delete or block the Personal Data processed on behalf of CT Assistance upon the written instructions of CT Assistance.

5.5. The Third Party Provider may amend or correct the Personal Data following receipt of instructions directly from the Data Subject or their approved representative. The Third Party Provider will notify CT Assistance of the change and will advise the Data Subject how to contact CT Assistance directly.

5.6. The Third Party Provider must provide all assistance reasonably required by CT Assistance from time to time at no additional cost to CT Assistance, to enable CT Assistance to comply with its obligations under the Data Protection Legislation.

6. INTERNATIONAL DATA TRANSFERS

6.1. In respect of any Restricted Transfer from CT ASSISTANCE to the Third Party Provider, the Parties hereby enter into the Controller – Controller SCCs as amended as follows:

(a) the governing law of the clauses shall be the law of England and Wales, disputes are subject to the jurisdiction of the English courts and the competent Supervisory Authority shall be the UK Information Commissioner's Office

(b) Clause 7 shall be held to apply;

(c) the Option within clause 11 shall not be held to apply;

(d) Annex IA of this Data Protection Agreement shall serve as Annex I; and

(e) Annex II of this Data Protection Agreement shall serve as Annex II.

6.2. If such Restricted Transfer includes any Personal Data which the Third Party Provider processes as a Processor, the Parties shall comply with the Controller- Processor SCCs amended as follows:

(a) the governing law of the clauses shall be the law of England and Wales, disputes are subject to the jurisdiction of the English courts and the competent Supervisory Authority shall be the UK Information Commissioner's Office;

(b) Clause 7 shall be held to apply;

(c) Option 2 shall be held to apply in respect of clause 9(a) with a time period of [10 business days];

(d) the Option within clause 11 shall not be held to apply;

(e) Annex I of this Data Protection Agreement shall serve as Annex I;

(f) Annex II of this Data Protection Agreement shall serve as Annex II; and

(g) Part 2 of Annex III of this Data Protection Agreement shall serve as Annex III.

6.3. Where the performance of the Services requires the Third Party Provider to make any Restricted Transfers, the Third Party Provider must take and continue to take those steps CT ASSISTANCE deems to be necessary to ensure that the Restricted Transfer may occur in compliance with the Data Protection Legislation. The Third Party Provider shall not (and shall ensure that any third party provider shall not) make a Restricted Transfer to a Data Importer without ensuring Appropriate Safeguards are in place and that enforceable Data Subject rights and effective legal remedies are available for Data Subjects in accordance with the Data Protection Legislation. Such safeguards shall include:

(a) conducting a Data Transfer Risk Assessment;

(b) entering into (or procuring that the third party enters into) a Data Transfer Agreement with each relevant Data Importer;

(c) terminating (or procuring that the third party terminates) any set of Old Standard Contractual Clauses that the Third Party Provider (or the third party, as applicable) has entered into, or incorporated into an agreement with, each relevant Data Importer within the timeframe stipulated by the Data Protection Supervisory Authority; and

(d) implementing any other supplementary measures that the Data Transfer Risk Assessment identifies as necessary to achieve Local Equivalency.

6.4. Where, in any circumstances, the Third Party Provider receives, or becomes aware that a third party to whom it has transferred Personal Data has received, a Public Authority Access Request, the Third Party Provider shall

(and shall procure that the relevant third party shall) use reasonable endeavours to advise CT ASSISTANCE in advance of such disclosure, unless the Third Party Provider or any third party (as applicable) is prohibited by Applicable Laws from notifying CT ASSISTANCE of that disclosure, in which case it shall do so as soon as practicable thereafter (where permitted by Applicable Laws).

6.5. In the event that the Third Party Provider (and/or its affiliates or any third party with whom it has shared Personal Data) has made any transfer of Personal Data on the basis of a determination of adequacy which determination is suspended, held to be invalid, or otherwise ceases to be available, the Third Party Provider shall:

(a) notify CT ASSISTANCE in writing; and

(b) promptly take such measures as are necessary to ensure that the medical treatment can continue to be provided in compliance with the provisions of this Agreement and Data Protection Legislation where possible.

6.6. The Third Party Provider shall maintain and provide to CT Assistance on demand records of all Data Processing activities undertaken under this Agreement, including full details of Restricted Transfers together with details of supplementary measures required by clause 6.3(d) to achieve Local Equivalency.

7. SECURITY OF PROCESSING

7.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing undertaken, together with the risks for the rights and freedoms of natural persons, the Third Party Provider shall implement such technical and organisational measures as required to prevent unlawful or unauthorised processing, accidental or unlawful destruction, damage, loss, alteration, disclosure or access to the Personal Data and shall ensure the security of personal data provided under this Agreement.

7.2 The minimum technical and organisational measures required by CT Assistance are detailed in Appendix Two to this Agreement. The Third Party Provider shall provide a written description of the technical and organisational methods employed by the Third Party Provider for processing Personal Data.

7.3 The Third Party Provider must provide all assistance reasonably required by CT Assistance without cost to CT Assistance from time to time to enable CT Assistance to comply with its obligations under Data Protection Legislation.

8. COOPERATION OBLIGATIONS

8.1. The Third Party Provider shall provide notification (including full details and a copy of the request) by email of any request from a Data Subject to exercise any data subject right provided for by Applicable Laws within 3 Working Days of receipt.

8.2. Where the Third Party Provider acts as a Processor, it shall provide electronic copies of any documents required by CT ASSISTANCE to discharge its obligations to the Data Subject within 5 working days of receipt of the request from the Data Subject.

8.3. The Third Party Provider must fully co-operate with and promptly and properly respond to all enquiries from CT Assistance to enable CT Assistance to respond promptly to any enquiry made by any regulator or data

supervisory authority or investigation or assessment of processing initiated by the same in respect of the Personal Data.

8.4. In the event that the Third Party Provider is contacted by any regulator in respect of its medical treatment generally to its customers, any aspect of the medical treatment or in respect of any Personal Data, the Third Party Provider undertakes to promptly inform CT Assistance of all details relating to the same, unless prohibited from doing so by any legal or equitable obligation.

9. PERSONAL DATA BREACH

9.1. If the Third Party Provider suspects or becomes aware of a Security Breach, it shall, without undue delay (and in any event within twenty-four (24) hours of becoming aware) notify CT Assistance of the following:

(a) the date and time of when the Security Breach occurred;

(b) a detailed description of how and when the Security Breach occurred including, where possible, the categories and approximate number of Data Subjects concerned and the measures in place to prevent or mitigate the effect of such Security Breach;

(c) the names and contact details of a contact point within the Third Party Provider where more information may be obtained;

(d) a detailed description of how and when the Security Breach was identified;

(e) the likely consequences of the Security Breach;

(f) the type of Personal Data that was the subject of the Security Breach;

(g) whether steps had been taken to encrypt the Personal Data which was the subject of the Security Breach;

(h) the identity of each affected Data Subject that has been identified to date;

(i) information about any action already taken or proposed to be taken to address the Security Breach, including measures to mitigate its possible adverse effects

as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information that CT Assistance may reasonably request relating to the Security Breach).

9.2. Unless otherwise agreed with CT Assistance in writing, the Third Party Provider shall take action immediately, at its own expense, to stop the Security Breach, investigate the Security Breach and to identify, prevent and mitigate the effects of the Security Breach and to carry out any recovery or other action reasonably necessary to remedy the Security Breach.

9.3. The Third Party Provider shall allow CT Assistance, or any third-party investigator appointed by it, access to the premises, files, IT systems and any other documentation relating to the Security Breach and assist with any investigation of the same.

9.4. The Third Party Provider shall not release or publish any filing, communication, notice, press release, or report concerning the Security Breach without CT Assistance's express prior written approval, save where it is required to do so by Applicable Law. Wherever legally permitted to do so, the Third Party Provider shall provide advance notice to CT Assistance in respect of such filing, communication etc.

10. AUDIT AND COMPLIANCE WITH LAWS

10.1. The Third Party Provider shall submit and contribute to inspections and audits undertaken by CT Assistance (or any agent appointed by CT Assistance) in relation to its data processing activities. This includes the Third Party Provider providing access to any premises under its control where processing under this Agreement is undertaken, on reasonable notice and during normal working hours, subject to appropriate security restrictions. In the case of an emergency or crisis situation, the Third Party Provider must provide immediate access to the same.

10.2. The Third Party Provider shall notify CT Assistance immediately upon it becoming aware that any instruction provided to it infringes any provision of United Kingdom, Member State or European Union Law.

10.3. The Third Party Provider shall notify CT Assistance if it considers that it is, or is likely to become, unable to comply with either its obligations under this Agreement or the Data Protection Legislation, and/or CT Assistance's requirements or instructions regarding the processing of the Personal Data.

10.4. In the event of any occurrence within 10.3 above, CT Assistance shall be entitled at no additional cost, to:

(a) suspend the right of the Third Party Provider to process Personal Data (to such extent and for howsoever long as CT Assistance may determine) until the Third Party Provider is able to demonstrate to the reasonable satisfaction of CT Assistance that the Third Party Provider is able and will continue to be able to so comply; or

(b) in the event that the Third Party Provider is unable to demonstrate to the reasonable satisfaction of the CT Assistance, CT Assistance shall be entitled to terminate this Agreement and any underlying contract between the Parties to which it attaches on ten (10) Working Days' written notice.

11. TERMINATION

11.1. Upon termination of this Agreement, the Third Party Provider shall return to CT Assistance all Personal Data it processes as a Processor pursuant to this Agreement, save that it may retain one complete copy of the Personal Data.

11.2. The Personal Data retained by the Third Party Provider post termination of this Agreement shall be retained on an archived basis only and shall not be held as an active record. The data shall be encrypted with strictly limited access to the information.

11.3. The Personal Data retained by the Third Party Provider post termination of this Agreement shall not be processed by the Third Party Provider (other than continued archive retention) unless the Third Party Provider becomes aware that it is, or is to be, subject to a claim or any other action resultant upon its processing operations under this Agreement.

11.4. In the event that further processing pursuant to clause 11.3 is required, the Third Party Provider shall be entitled to process the Personal Data solely for the purposes of defending itself against any claim or complaint brought.

11.5. The Third Party Provider undertakes to permanently delete any retained Personal Data upon the expiry of a term of 7 years commencing on the date of the last activity undertaken in relation to that Personal Data unless the Third Party Provider is under a legal obligation to retain the Personal Data for longer. Where such legal obligation

exists, the Third Party Provider shall only retain the Personal Data for as long as necessary in respect of that legal obligation.

12. LIABILITY

The Third Party Provider is liable for and shall indemnify and keep CT Assistance fully indemnified on demand from and against each and every action, proceeding, liability, loss, damage, cost, claim, administrative fine, expense or demand suffered or incurred by CT Assistance or its Group which arise from, or in connection with, or pursuant to, any act or omission of the Third Party Provider in its performance of its obligations under this Agreement, howsoever arising.

13. CONTACT PERSONS

The relevant persons with responsibility for Data Privacy issues within their respective organisations are:

For CT Assistance: Charles Taylor Group DPO
2 Minster Court
Mincing Lane
London EC3R 7BB
Telephone 0203 320 8888
Email: DPO@charlestaylor.com

For the Third Party Provider: [TO BE INSERTED].

ANNEX I - DETAILS OF DATA TO BE PROCESSED UNDER THE AGREEMENT

Data

A description of the data transferred and the processing that will take place under the Agreement

Subject matter:

- The purpose, nature and subject matter of the Processing of Personal Data by the Third-Party Provider, under this Agreement are those Processing operations which are necessary to provide the medical treatment which the Third Party Provider delivers to CT Assistance or otherwise delivers directly to or on behalf of the Data Subject.

Duration of the processing:

- The Processing of the Personal Data referred to in this Agreement shall occur throughout the duration of the Medical treatment rendered as set out above, but in no event for longer than the term of this Agreement .

Type of personal data:

- Name
- Address
- Date of Birth
- Gender
- Email contact details
- Telephone contact details
- Details of family members
- Bank Account details
- Details of pre-existing medical conditions
- Details of injuries or medical conditions which prevent travelling
- Height
- Weight
- GP details and Medical Records
- Details of Medications

Categories of data subjects:

- Customers
- Policy Holders
- Policy Beneficiaries
- Third Parties
- Next of Kin/Relatives
- Vendors
- Service Providers

ANNEX IA – DESCRIPTION OF CONTROLLER-TO-CONTROLLER DATA TRANSFER

A. LIST OF PARTIES

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: CEGA GROUP SERVICES LIMITED TRADING AS CHARLES TAYLOR ASSISTANCE

Address: 2 Minster Court, Mincing Lane, London, EC3R 7BB
Contact person's name, position and contact details:
Group DPO: DPO@charlestaylor.com
EU Representative: DPOSpain@cegagroup.com

Activities relevant to the data transferred under these Clauses:

(a) the provision of the medical treatment; or remedi

(b) the proper performance of obligations under this Agreement; or

(c) as authorised by law or any regulatory body.

Signature and date: _____

Role (controller/processor): Data Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transfered [*e.g. customer/employee/vendor*]	• Policy Holders • Policy Beneficiaries • Third Parties • Next of Kin/Relatives • Vendors • Service Providers
Categories of Personal Data transferred [*e.g. Names, contact details, information about employment situation, information about financial situation, payment card details*]	• Name • Address • Date of Birth • Gender • Email contact details • Telephone contact details • Details of family members

	• Bank Account details • Details of pre-existing medical conditions • Details of injuries or medical conditions which prevent travelling • Height • Weight • GP details and Medical Records • Details of Medications
Special Category Personal Data transferred [*e.g. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data, data concerning health or sex life, criminal convictions and offences*]. *Note* - If none put N/A	• Financial information including financial position and bank details. • Special category personal data including, potentially, medical history, race, ethnicity, sexual orientation, religious beliefs, trade union membership, genetic and biometric data, political opinions, and any other physical or mental health details including injury details.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	As required for the performance of the Services under the Agreement but in no event for longer than the term of this Agreement.
Nature of the processing Purpose(s) of the data transfer and further processing	Personal Data is to be collected and processed in order to provide the Services under the Agreement which the Third Party Provider delivers to CT ASSISTANCE or otherwise delivers directly to or on behalf of the Data Subjects.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	The terms are set out in the Third Party Provider Data Retention Policy
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As above

C. COMPETENT SUPERVISORY AUTHORITY

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 shall act as competent supervisory authority – Spain.

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

MINIMUM TECHNICAL AND ORGANISATIONAL MEASURES

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorised access to IT systems and to limit any access to authorised Third Party Provider Personnel only. These must include the following technical and organisational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous account.
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators
- The implementation of network, device application, database and platform security

3. Access control to data

Measures must be taken to prevent authorised users from accessing data beyond their authorised access rights and prevent the unauthorised [input, reading, copying, removal] modification or disclosure of data. These measures shall include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems
- Software security measures

4. Disclosure control

Measures must be taken to prevent the unauthorised access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

- Compulsory use of a wholly owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.
- Prohibition of portable media
- Creating an audit trail of all data transfers

5. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.
Measures should include:

- Logging user activities on IT systems

6. Job control

Measures should be put in place to ensure that data is processed strictly in compliance with the Data Processor's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance
- Employee screening
- Employee supervision

7. Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss.
These measures must include:

- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.
These should include:

- Restriction of access to data stored for different purposes according to staff duties
- Segregation of business IT systems
- Segregation of IT testing and production environments

Storage control

Measures should be put in place to secure business facilities, data centres, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability.

Additional Measures

The Parties acknowledge and agree that the following additional measures shall apply to the processing of Personal Data by Supplier pursuant to the following Standard Contractual Clauses:

Contractual Measures:

1. The Supplier must disclose within 48 hours of receipt of any request from any law enforcement agency or authority or government agency or authority to access any personal data processed by the Supplier, whether in respect of CT Personal Data or not. Notice should be provided to the Charles Taylor Group Data Protection Officer at DPO@charlestaylor.com.
2. Where CT, as the Data Exporter, does not consent to the disclosure of Personal Data to a Regulator on the grounds that such disclosure would breach the Data Exporter's applicable Data Protection Laws, the Supplier shall utilise available remedies to challenge the disclosure to the requesting Regulator and to seek interim measures to suspend the effects of the request disclosure until such time as a court of competent jurisdiction has made a final determination that such disclosure is permitted.
3. Any Data Subject that has suffered loss or damage as a result of the Supplier's breach of the Standard Contractual Clauses shall be entitled to recover compensation pursuant from the Supplier (as Processor), without prejudice to its rights to recover compensation from CT (as Controller).
4. The Data Importer is required to implement the technical and organisational measures set out above - the Minimum Technical and Organisational Measures.
5. The Supplier shall, upon reasonable request by the Data Exporter, assist the Data Exporter in the completion of any data transfer impact assessment in respect of any Restricted Transfer.

Organisational measures:

6. The Supplier, as Data Importer, must make available to CT a transparency report on an annual basis, setting out the volume of requests for access to personal data (including, but not limited to CT Personal Data), the nature of the request and, where legally permitted, the government agency or authority making the request.

7. The Supplier shall ensure that user accounts and access management to Supplier systems on which any CT Personal Data is processed will utilise the following access controls:

User accounts and access management.	Active Directory and Microsoft Azure single sign-on with Office 365
Periodic review of user access rights.	Reviewed Quarterly in line with Supplier's IT security policies

8. All personnel of the Supplier are bound by a Code of Ethics governing data use within the Supplier. That Code of Ethics requires Supplier personnel to attest that:

a. they understand that the Supplier is bound by confidentiality obligations under the Agreement;

b. that personal data (including CT Personal Data) is to be treated with discretion and disseminated strictly on a need-to-know basis; and

c. that violation of the Supplier's Code of Ethics can result in discipline, up to and including termination of employment.

Technical Measures

9. The Supplier shall ensure that the following encryption measures are in place and remain in place for the duration of the processing and undertakes to review these measures periodically and update continuously to meet best industry standards for data integrity and security:

Encryption of data in transit	HTTPS for all communications with the Portal, which is secured via Transport Layer Security
Encryption of data at rest	MySQL Enterprise TDE, enabling data- at-rest encryption by encrypting the physical files of the database automatically, in real time, prior to writing to storage and decrypted when read from storage.
Detection of data leakage via email or other communication channel	The Supplier uses data encryption and data backups to help preserve data against attackers or internal mishaps. The Supplier uses data security and retention tools to track, store and classify data built into Microsoft Office 365.

ANNEX III – LIST OF SUBPROCESSORS
PART 1 – LIST OF SUBPROCESSORS APPROVED BY CT ASSISTANCE

[TO BE COMPLETED BY THE THIRD PARTY PROVIDER/DATA IMPORTER UPON EXECUTION WHERE THE THIRD PARTY PROVIDER IS A PROCESSOR]

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

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.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer) CEGA Group Services Limited trading as Charles Taylor Assistance	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: CEGA Group Services Limited Trading name (if different): Charles Taylor Assistance Main address (if a company registered address): 2 Minster Court, Mincing Lane, London, EC3R 7BB Official registration number (if any) (company number or similar identifier): 01303318	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation	Clause 9a (Time period)	Is personal data received from the Importer combined

				or General Authorisation)		with personal data collected by the Exporter?
1	C2C	No	No	NA	NA	NA
2						
3						
4						

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: CEGA Group Services Limited trading as Charles Taylor Assistance
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

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

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.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.