Annex 1
GDPR – Data Protection Act 2018

1. OPERATIVE PROVISIONS

1.1 **Compliance with laws [and confidentiality]**

1.1.1 In performing the Services and its other obligations under this Agreement SCOTT&MEARS will, and will procure that any Authorised Sub-Processor will, comply with the Data Protection Laws.

1.1.2 SCOTT&MEARS, and any persons authorised to process the Personal Data, will keep the Personal Data secret and confidential in accordance with the terms of this Agreement.

1.1.3 Any Authorised Sub-Processor will keep the Personal Data secret and confidential in accordance with the terms of this Agreement.

1.2 **Authority and roles**

1.2.1 Without prejudice to **clause 1.4.1.1,** (INSERT CLIENT NAME) authorises SCOTT&MEARS, on its own behalf, to Process the Personal Data during the term of this Agreement as a Data Processor and solely for the purpose of providing the Services.

1.2.2 The Parties acknowledge and agree that (INSERT CLIENT NAME) is the Data Controller(s) of the Personal Data.

1.3 **Sub-Processing**

1.3.1 The SCOTT&MEARS will not engage or use any third party for the Processing of Personal Data or otherwise cause or permit any third party to Process Personal Data without the prior written consent of (INSERT CLIENT NAME).

1.3.2 If SCOTT&MEARS appoints an Authorised Sub-Processor pursuant to **clause 1.3.1**, SCOTT&MEARS will ensure that there is in place a written contract between SCOTT&MEARS and the Authorised Sub-Processor that specifies the Authorised Sub-Processor's Processing activities and imposes on the Authorised Sub-Processor the same terms as are imposed on the SCOTT&MEARS in this **Annex 1**.

1.3.3 SCOTT&MEARS will remain responsible and fully liable to (INSERT CLIENT NAME) for all acts and omissions of Authorised Sub-Processors as if they were its own. .

1.4 **SCOTT&MEARS's obligations as Data Processor**

1.4.1 SCOTT&MEARS will, and will procure that any Authorised Sub-Processor will:

1.4.1.1 Process the Personal Data only on documented instructions from (INSERT CLIENT NAME) (including for the avoidance of doubt the instructions as are set out in this Agreement;

1.4.1.2 Immediately inform (INSERT CLIENT NAME) if, in its reasonable opinion, any instruction received in connection with this **Annex 1** infringes any Data Protection Laws;

1.4.1.3 Without prejudice to **clause 1.4.1.1**, ensure that Personal Data will be used solely for the purpose of providing, and to the extent required to provide, the Services;

1.4.1.4 Not cause or permit any Processing of Personal Data to occur outside the United Kingdom and/or the European Economic Area (as it is made up from time to time), including by way of any transfer, without (INSERT CLIENT NAME)'s prior written consent;

1.4.1.5 (In the event that the consent more particularly referred to in **clause 1.4.1.4** is given, SCOTT&MEARS will, prior to causing or permitting any such Processing to occur outside the United Kingdom and/or the European Economic Area:

(a) verify that the transfer is to a recipient located within an Adequate Jurisdiction (subject to any applicable restrictions);

(b) ensure that the Standard Contractual Clauses are entered into as between (INSERT CLIENT NAME) (and/or the relevant member of (INSERT CLIENT NAME) Group) as '*data exporter*' and the recipient of the Personal Data (including the Approved Sub-Processor, as relevant) as '*data importer*' and that they remain in place throughout the term of the Agreement;

(c) provide evidence in writing to (INSERT CLIENT NAME) that the recipient of the Personal Data (including the Approved Sub-Processor, as relevant) is certified under the EU/US Privacy Shield framework and that the certification is valid in respect of Processing of Personal Data under this Agreement (and SCOTT&MEARS hereby warrants and undertakes to ensure that the

Standard Contractual Clauses are entered into in the manner more particularly described at **clause 1.4.1.5(b)** immediately in the event that the recipient of the Personal Data is no longer certified under the EU/US Privacy Shield framework); or

(d) provide evidence in writing to (INSERT CLIENT NAME) that the recipient of the Personal Data (including the Approved Sub-Processor, as relevant) has entered into Binding Corporate Rules which are valid in respect of Processing of Personal Data under this Agreement and which have been approved by the European Commission and/or appropriate regulators (and SCOTT&MEARS hereby warrants and undertakes to ensure that the Standard Contractual Clauses are entered into in the manner more particularly described at **clause 1.4.1.5(b)** immediately in the event that the recipient of the Personal Data is no longer a party bound by the Binding Corporate Rules);)

1.4.1.6 (Should any of the transfer mechanisms more particularly referred to in **clause 1.4.1.5** which are being used by SCOTT&MEARS for the purposes of transfers under this Agreement be held by the European Commission to be invalid under the Data Protection Laws or be formally described by the Supervisory Authority as no longer providing for adequate protection for Personal Data under the Data Protection Laws, SCOTT&MEARS will (at the option of (INSERT CLIENT NAME)):

(a) immediately at no additional cost to (INSERT CLIENT NAME) put in place an alternative mechanism for transfers which has been prior approved in writing by (INSERT CLIENT NAME) having regard to the Data Protection Laws; or

(b) cease transfers of the Personal Data to the relevant recipient forthwith and procure that the relevant recipient immediately takes all actions as are necessary in order for SCOTT&MEARS to comply with **clause 1.4.1.11**;)

1.4.1.7 Ensure that every individual who is authorised to Process Personal Data (including for the avoidance of doubt employees and other staff working for SCOTT&MEARS or for any Approved Sub-Processor) has committed themselves to confidentiality (meaning that they are either subject to confidentiality obligations equivalent to those set out in [the terms of this Agreement or that they are under an appropriate statutory obligation of confidentiality), and ensure that

they will comply with this **Annex 1**, be appropriately reliable, qualified and trained, and that they will only be permitted to have access to the Personal Data as necessary to perform their roles in relation to the provision of the Services;

1.4.1.8 Implement (and assist (INSERT CLIENT NAME) to implement) technical and organisational measures so as to ensure a level of security appropriate to the risk presented by Processing the Personal Data including the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, and in particular from a Data Security Incident**.** This may include, but is not limited to; encryption, Pseudonymisation, resilience of processing systems and backing up Personal Data.

1.4.1.9 Notify (INSERT CLIENT NAME) without undue delay (and in any event no later than 12 hours) after becoming aware of any Data Security Incident, including the nature of the Data Security Incident, the categories and approximate number of Data Subjects and Personal Data records concerned, the name and contact details of the data protection officer or other contact point at SCOTT&MEARS (or the relevant Approved Sub-Processor) where more information can be obtained, the likely consequences of the Data Security Incident, and any measure(s) taken or proposed to be taken to address the Data Security Incident and to mitigate its possible adverse effects, in each case taking into account the nature of the Processing and the information available to SCOTT&MEARS, and where and in so far as it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay, but SCOTT&MEARS (and Authorised Sub-Processors, as applicable) may not delay notification under this **clause 1.4.1.9** on the basis that an investigation is incomplete or ongoing;

1.4.1.10 Taking into account the nature of the Processing, and at no additional cost to (INSERT CLIENT NAME), assist (INSERT CLIENT NAME) in fulfilling its/their obligations under the Data Protection Laws, including in relation to:

(a) responding to requests for exercising Data Subjects' rights under the Data Protection Laws, including by appropriate technical and organisational measures, insofar as this is possible, and including the right to be informed, the right to have personal information corrected if it is inaccurate, the right to object to certain processing of personal information, the right to restrict

processing of personal information, the right to have personal information erased (commonly known as 'right to be forgotten'), the right to request access to personal information, the right to move, copy or transfer certain personal information (commonly known as 'data portability'), rights in relation to automated decision making including profiling, and the right to complain to the Supervisory Authority about infringements of the Data Protection Laws, and for the avoidance of doubt in cases where a Data Subject has engaged the right to have personal information erased under the Data Protection Laws, SCOTT&MEARS acknowledges and agrees that merely putting beyond use the Personal Data or suppressing the same will not amount to erasure so as to enable it to comply with this **clause 1.4.1.10(a)**];

(b) (without prejudice to **clause 1.4.1.9**) documenting any Data Security Incidents (including the facts relating to the Data Security Incidents, their effects and the remedial action taken) and reporting any Data Security Incidents to the Supervisory Authority, any other Regulator and/or Data Subjects, including by taking into account the information available to SCOTT&MEARS;

(c) (without prejudice to **clause 1.4.1.9**) taking measures to address Data Security Incidents, including, where appropriate, measures to mitigate their possible adverse effects; and

(d) conducting privacy impact assessments of any Processing operations and consulting with supervisory authorities, Data Subjects and their representatives in respect of the same; and

1.4.1.11 Promptly after the end of the provision of Services relating to Processing of the Personal Data (including following termination of this Agreement if that is when the provision of Services ends) and sooner at any other time at the written request of the Customer (provided the Customer is acting reasonably):

(a) securely delete all Personal Data (including by irrevocably, completely and permanently deleting the same, including from archives and back up facilities, as relevant, and in such a way that there shall be no ability to recover the same at any time from any medium, repository, or location whatsoever), or return to the Customer all Personal Data (and it shall be at the option of the Customer whether there is deletion or, in the alternative, return under this **clause 1.4.1.11(a)**);

(b) (in the event that the Customer opts for return pursuant to **clause 1.4.1.11(a)**) securely delete any existing or remaining copies of the Personal Data (deletion having the same meaning as is set out above); and

(c) promptly certify (via a director) when the exercise described in this **clause 1.4.1.11** has been completed

1.4.1.12 assist the Data Controller with meeting the GDPR Article 32 obligation to keep Personal Data secure.

1.4.1.13 assist the Data Controller with meeting the GDPR Article 35 obligation to carry out Data Protection Impact Assessments (DPIAs).

1.4.1.14 assist the Data Controller with meeting the GDPR Article 36 obligation to consult with their supervisory authority where Data Protection Impact Assessments (DPIAs) indicate there is an unmitigated high risk to the processing.

1.5 **Information provision**

1.5.1 SCOTT&MEARS will, and will procure that Authorised Sub-Processors will, and at no additional cost to (INSERT CLIENT NAME):

1.5.1.1 make available to (INSERT CLIENT NAME) all information necessary to demonstrate compliance with the obligations set out in this **Annex 1**; and

1.5.1.2 allow for and contribute to audits, including inspections, conducted by the or another auditor mandated by (INSERT CLIENT NAME); and

1.5.1.3 allow for and contribute to audits, including inspections, conducted by the Supervisory Authority and provide all information necessary in response to any request from the Supervisory Authority in relation to the same, in each case which relates in whole or in part to the Personal Data; [and

1.5.1.4 without prejudice to **clauses 1.5.1.1, 1.5.1.2 and 1.5.1.3,** conduct an annual audit in respect of its processing of the Personal Data, its compliance with the Data Protection Laws including in relation to the Personal Data, and its compliance with this **Annex 1**, and promptly thereafter supply (INSERT CLIENT NAME) with a copy of a written report in respect of the annual audit including the findings and outcomes relating to the same.

1.6 **Indemnity**

SCOTT&MEARS will indemnify (INSERT CLIENT NAME) and hold it harmless against all of the Liabilities suffered or incurred by it, in each case arising out of or in connection with any breach by SCOTT&MEARS of any of its obligations under this **Annex 1** (including any failure or delay in performing, or negligent performance or non-performance of, any of those obligations) including for the avoidance of doubt any breach by SCOTT&MEARS which arises out of the actions or omissions of any of the Approved Sub-Processors.

1.7 **Liability**

SCOTT&MEARS's liability for any breach of this **Annex 1** and in respect of the indemnity at **clause 1.6** will be unlimited and for the avoidance of doubt all such liability will be outside of any cap(s) or limitation(s) as may be set out in the Agreement.

1.8 **Termination for breach**

A breach of this **Annex 1** by SCOTT&MEARS, including for the avoidance of doubt any breach by SCOTT&MEARS which arises out of the actions or omissions of any of the Approved Sub-Processors, or of the Standard Contractual Clauses (as relevant) will be a material breach of this Agreement.

1.9 **Conflict**

The provisions of the Agreement shall at all times be subject to SCOTT&MEARS's obligations under this **Annex 1**

1.10 **Interpretation of consent**

Wherever **under** this **Annex 1** (INSERT CLIENT NAME)S consent is required before SCOTT&MEARS is permitted to do a particular act or thing, unless expressly provided otherwise, the (INSERT CLIENT NAME) shall be entitled to give or withhold consent or make consent subject to conditions at its sole discretion.

1.11 **Further assurance**

SCOTT&MEARS will execute all such documents and do all such acts or things as (INSERT CLIENT NAME) may **reasonably** request from time to time in order for (INSERT CLIENT NAME) to comply with its/their obligation(s) under the Data Protection Laws, in particular in respect of what is required in written terms between Data Controllers and Data Processors, including having regard to any updates to **Annex 1** which may be necessary from time to time by reason of formal guidance or codes of practice issued by the Supervisory Authority and which are relevant to the subject matter of this **Annex 1**.

1.12 **Description of Processing**

1.12.1 SCOTT&MEARS warrants and undertakes to ensure that its description of the Processing carried out on the Personal Data under

this **Annex 1**is complete and accurate as at the date of SCOTT&MEARS's signature on this **Annex 1.**

1.12.2 (INSERT CLIENT NAME) reserves the right to review and amend the description of the Processing more particularly referred to in **clause 1.12.1** at its sole discretion.

1.13 **Survival**

The clauses in this **Annex 1** shall survive termination of the Agreement.