Data Processing Addendum

1. Definitions:

1.1 "Data Controller" has the meaning given to 'Data Controller' or 'Controller' as appropriate in the Data Protection Laws;

1.2 "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

1.3 "Data Processor" has the meaning given to 'Data Processor' or 'Processor' as appropriate, in the Data Protection Laws;

1.4 "Data Protection Laws" means any and all laws, statutes, enactments, orders or regulations or other similar instruments of general application and any other rules, instruments or provisions in force from time to time relating to the processing of personal data and privacy applicable to the performance of this Agreement, including where applicable the Data Protection Act 1998, the Data Protection Bill, the Regulation of Investigatory Powers Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) as amended or superseded and the GDPR (Regulation (EU) 2016/679);

1.5 "GDPR" means 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to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC as updated, superseded or repealed from time to time;

1.6 "Personal Data" has the meaning given in the Data Protection Laws

2 Compliance with Data Protection Laws

2.1 The Parties shall each comply with their respective obligations under the applicable Data Protection Laws

3 Data Processing Obligations

3.1 In respect of any Personal Data to be processed by a party acting as a Data Processor pursuant to this Agreement for which the other party is Data Controller, the Data Processor shall:

3.1.1 Provide appropriate technical and organisational measures to ensure the protection of the rights of the data subject and to ensure a level of security appropriate to the risk, as required by Article 32 of GDPR or any other relevant Data Protection Laws;

3.1.2 Not engage any other sub-processor without the prior specific or general written authorisation of the Data Controller (and in the case of general written authorisation; the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Data Controller the opportunity to object to such changes);

3.1.3 Ensure that any sub-processor that is engaged to process such Personal Data by the Data Processor is subject to data obligations no less stringent than those applicable to the Data Processor under this Schedule;

3.1.4 Process only that personal data required to perform its obligations under this Agreement or other documented instructions for no other purpose except that required by law;

3.1.5 On termination of this Agreement, at the Data Controller's option, either return or destroy the personal data (including all copies of it) immediately;

3.1.6 Ensure that all persons authorised to access the personal data are subject to obligations of confidentiality;

3.1.7 Make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid out in Article 28 of GDPR and this Schedule, and allow for and contribute to audits, including inspections, conducted by the Data Controller or another

auditor mandated by the Data Controller; provided that, in respect of this provision the Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes Data Protection Laws;

3.1.8 Taking into account the nature of the processing, provide all possible assistance to the Data Controller in connection with the fulfilment of the Data Controller's obligation to respond to requests for the exercise of data subjects' rights pursuant to Chapter III of the GDPR to the extent applicable. Such assistance to be chargeable at the Data Processor's standard rates or rates agreed by the parties from time to time.

3.1.9 Provide the data Controller with assistance in ensuring compliance with articles 32 to 36 (inclusive) of the GDPR (concerning security processing, data breach notification, communication of a personal data breach to the data subject, data protection impact assessments, and prior consultation with supervisory authorities) to the extent applicable to the Data Controller, taking into account the nature of the processing and the information available to the Data Processor. Such assistance to be chargeable at the Data Processor's standard rates or rates agreed by the parties from time to time.

3.1.10 Notify the data controller without undue delay (and in any event, within 24hours) of becoming aware of a security breach in respect of Personal Data that it processes on behalf of the Data Controller in writing if the Data Processor becomes aware of a Data Breach.

3.1.11 Maintain a record of its processing activities in accordance with Article 30(1) of the GDPR

3.1.12 Allow the Data Controller (or its appointed third party auditor) to conduct an audit of compliance of this Schedule by the Data Processor pursuant to this Agreement (including by way of physical inspection) no more frequently than once per year during the term and on at least 10 days' notice to the Data Processor in advance (provided that the Data Processor shall be entitled to require than any third party auditor appointed to conduct such an audit enters into a confidentiality agreement with the Data Processor prior to such an audit being conducted). Support for audits to be chargeable at the Data Processor's standard rates or rates agreed by the parties from time to time.

4. International Data Transfers

4.1 In respect of any Personal Data to be processed by a party acting as Data Processor pursuant to this agreement for which the other party is Data Controller, the Data Processor shall not transfer the Personal Data outside of the EEA or to an international organisation without:

4.1.1 obtaining written permission of the Data Controller;

4.1.2 ensuring appropriate levels of protection including any appropriate safeguards if required, are in place for the Personal Data in accordance with the Data Protection Laws;

4.1.3 notifying the Data Controller of the protections and adequate safeguards in clause 4.1.2 above;

4.1.4 Documenting and evidencing the protections and adequate safeguards in clause 4.1.2 above and allowing the Data Controller access to any relevant documents and evidence