SCHEDULE 9

DATA PROTECTION

PART A

Data Protection

Unless otherwise defined in this Schedule 9, terms and expressions defined in the *conditions of contract* (as amended) have the same meanings herein

1. The following defined terms apply to this Schedule 9:

Client Data means all data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any media (including without limitation electronic, magnetic, optical and tangible media) and which are supplied to the *Contractor* by or on behalf of the *Client* and any IPR relating to the same which are vested in the *Client*.

Client Personal Data Personal Data and/or Sensitive Personal Data Processed by the *Contractor* (including any Subcontractor) on behalf of the *Client*, pursuant to or in connection with this contract as set out in the Processing Statement.

Connected Persons means all and any of the *Contractor's* employees, directors, contractors, agents, Subcontractors, suppliers, shareholders, professional advisers (including lawyers, auditors, financial advisers, accountants and technical consultants) or underwriters.

Data Controller has the meaning given to it in Data Protection Legislation, noting that under General Data Protection Regulation this would be using the definition of “Controller”.

Data Processor has the meaning given to it in Data Protection Legislation, noting that under General Data Protection Regulation this would be using the definition of “Processor”.

Data Protection Impact Assessment a process used to identify and mitigate the privacy and data protection risks associated with an activity involving the Processing of Personal Data.

Data Protection Legislation means:

- any legislation in force from time to time in the United Kingdom which implements the European Community’s Directive 95/46/EC and Directive 2002/58/EC, including but not limited to the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003;
- the General Data Protection Regulation;
- any other legislation in force from time to time in the United Kingdom relating to privacy and/or the Processing of Personal Data; and
- any statutory codes of practice issued by the Information Commissioner in relation to such legislation.

Data Subject has the meaning given to it in Data Protection Legislation.

Fair Processing Notice means such information as the *Client* deems reasonably necessary to comply with its legal obligations in terms of fair, lawful and transparent Processing under the Data Protection Legislation.

General Data Protection Regulation means the Regulation (EU) 2016/679 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data.

Personal Data has the meaning given to it in the Data Protection Legislation.

Processing has the meaning given to it in Data Protection Legislation and “Process”, “Processes” and “Processed” will be construed accordingly.

Processing Statement is to be completed in the form set out at Part B of this Schedule 9.

Restricted Countries any country outside the European Economic Area as may be constituted from time to time or the UK.

Sensitive Personal Data sensitive or special categories of Personal Data including criminal allegations, offences and outcomes data (as defined in Data Protection Legislation) which is Processed pursuant to or in connection with this contract.

Subject Access Request a request made by a Data Subject to access his or her own Personal Data in accordance with rights granted in Data Protection Legislation.

1A Each of the Parties complies at all times with its obligations under the Data Protection Legislation, and the Parties acknowledge that where the *Client* is the Data Controller and is solely responsible for determining the purposes and manner in which Personal Data is to be Processed, the *Contractor* is a Data Processor and will comply with paragraph 3 of this Schedule 9.

2. Details of the Client Personal Data to be Processed by the *Contractor* and the purposes of such Processing are as set out in the Processing Statement, which the Parties complete before any Processing takes place.

3. The *Contractor*:

(a) Processes the Client Personal Data only in accordance with documented instructions from the *Client* to perform its obligations under this contract,

(b) uses its reasonable endeavours to assist the *Client* in complying with its obligations under Data Protection Legislation and does not perform its obligations under this contract in such a way as to cause the *Client* to breach any of its obligations under Data Protection Legislation to the extent the *Contractor* is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations,

(c) notifies the *Client* immediately if it determines or is notified that an instruction to Process Personal Data issued to it by the *Client* is incompatible with any obligations under Data Protection Legislation to the extent the *Contractor* is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations,

(d) maintains, and makes available to the *Client* on its request, documentation which describes the Processing operations for which it is responsible under this contract including:

- the purposes for which Client Personal Data is Processed,
- the types of Personal Data and categories of Data Subject involved,
- the source(s) of the Personal Data,
- any recipients of the Personal Data,
- the location(s) of any overseas Processing of Client Personal Data,
- retention periods for different types of Client Personal Data and
- where possible a general description of the security measures in place to protect Client Personal Data,

(e) where requested to do so by the *Client*, or where Processing Client Personal Data presents a specific risk to the rights and freedoms of Data Subjects, carries out or assists the *Client* to carry out a Data Protection Impact Assessment in accordance with guidance issued from time to time by the Information Commissioner's Office (and any relevant requirements detailed in Data Protection Legislation) and makes the results of such an assessment available to the *Client*,

(f) without prejudice to any cyber security and/or payment card industry data security standard obligations in this contract, takes appropriate technical and organisational

security measures that are satisfactory to the *Client* from time to time, against unauthorised or unlawful Processing of Client Personal Data and against accidental loss, destruction of, or damage to such Client Personal Data,

(g) without prejudice to any cyber security and/or payment card industry data security standard obligations in this contract, provides the *Client* with such information as the *Client* may from time to time require to satisfy itself of compliance by the *Contractor* (including any Subcontractor) with paragraphs 3(f) and 3(h) of this Schedule 9, Part A, including, protocols, procedures, guidance, training and manuals. For the avoidance of doubt, this includes a full report recording the results of any privacy or security audit carried out at the request of the *Contractor* itself or the *Client*,

(h) notifies the *Client* without undue delay and in any event within 24 hours by written notice with all relevant details reasonably available of any actual or suspected breach of this Schedule 9 including the unauthorised or unlawful Processing of Client Personal Data, or its accidental loss, destruction or damage,

(i) having notified the *Client* of a breach in accordance with paragraph 3(h) of this Schedule 9, Part A, keeps the *Client* properly and regularly informed in writing until the breach has been resolved to the satisfaction of the *Client*,

(j) fully cooperates as the *Client* requires with any investigation or audit in relation to Client Personal Data and/or its Processing including allowing access to premises, computers and other information systems, records, documents and agreements as may be reasonably necessary (whether in relation to Processing pursuant to this contract, in relation to compliance with Data Protection Legislation or in relation to any actual or suspected breach), whether by the *Client* (or any agent acting on its behalf), any relevant regulatory body, including the Information Commissioner's Office, the police and any other statutory law enforcement agency, and does so both during the contract and after its termination or expiry (for so long as the *Contractor* retains and/or Processes Client Personal Data),

(k) notifies the *Client* within two (2) business days if the *Contractor* (including any Subcontractor), receives:

- from a Data Subject (or third party on their behalf):
    - a Subject Access Request (or purported Subject Access Request),
    - a request to rectify, block or erase any Client Personal Data or
    - any other request, complaint or communication relating to the *Client's* obligations under Data Protection Legislation.
- any communication from the Information Commissioner or any other regulatory authority in connection with Client Personal Data; or
- a request from any third party for disclosure of Client Personal Data where compliance with such request is required or purported to be required by law,

(l) provides the *Client* with full cooperation and assistance (within the timescales reasonably required by the *Client*) in relation to any complaint, communication or request made as referred to in paragraph 3(k) of this Schedule 9, Part A, including by promptly providing:

- the *Client* with full details and copies of the complaint, communication or request,
- where applicable, such assistance as is reasonably requested by the *Client* to enable it to comply with the Subject Access Request within the relevant timescales set out in Data Protection Legislation and
- where applicable, such assistance as is reasonably required by the *Client* to enable it to comply with a request from a Data Subject to rectify, block or erase any Client Personal Data,

(m) when notified in writing by the *Client*, supplies a copy of, or information about, any Client Personal Data. The *Contractor* supplies such information or data to the *Client* within such time and in such form as specified in the request (such time to be reasonable) or if no period of time is specified in the request, then within two (2) business days from the date of the request,

(n) prepares and securely maintains a record of all categories of Processing activities carried out on behalf of the *Client* in relation to the Client Personal Data, as a minimum: (i) its name and contact details and details of a Data Protection Officer (if appointed) or other person with responsibility for data protection compliance; (ii) the categories of Processing it carries out on behalf of the *Client*; (iii) transfers to Restricted Countries; (iv) a general description of the technical and organisational security measures referred to in this Schedule 9; and (v) the same information in relation to any Subcontractor, together with its name and contact details (together the "Data Record") and when notified in writing by the *Client*, complies with any agreement between the *Client* and any Data Subject in relation to any Processing which causes or is likely to cause substantial and unwarranted damage or distress to such Data Subject, or any court order requiring the rectification, blocking, erasure or destruction of any Client Personal Data,

(o) if required to do so by Data Protection Legislation, appoints a designated Data Protection Officer,

(p) provides all Connected Persons (and any other worker and/or visitor who may enter the Affected Property on behalf of the *Contractor*) a copy of or directions on how to access the Fair Processing Notice provided by the *Client* prior to any Connected Person (or any other worker and/or visitor) entering the Affected Property, and the *Contractor* acknowledges that, if a Connected Person (or any other worker and/or visitor of the *Contractor*) refuses or withdraws consent to use of any security system in place at the Affected Property without proper and reasonable circumstance, they may be denied access at the *Client's* discretion, and

(q) makes available to the *Client* all information necessary to demonstrate compliance with the obligations set out in this Schedule 9.

4. The *Contractor* does not share Client Personal Data with any Subcontractor without prior written consent from the *Client* and only where there is a written contract in place between the *Contractor* and the Subcontractor which requires the Subcontractor to:

(a) only Process Client Personal Data in accordance with the *Client's* documented instructions to the *Contractor* and

(b) comply with the same obligations which the *Contractor* is required to comply with under this Schedule 9 (and clause 130 of this contract).

The *Contractor* remains responsible and liable to the *Client* for all acts and omissions of any Subcontractor as if they were its own.

5. The *Contractor* itself, and procures that any Subcontractor:

(a) only Processes Client Personal Data in accordance with the *Client's* documented instructions to the *Contractor* and as reasonably necessary to perform this contract in accordance with its terms,

(b) does not Process Client Personal Data for any other purposes (in whole or part) and specifically, but without limitation, reproduce or refer to it in training materials, training courses, commercial discussions and negotiations with third parties or in relation to proposals or tenders with the *Client*,

(c) does not Process Client Personal Data in such a way as to:

- place the *Client* in breach of Data Protection Legislation,
- expose the *Client* to the risk of actual or potential liability to the Information Commissioner or Data Subjects,

- expose the *Client* to reputational damage including adverse publicity,

(d) does not allow its personnel to access Client Personal Data unless such access is necessary to Provide the Service,

(e) takes all reasonable steps to ensure the reliability and integrity of all Connected Persons who can access Client Personal Data,

(f) ensures that all Connected Persons who can access Client Personal Data:

- are informed of its confidential nature,
- are made subject to an explicit duty of confidence,
- understand and comply with any relevant obligations created by either this contract or Data Protection Legislation and
- receive adequate training in relation to the use, care, protection and handling of Personal Data on an annual basis,

(g) does not disclose or transfer Client Personal Data to any third party without the *Contractor* having obtained the prior written consent of the *Client* (save where such disclosure or transfer is specifically authorised under this contract),

(h) without prejudice to paragraph 3 of this Schedule 9, Part A, wherever the *Contractor* uses any mobile or portable device for the transmission or storage of Client Personal Data, ensures that each such device encrypts Client Personal Data and

(i) complies during the course of this contract with any written retention and/or deletion policy or schedule provided by the *Client* to the *Contractor* from time to time.

6. The *Contractor* does not, and procures that any Subcontractor does not, Process or otherwise transfer any Client Personal Data in or to any Restricted Countries without prior written consent from the *Client* (which consent may be subject to additional conditions imposed by the *Client*).

7. If, after the Contract Date, the *Contractor* or any Subcontractor wishes to Process and/or transfer any Client Personal Data in or to any Restricted Countries, the following provisions apply:

(a) the *Contractor* submits a written request to the *Client* setting out details of the following:

- the Client Personal Data which will be transferred to and/or Processed in any Restricted Countries,
- the Restricted Countries which the Client Personal Data will be transferred to and/or Processed in,
- any Subcontractor or other third parties who will be Processing and/or receiving Client Personal Data in Restricted Countries,
- how the *Contractor* ensures an adequate level of protection and adequate safeguards in respect of the Client Personal Data that will be Processed in and/or transferred to Restricted Countries so as to ensure the *Client's* compliance with Data Protection Legislation,

(b) in preparing and evaluating such a request, the Parties refer to and comply with applicable policies, procedures, guidance and codes of practice produced by the Parties and/or the Information Commissioner in connection with the Processing of Personal Data in (and/or transfer of Personal Data to) any Restricted Countries,

(c) the *Contractor* complies with any instructions and carries out such actions as the *Client* may notify in writing when providing its consent to such Processing or transfers, including:

- incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) into this contract or a separate data processing agreement between the Parties and

- procuring that any Subcontractor or other third party who will be Processing and/or receiving or accessing the Client Personal Data in any Restricted Countries enters into a data processing agreement with the *Contractor* on terms which are equivalent to those agreed between the *Client* and the *Contractor* in connection with the Processing of Client Personal Data in (and/or transfer of Client Personal Data to) any Restricted Countries, and which may include the incorporation of the clauses referred to in the bullet point above.

8. The *Contractor* and any Subcontractor, acknowledges:

(a) the importance to Data Subjects and the *Client* of safeguarding Client Personal Data and Processing it only in accordance with the *Client's* instructions and this contract,

(b) the loss and damage the *Client* is likely to suffer in the event of a breach of this contract or negligence in relation to Client Personal Data,

(c) any breach of any obligation in relation to Client Personal Data and/or negligence in relation to performance or non-performance of such obligation is deemed a material breach of this contract and a substantial failure by the *Contractor* to comply with his obligations,

(d) without limiting clause 91.8, if the *Contractor* has committed a material breach under paragraph 8(c) of this Schedule 9, Part A on two or more separate occasions, the *Client* may at its option withdraw authorisation for Processing by a specific Subcontractor by immediate written notice.

9. Compliance by the *Contractor* with this Schedule 9 is without additional charge to the *Client* and is not a compensation event.

10. Following termination or expiry of this contract or termination of the *Contractor's* obligation to Provide the Service, in each case howsoever arising, the *Contractor*:

(a) may Process the Client Personal Data only for so long and to the extent as is necessary to properly comply with its non-contractual obligations arising under law (and will then comply with paragraph 10(b) of this Schedule 9, Part A) and only in accordance with the Data Protection Legislation,

(b) subject to paragraph 10(a) of this Schedule 9, Part A:

- on written instructions from the *Client* either securely destroys or securely and promptly returns to the *Client* or a recipient nominated by the *Client* (in such usable format as and to the extent the *Client* may reasonably require) the Client Personal Data or

- in the absence of instructions from the *Client* after 12 months from the expiry or termination of this contract or termination of the *Contractor's* obligation to Provide the Service securely destroys the Client Personal Data.

11. Client Personal Data may not be Processed following termination or expiry of this contract or termination of the *Contractor's* obligation to Provide the Service save as permitted by paragraph 10 of this Schedule 9, Part A.

12. For the avoidance of doubt, and without prejudice to paragraph 10 of this Schedule 9, Part A, the obligations in this Schedule 9 apply following termination or expiry of this contract or termination of the *Contractor's* obligation to Provide the Service to the extent the Party concerned retains or Processes Client Personal Data.

13. The *Contractor* takes reasonable precautions to preserve the integrity of the Client Data and to prevent any corruption or loss of the Client Data.

14. The *Contractor* is responsible for and indemnifies the *Client* from and against any and all fines, court awards, settlements, legal costs, expenses, liabilities, losses, claims and proceedings whatsoever resulting from any breach by the *Contractor* or any *Subcontractor* of the Data Protection Legislation or paragraphs 1 to 14 (inclusive) of this Schedule 9, Part A. The Contractor's liability in respect of any breach of this Schedule 9 insofar as they relate to fines, court awards, settlements and legal costs is unlimited.

PART B

Client Personal Data

1. The Client Personal Data to be Processed by the *Contractor* (if any) concerns the following categories of Data Subject:

[***List the relevant categories of Data Subject, e.g. staff, customers, members of the public.]***

Not Applicable

2. The Client Personal Data to be Processed includes the following types of Personal Data and/or Sensitive Personal Data:

[***List the relevant types of Personal Data, e.g. names, email or postal addresses, telephone numbers, images, other unique identifiers.]***

Not Applicable

3. The Client Personal Data is to be Processed for the following purpose(s):

[***List and summarise the relevant purpose(s).]***

Not Applicable

4. The Client Personal Data is to be Processed in the following Restricted Countries:

[List if applicable]