THE AGREEMENT has been signed for and on behalf of the Parties the day and year written above.

SCHEDULE 1 - KEY AGREEMENT INFORMATION

1.	**Agreement Reference Number:**	**TfL 91209 (Lot 1)**
2.	**Name of Service Provider:**	Mediaedge:cia UK Limited

[redacted]

SCHEDULE 2 - SPECIAL CONDITIONS OF AGREEMENT

PART A – SPECIAL CONDITIONS APPLYING TO ALL CONTRACTS

A1 PRIVACY AND DATA PROTECTION

For the purposes of this paragraph A1, unless the context indicates otherwise, the following expressions shall have the following meanings:

"Authority Personal Data"	Personal Data and/or Sensitive Personal Data Processed by the Service Provider on behalf of the Authority;
"Data Controller"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Data Processor"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Data Subject"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Data Protection Legislation"	the Data Protection Act 1998 (as interpreted in accordance with Directive 95/46/EC) including all regulations made under it and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any amendment or re-enactment of any of them; any other legislation relating to privacy and/or the processing of Personal Data (as amended from time to time); and any guidance or statutory codes of practice issued by the Information Commissioner in relation to such legislation;
"Personal Data"	has the meaning given to it by section 1(1) of the Data Protection Act 1998;
"Privacy Impact Assessment"	a process used to identify and mitigate the privacy and data protection risks associated with an activity involving the Processing of Authority Personal Data;
"Processing"	has the meaning given to it by section 1(1) of the Data Protection Act 1998 and **"Process"** and **"Processed"** will be construed accordingly;
"Restricted Countries"	any country outside the European Economic Area;

"Sensitive Personal Data"	has the meaning given to it by section 2 of the Data Protection Act 1998; and
"Subject Access Request"	a request made by a Data Subject to access his or her own Personal Data in accordance with rights granted pursuant to Data Protection Legislation.

A1.1 With respect to the Parties' rights and obligations under this Agreement and any Contract, the Parties acknowledge that the Authority is a Data Controller and that the Service Provider is a Data Processor in respect of Authority Personal Data.

A1.2 Details of the Authority Personal Data which may be Processed by the Service Provider and the purposes of such Processing are as follows:

A1.2.1 Categories of Data Subject

The Authority Personal Data to be Processed by the Service Provider (if any) concerns the following categories of Data Subjects:

TfL customers

Members of the public

A1.2.2 Categories of Authority Personal Data

The Authority Personal Data to be Processed concerns the following categories of Personal Data and/or Sensitive Personal Data:

Names

Email addresses

Postal addresses

Telephone numbers

A1.2.3 Purpose(s) of the Processing

The Authority Personal Data is to be Processed for the following purpose(s):

For marketing and communications campaigns

A1.2.4 Permitted offshore Processing

The Authority Personal Data is to be Processed in the following Restricted Countries:

Subject to A.1.7 and A1.8 below, none

A1.3 Without prejudice to the generality of Clause 24, the Service Provider shall:

A1.3.1 process the Authority Personal Data only in accordance with instructions from the Authority to perform its obligations under this Agreement and any Contract;

A1.3.2 use its reasonable endeavours to assist the Authority in complying with any obligations under Data Protection Legislation and shall not perform its obligations under this Agreement or any Contract in such a way as to cause the Authority to breach any of its obligations under Data Protection Legislation to the extent the Service Provider is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations;

A1.3.3 if the General Data Protection Regulation of 27 April 2016 (the "GDPR") is in effect, or if regulations imposing obligations of an equivalent nature to the GDPR are in effect, then from the effective date of the GDPR (currently 25 May 2018) or the effective date of such equivalent regulations, maintain a record of all categories of processing activities carried out on behalf of the Authority in accordance with Article 30(2) of the GDPR or the equivalent regulations;

A1.3.4 take appropriate technical and organisational security measures, that are satisfactory to enable the Authority to comply with Data Protection Legislation from time to time, against unauthorised or unlawful Processing of Authority Personal Data and against accidental loss, destruction of, or damage to such Authority Personal Data;

A1.3.5 without prejudice to paragraph A1.3.4, wherever the Service Provider uses any mobile or portable device for the transmission or storage of Authority Personal Data, ensure that each such device encrypts Authority Personal Data;

A1.3.6 provide the Authority with such information as the Authority may reasonably require from time to time require to satisfy itself of compliance by the Service Provider (and/or any authorised sub-contractor) with paragraph A1.3.4 and A1.3.5, including, protocols, procedures, guidance, training and manuals. For the avoidance of doubt, this shall include a report recording the results of any privacy or security audit carried out at the request of the Authority under paragraph A1.15 below;

A1.3.7 where requested to do so by the Authority, or where Processing Authority Personal Data presents a specific risk to privacy, carry out a Privacy Impact Assessment in accordance with guidance

issued from time to time by the Information Commissioner (and any relevant statutory requirements) and make the results of such an assessment available to the Authority;

A1.3.8 notify the Authority within two (2) Business Days if it, or any Sub-contractor, receives:

A1.3.8.1 from a Data Subject (or third party on their behalf):

A1.3.8.1.1 a Subject Access Request (or purported Subject Access Request);

A1.3.8.1.2 a request to rectify, block or erase any Authority Personal Data; or

A1.3.8.1.3 any other request, complaint or communication relating to the Authority's obligations under Data Protection Legislation;

A1.3.8.2 any communication from the Information Commissioner or any other regulatory authority in connection with Authority Personal Data; or

A1.3.8.3 a request from any third party for disclosure of Authority Personal Data where compliance with such request is required or purported to be required by law;

A1.3.9 provide the Authority with full cooperation and assistance (within the timescales reasonably required by the Authority) in relation to any complaint, communication or request made as referred to in paragraph A1.3.8, including by promptly providing:

A1.3.9.1 the Authority with full details and copies of the complaint, communication or request; and

A1.3.9.2 where applicable, such assistance as is reasonably requested by the Authority to enable it to comply with the Subject Access Request within the relevant timescales set out in Data Protection Legislation.

A1.3.10 when notified in writing by the Service Provider, supply a copy of, or information about, any Authority Personal Data. The Service Provider shall supply such information or data to the Authority 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 five (5) Business Days from the date of the request.

A1.3.11 when notified in writing by the Authority, comply with any agreement between the Authority 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 Authority Personal Data;

A1.4 The Authority remains solely responsible for determining the purposes and manner in which Authority Personal Data is to be Processed. The Service Provider shall not share any Authority Personal Data with any sub-contractor or third party without prior written consent from the Authority (in this Agreement, any Contract or otherwise) and unless there is a written contract in place with the sub-contractor which requires the sub-contractor or third party to:

A1.4.1 only Process Authority Personal Data in accordance with the Authority's instructions to the Service Provider; and

A1.4.2 comply with the same obligations with which the Service Provider is required to comply with under this paragraph A1 and Clauses 11.1, 14.1, 18.1, 21, 22, 24 and 25.

A1.5 The Service Provider agrees that, and shall procure that any sub-contractor shall agree that, Authority Personal Data:

A1.5.1 must only be Processed in accordance with the Authority's obligations to comply with Data Protection Legislation and by such of their personnel as need to view or otherwise access Authority Personal Data;

A1.5.2 must only be used as instructed by the Authority and as reasonably necessary to perform this Agreement and any Contract in accordance with their terms;

A1.5.3 must not be used for any other purposes (in whole or part) by any of them (and specifically but without limitation must not be copied or referred to in whole or part through training materials, training courses, discussions or negotiations or contractual arrangements with third parties or in relation to proposals or tenders with the Authority (or otherwise), whether on renewal of this Agreement, any Contract or otherwise, without the prior written consent of the Authority); and

A1.5.4 must not be used so as to place the Authority in breach of Data Protection Legislation and/or to expose it to risk of actual or potential liability to the Information Commissioner, Data Subjects and/or reputational damage and/or to any order being made against the Authority preventing, suspending or limiting the Processing of Authority Personal Data provided that the Service

Provider shall not be in breach of this paragraph A1.5.4 unless it has also breached paragraph A1.5.2.

A1.6 The Service Provider shall, and shall procure that any sub-contractor shall:

A1.6.1 not disclose or transfer Authority Personal Data to any third party or their own personnel unless necessary for the provision of the Services and, for any disclosure or transfer of Authority Personal Data to any third party, obtain the prior written consent of the Authority (save where such disclosure or transfer is specifically authorised under this Agreement or any Contract);

A1.6.2 notify the Authority by written notice with all relevant details reasonably available of any breach of security and/or paragraph A1 in relation to Authority Personal Data including unauthorised or unlawful access or Processing of, or accidental loss, destruction or damage of any Authority Personal Data within 24 hours of the Service Provider becoming aware of such breach;

A1.6.3 keep the Authority properly and regularly informed consequently;

A1.6.4 fully cooperate with the reasonable instructions of the Authority in relation to the Processing and security of Authority Personal Data in accordance with this Agreement and any Contract and in compliance with Data Protection Legislation;

A1.6.5 without prejudice to the Authority's rights under paragraph A1.15, cooperate with any investigation or audit in relation to Authority 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 and having regard to the confidential information of the Service Provider and its clients (whether in relation to Processing pursuant to this Agreement and any Contract, in relation to Data Protection Legislation or in relation to any actual or suspected breach) by any relevant regulatory body, including the Information Commissioner, by the police, or by any other statutory law enforcement agency and shall do so both during this Agreement or any Contract and after its termination or expiry (for so long as the Party concerned retains and/or Processes Authority Personal Data);

A1.6.6 take all reasonable steps to ensure the reliability and integrity of all Service Provider's personnel who can/or do access Authority Personal Data;

A1.6.7 ensure all Service Provider's personnel who can/or do access Authority Personal Data are informed of its confidential nature and do not publish, disclose or divulge any of the Authority

Personal Data to any third party without the prior written consent of the Authority ;

A1.6.8 ensure all Service Provider's personnel who can and/or do access Authority Personal Data have undergone adequate training in relation to the use, care, protection and handling of Personal Data in accordance with Data Protection Legislation and this Agreement or any Contract, understand such obligations and comply with them and ensure that such training is updated at reasonable intervals; and

A1.6.9 comply during the course of this Agreement or any Contract with any written retention and/or deletion policy or schedule proposed by the Authority and agreed by the parties acting reasonably from time to time.

A1.7 The Service Provider shall not, and shall procure that any sub-contractor shall not, Process or otherwise transfer any Authority Personal Data in or to any Restricted Countries without prior written consent from the Authority (which consent may be subject to additional reasonable conditions imposed by the Authority).

A1.8 if, after the Service Commencement Date, the Service Provider or any sub-contractor wishes to Process and/or transfer any Authority Personal Data in or to any Restricted Countries, the following provisions shall apply:

A1.8.1 the Service Provider shall submit a written request to the Authority setting out details of the following:

A1.8.1.1 the Authority Personal Data which will be transferred to and/or Processed in any Restricted Countries;

A1.8.1.2 the Restricted Countries which the Authority Personal Data will be transferred to and/or Processed in;

A1.8.1.3 any sub-contractors or other third parties who will be Processing and/or receiving Authority Personal Data in Restricted Countries;

A1.8.1.4 how the Service Provider shall ensure an adequate level of protection and adequate safeguards in respect of the Authority Personal Data that will be Processed in and/or transferred to Restricted Countries so as to ensure the Authority's compliance with Data Protection Legislation;

A1.8.2 in preparing and evaluating such a request, the Parties shall 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;

A1.8.3 the Service Provider shall comply with any instructions and shall carry out such actions as the Authority may notify in writing when providing its consent to such Processing or transfers, including:

A1.8.3.1 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

A1.8.3.2 procuring that any sub-contractor or other third party who will be Processing and/or receiving or accessing the Authority Personal Data in any Restricted Countries enters into a data processing agreement with the Service Provider on terms which are equivalent to those agreed between the Authority and the Service Provider in connection with, the Processing of Authority Personal Data in (and/or transfer of Authority Personal Data to) any Restricted Countries, and which may include the incorporation of the clauses referred to in A1.8.3.1.

A1.9 The Service Provider and any sub-contractor (if any), acknowledge:

A1.9.1 the importance to Data Subjects and the Authority of safeguarding Authority Personal Data and Processing it only in accordance with this Agreement or any Contract;

A1.9.2 the loss and damage the Authority is likely to suffer in the event of a breach of this Agreement or any Contract or negligence in relation to Authority Personal Data;

A1.9.3 any breach of any obligation in relation to Authority Personal Data and/or negligence in relation to performance or non performance of such obligation shall be deemed a material breach of Contract;

A1.9.4 notwithstanding Clause 28.1.1, if the Service Provider has committed a material breach under paragraph A1.9.3 on two or more separate occasions, the Authority may at its option:

A1.9.4.1 withdraw authorisation for Processing by a specific sub-contractor by immediate written notice; or

A1.9.4.2 terminate this Agreement or any Contract in whole or part with immediate written notice to the Service Provider.

A1.10 If the Service Provider Processes payment card data under this Agreement or any Contract, it shall ensure that it is and that its internal processes and procedures, information technology systems and any equipment that it provides or is provided on its behalf pursuant to this Contract are compliant with the Payment Card Industry Data Security Standard as updated from time to time ("PCI DSS"). In addition the Service Provider shall:

A1.10.1 at least once every 12 months appoint a PCI DSS Qualified Security Assessor ("QSA") to validate that the Service Provider is compliant with (including as set out above) PCI DSS when providing the Services;

A1.10.2 without prejudice to any other audit and inspection rights that the Authority has under this Contract, provide the Authority with copies of any reports and other documents provided by or to the QSA in respect of each such validation; and

A1.10.3 where the QSA recommends that certain steps should be taken by the Service Provider, promptly take those steps and demonstrate to the Authority that those steps have been taken without charge to the Authority.

A1.11 Compliance by the Service Provider with this paragraph A1 shall be without additional charge to the Authority.

A1.12 Following termination or expiry of this Contract, howsoever arising, the Service Provider:

A1.12.1 may Process the 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 A1.12.2);

A1.12.2 subject to paragraph A1.12.1, shall;

(a) on written instructions from the Authority either securely destroy or securely and promptly return to the Authority or a recipient nominated by the Authority (in such usable format as and to the extent the Authority may reasonably require) the Authority Personal Data and relevant records and documentation accordingly; or

(b) in the absence of instructions from the Authority after 12 months from the expiry or termination of this Agreement or any Contract securely destroy the Authority Personal Data and relevant records and documentation accordingly.

Authority Personal Data may not be Processed following termination or expiry of this Agreement or any Contract save as permitted by this paragraph A1.12.

A1.13 For the avoidance of doubt, and without prejudice to paragraph A1.12, the obligations in this paragraph A1 shall apply following termination or expiry of this Agreement or any Contract to the extent the Party concerned retains or Processes Authority Personal Data.

A1.14 The indemnity in Clause 20 shall apply to any breach of paragraph A1 and shall survive termination or expiry of this Agreement or any Contract.

A1.15 Subject to paragraph A1.6.5, the Authority has the right on 20 Business Days' written notice, and during business hours) to audit the Service Provider's compliance with its obligations under this paragraph A1, subject to the following conditions:

A1.15.1 the audit shall be conducted by one of the "Big 4" international audit firms, namely Deloitte, KPMG, Ernst & Young or PWC or any reputable independent appropriately qualified auditor agreed by the Parties and appointed by the Service Provider and shall continue for no more than 5 Business Days;

A1.15.2 ;

A1.15.3 The scope of the audit will be agreed by both Parties acting reasonably in writing prior to its commencement;

A1.15.4 The Authority shall bear the cost of any audit (except where a material breach is found in which case the Service Provider shall reimburse the Authority for any third party costs reasonably incurred by the Authority in connection with the audit);

A1.15.5 No access to be given to Service Provider personnel information, other Service Provider confidential information or information relating to other clients;

A1.15.6 If necessary to satisfy the purpose of the audit, the auditor shall on request be provided with: (i) a sufficient summary or the Service Provider's business continuity plans and firewall rules (but the full business continuity plans and firewall rules shall not be provided); and (ii) sufficient evidence that access control to IT server rooms is managed securely and reviewed regularly (but the auditor shall not be permitted access to IT server rooms);