

SCHEDULE 6 - FORM FOR VARIATION

Contract Parties:

- (1) London Transport Museum (Trading) Limited (“the Authority”); and
- (2) BDRC Continental Ltd (trading as BVA BDRC), a company registered in England and Wales (Company Registration Number 02578457 whose registered office is at 12-20 Baron Street, London, N1 9LL, United Kingdom (“the Service Provider”).

Contract Number: TfL 95855

Variation Number: 1

Start Date: 29/02/2024. Expiry Date: 31/10/2027.

AUTHORITY FOR VARIATION TO CONTRACT (AVC)

Pursuant to Clause 32 of the Contract, authority is given for the variation to the Services and the Charges as detailed below. The duplicate copy of this form must be signed by or on behalf of the Service Provider and returned to the Procurement Manager as an acceptance by the Service Provider of the variation shown below.

DETAILS OF VARIATION	AMOUNT (£)
TOTAL	£131,600


For the Authority (Signed)

27/3/2024

(Date Signed)

(Print Name)

(Job Title)

<b>ACCEPTANCE BY THE SERVICE PROVIDER</b>	<b>Signed</b>  	<b>Name</b>
<b>Date Signed</b> <b>8/3/24</b>	<b>Job Title</b> 	

## SCHEDULE 3 – SPECIFICATION

### Approach Summary Fieldwork

April to March in the following year (i.e., 2024 to 2027)

### Sample

Two sample options:

- Around 1,200 interviews for 'core & profile' questions, with around 400 interviews for each of the three 'topic focus' sections

N.B. The exact total will depend on footfall.

### Fieldwork

#### Computer Assisted Personal Interviews (CAPI)

- 15-minute questionnaire covering the full visitor experience
- Experienced interviewer team, familiar with the site and staff

### Deliverables

- Annual report and presentation in May (circa 140 slides)
- Mid year report (circa 40 slides)
- Response to ad hoc data requests throughout the year (3-4 per year)
- MOSAIC profiling of LTM's visitor postcodes (once per year)
- Analysis and reporting of ALVA visitor experience data
- Provision of data to ACE (twice per year)

### Fieldwork detail

- Face-to-face interviews will be conducted by an experienced team of interviewers, familiar with the LTM site, and its staff members.
- Visitors will be stopped as they exit the site, allowing the agency to evaluate the whole visit experience, including visits to the shop, at the point their memory is freshest.
- Sampling will be designed to achieve a representative sample of non-educational adult visitors aged 16+ years.
- Interviews to be spread throughout the year, ensuring coverage of key London school holiday periods (Exact dates to be researched and confirmed nearer the time).

Easter (March to April) (i.e., 2024 to 2027)

Summer (May to June) (i.e., 2024 to 2027)

Summer (July to September) (i.e., 2024 to 2027)

October (half term) (i.e., 2024 to 2027)

Christmas (December to January) (i.e., 2024 to 2027)

February (half term) (i.e., 2024 to 2027)

## Questionnaire detail

- The questionnaire will be reviewed to ensure it remains fit for purpose and to make any broader changes, for example updating exhibition questions and LTM's focus on diversity.
- The core questionnaire will be maintained throughout the year to allow for accurate year-on-year comparisons. However, costs are included for 6 seasonal variations of the questionnaire to accommodate changes to marketing and temporary exhibitions at the museum to ensure new elements are assessed through the research.
- To keep the questionnaire length manageable, while also allowing coverage of all areas required, BVA BDRC will continue to divide the survey into 'core' and 'specialist' questions. The questionnaire will be structured such that:
  - Core questions (including visitor profile) are asked of all respondents, to provide a robust sample size for sub-group analysis and to allow topic focus questions to be assessed in line with these.
  - The core questionnaire will include all sections that are filtered to ensure robust sample sizes e.g. catering, retail, exhibitions.
  - Topic focus questions will each be asked to a third of the respondents. There are 3 'topic focus' sections (A,B,C), which will be rotated between respondents.

## Deliverables detail

- BVA BDRC will use LTM supplied admissions data to weight the survey data to be representative by month, day-type (term-time vs. holiday) and day of week (weekday vs. weekend).
- Costs include assignment to MOSAIC categories.
- BVA BDRC will also apply LTM's new visitor segmentation and will look for differences between segments in our analysis of the results.

## Deliverables for LTM:

- **Annual report (approx. 140 slides)** – based on full year data and including analysis by key subgroups for core questions (e.g. families/ adult only or repeat/first time visitors), sector trends analysis, MOSAIC profiling and ALVA visitor benchmarking data\*.
- **Annual presentation** either online or at London Transport Museum (or other agreed London location).
- **Mid year report** (circa 40 slides)

- **Response to ad hoc data/ analysis requests** (3-4 a year on average).
- **Provision of data for ACE/ Illuminate (PWC) reporting** (twice per year)
- **Provision of data tables and datafile**, as required.
- **Data collection and processing for the ALVA benchmarking survey and use of this data in the CSS reports** (service purchased from ALVA, delivered by BVA BDRC).

\* assuming LTM's continued subscription to the benchmark in order to provide context for interpretation of the findings.

#### ALVA visitor experience benchmarking research

BVA BDRC has managed the visitor benchmarking on behalf of ALVA (Association of Leading Visitor Attractions) for the past two decades.

It is a unique benchmark with around 70 leading UK visitor attractions currently participating, all with over 100,000 visitors a year. This allows BVA BDRC to provide benchmarks cut by region, attraction category, paid/ free sites and indoor/outdoor sites. Moreover, BDRC are able to look at specific sites of interest, such as other London museums, other art & design attractions, or ones with a transport focus (e.g. Museum of London, RAF Museum London, HMS Belfast, Design Museum, Brooklands Museum, SS Great Britain, Tank Museum, Ulster Transport Museum).

In addition to the visitor experience benchmarking, the ALVA research subscription now additionally provides brand health benchmarking at no additional cost. This includes benchmarks against around 100 of the UK's top attractions.

BDRC's co-ordination of the research and direct data access allows BVA BDRC to:

- manage the fieldwork shifts to avoid any clashes, reducing the workload of LTM staff
- do additional analysis above and beyond standard outputs to create bespoke benchmarks and interrogate data in the most meaningful way for LTM

SCHEDULE 4 – CHARGES

2024-27 Visitor Satisfaction Research

The cost for conducting this service as outlined in SCHEDULE 3 - SPECIFICATION is:  
**£131,600**

A breakdown of the costs is detailed below:

	2024/25	2025/26	2026/27
LTM visitor tracking			
• Sample size = 1200			
• Full end of year report (140 pages)			
Optional mid-year report (40 pages)			
Cost for an additional data send to ACE (2 per year instead of 1)			
TOTAL			

## SCHEDULE 5 - SPECIAL CONDITIONS OF CONTRACT

### 1. Privacy and Data Protection

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

<b>“Authority Personal Data”</b>	Personal Data and/or Sensitive Personal Data Processed by the Service Provider or any sub-contractor on behalf of the Authority, pursuant to or in connection with this Contract;
<b>“Data Controller”</b>	has the meaning given to it in Data Protection Legislation;
<b>“Data Processor”</b>	has the meaning given to it in Data Protection Legislation;
<b>“Data Protection Impact Assessment”</b>	a process used to identify and mitigate the privacy and data protection risks associated with an activity involving the Processing of Personal Data;
<b>“Data Protection Legislation”</b>	means:  (a) any legislation in force from time to time in the United Kingdom relating to privacy and/or the Processing of Personal Data, including but not limited to the Data Protection Act 2018;  (b) any statutory codes of practice issued by the Information Commissioner in relation to such legislation; and  (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003;

<b>“Data Subject”</b>	has the meaning given to it in Data Protection Legislation;
<b>“Personal Data”</b>	has the meaning given to it in Data Protection Legislation;
<b>“Processing”</b>	has the meaning given to it in Data Protection Legislation and <b>“Process”</b> and <b>“Processed”</b> will be construed accordingly;
<b>“Restricted Countries”</b>	any country outside the European Economic Area other than the UK following withdrawal from the European Union;
<b>“Sensitive Personal Data”</b>	sensitive or special categories of Personal Data (as defined in Data Protection Legislation) which is Processed pursuant to or in connection with this Contract; and
<b>“Subject Access Request”</b>	a request made by a Data Subject to access his or her own Personal Data in accordance with rights granted in Data Protection Legislation.

A1.1. With respect to the personal data processed in connection with the Contract, the parties agree the following:

- a) each Party shall be a Data Controller under Data Protection Legislation
- b) each Party shall comply with Data Protection legislation and shall not by its action or omission cause the other Party to breach Data Protection legislation
- c) the Contract shall cover the following classes of personal data
 

Names, email or postal addresses, telephone numbers; postcode, age, race or ethnic origin, physical or mental health condition, socio-economic grade expressions of opinion
- d) The Parties agree that in some cases the data may include special category personal data, particularly data relating to health or disability, or racial or ethnic origin of survey respondents. The Parties agree that the lawful basis for this will be consent from the data subjects.
- e) Each party shall be individually responsible for providing a privacy notice to current, past or prospective data subjects in accordance with Articles 13 and 14 of the UK GDPR.
- f) Each Party shall be individually responsible for supporting data subjects in the exercise of their data subject rights to the extent that they are able, based on the processing that they are undertaking at the time that a data subject request is received.



- g) In the event that they receive a Subject Access Request (SAR) for data that is only held by the other Party, each Party shall promptly advise the data subject of this and, with their agreement, shall promptly forward all such subject access requests to other party, or direct the requester to them. Neither Party shall be responsible for answering SARs unless and to the extent that the requested data has already been received by them.
- h) Each Party shall provide reasonable assistance to the other where it is not possible for one Party to handle a data subject request on its own
- i) Each Party shall nominate a single point of contact within their organisation who can be contacted in respect of queries or complaints in relation to this Agreement or any data protection issues.
- j) Each Party shall promptly notify the other in the event of a data security breach affecting the personal data or if it reasonably believes that any aspect of the personal data being processed under the Contract and this Agreement is not consistent with the requirements of data protection legislation
- k) Each Party shall notify the other in the event of a complaint to the Information Commissioner's Office regarding personal data processed under the terms of the Contract and this Agreement and provide them an opportunity to contribute where appropriate
- l) Where not otherwise mentioned in this Agreement, each Party shall be responsible for establishing their own technical and organisational measures to ensure that all personal data is processed in accordance with data protection legislation. This includes ensuring that any processing carried out in Restricted Countries is supported by an appropriate lawful transfer mechanism.

A1.2 To the extent that Service provider may act as a Processor on behalf of the authority, details of the Authority Personal Data to be Processed by the Service Provider and the purposes of such Processing are as follows:

A1.2.1 The Authority Personal Data to be Processed by the Service Provider (if any) concerns the following categories of Data Subject:

London Transport Museum customers or visitors

A1.2.2 The Authority Personal Data to be Processed includes the following types of Personal Data and/or Sensitive Personal Data:

Names, email or postal addresses, telephone numbers; postcode, age, race or ethnic origin, physical or mental health condition,

socio-economic grade, expressions of opinion.

A1.2.3 The Authority Personal Data is to be Processed for the following purpose(s):

For Customer Satisfaction and segmentation Surveys

A1.2.4 The Authority Personal Data is to be Processed in the following Restricted Countries

None

A1.2.5 The duration of the Processing shall be:

1 April 22 until 31 May 2023.

A1.2.6 The nature of the Processing is:

the nature of the Processing may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means).

A1.3 Without prejudice to the generality of Clause 22, and only to the extent that the Service Provider may act as the Authority's Processor, 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 the 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 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 notify the Authority without undue delay if it determines or is notified that an instruction to Process Personal Data issued to it by the Authority is incompatible with any 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;

A1.3.4 maintain, and make available to the Authority on its request, documentation which describes the Processing operations for which it is responsible under this Contract including:

A1.3.4.1 the purposes for which Authority Personal Data is Processed;

A1.3.4.2 the types of Personal Data and categories of Data Subject involved;

A1.3.4.3 the source(s) of the Personal Data;

A1.3.4.4 any recipients of the Personal Data;

A1.3.4.5 the location(s) of any overseas Processing of Authority Personal Data;

A1.3.4.6 retention periods for different types of Authority Personal Data; and

A1.3.4.7 where possible a general description of the security measures in place to protect Authority Personal Data.

A1.3.5 where requested to do so by the Authority, or where Processing Authority Personal Data presents a specific risk to privacy, carry out a Data Protection Impact Assessment in accordance with guidance issued from time to time by the Information Commissioner (and any relevant requirements detailed in Data Protection Legislation) and make the results of such an assessment available to the Authority;

A1.3.6 without prejudice to any cyber security and/or payment card industry data security standard obligations in this Contract, take appropriate technical and organisational security measures that are satisfactory to the Authority 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;

A1.3.7 without prejudice to any cyber security and/or payment card industry data security standard obligations in this Contract, provide the Authority with such information as the Authority may from time to time require to satisfy itself of compliance by the Service Provider

(and/or any authorised sub-contractor) with Clauses A1.3.6 and A1.3.8, including, protocols, procedures, guidance, training and manuals. For the avoidance of doubt, this shall include a full report recording the results of any privacy or security audit carried out at the request of the Service Provider itself or the Authority;

A1.3.8 notify the Authority 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 Clause A1, including the unauthorised or unlawful Processing of Authority Personal Data, or its accidental loss, destruction or damage;

A1.3.9 having notified the Authority of a breach in accordance with Clause A1.3.8, keep the Authority properly and regularly informed in writing until the breach has been resolved to the satisfaction of the Authority;

A1.3.10 fully cooperate as the Authority requires 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 (whether in relation to Processing pursuant to the Contract, in relation to compliance with Data Protection Legislation or in relation to any actual or suspected breach), whether by the Authority (or any agent acting on its behalf), any relevant regulatory body, including the Information Commissioner, the police and any other statutory law enforcement agency, and shall do so both during the Contract and after its termination or expiry (for so long as the Party concerned retains and/or Processes Authority Personal Data);

A1.3.11 notify the Authority within two (2) Business Days if it, or any sub-contractor, receives:

A1.3.11.1 from a Data Subject (or third party on their behalf):

A1.3.11.1.1 a Subject Access Request (or purported Subject Access Request);

A1.3.11.1.2 a request to rectify, block or erase any Authority Personal Data; or

A1.3.11.1.3 any other request, complaint or communication relating to the

Authority's obligations under Data Protection Legislation.

- A1.3.11.2 any communication from the Information Commissioner or any other regulatory authority in connection with Authority Personal Data; or
  - A1.3.11.3 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;
- A1.3.12 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 Clause A1.3.11, including by promptly providing:
  - A1.3.12.1 the Authority with full details and copies of the complaint, communication or request;
  - A1.3.12.2 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; and
  - A1.3.12.3 where applicable, such assistance as is reasonably required by the Authority to enable it to comply with a request from a Data Subject to rectify, block or erase any Authority Personal Data.
- A1.3.13 when notified in writing by the Authority, 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 two (2) Business Days from the date of the request;
- A1.3.14 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; and

A1.3.15 if required to do so by Data Protection Legislation, appoint a designated Data Protection Officer.

A1.4 The Service Provider shall not share Authority Personal Data with any sub-contractor without prior written consent from the Authority and only where there is a written contract in place between the Service Provider and the sub-contractor which requires the sub-contractor 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 which the Service Provider is required to comply with under this Clause A1 (and in particular Clauses 12.1, 16.1, 16.2, 18.1, 20.2, 22 and 23).

A1.5 The Service Provider shall, and shall procure that any sub-contractor shall:

A1.5.1 only Process Authority Personal Data in accordance with the Authority's instructions to the Service Provider and as reasonably necessary to perform the Contract in accordance with its terms;

A1.5.2 not Process Authority 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 Authority;

A1.5.3 not Process Authority Personal Data in such a way as to: A1.5.3.1 place the Authority in breach of Data Protection Legislation;

A1.5.3.2 expose the Authority to the risk of actual or potential liability to the Information Commissioner or Data Subjects; A1.5.3.3 expose the Authority to reputational damage including adverse publicity;

A1.5.4 not allow Service Provider's Personnel to access Authority Personal Data unless such access is necessary in connection with the provision of the Services;

A1.5.5 take all reasonable steps to ensure the reliability and integrity of all

Service Provider's Personnel who can access Authority Personal Data;

A1.5.6 ensure that all Service Provider's Personnel who can access Authority Personal Data:

A1.5.6.1 are informed of its confidential nature;

A1.5.6.2 are made subject to an explicit duty of confidence;

A1.5.6.3 understand and comply with any relevant obligations created by either this Contract or Data Protection Legislation; and

A1.5.6.4 receive adequate training in relation to the use, care, protection and handling of Personal Data on an annual basis.

A1.5.7 not disclose or transfer Authority Personal Data to any third party without the Service Provider having obtained the prior written consent of the Authority (save where such disclosure or transfer is specifically authorised under this Contract);

A1.5.8 without prejudice to Clause A1.3.6, 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; and

A1.5.9 comply during the course of the Contract with any written retention and/or deletion policy or schedule provided by the Authority to the Service Provider from time to time.

A1.6 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 conditions imposed by the Authority).

A1.7 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:

A1.7.1 the Service Provider shall submit a written request to the Authority setting out details of the following:

A1.7.1.1 the Authority Personal Data which will be transferred to and/or Processed in any Restricted Countries;

A1.7.1.2 the Restricted Countries which the Authority Personal Data will be transferred to and/or Processed in;

A1.7.1.3 any sub-contractors or other third parties who will be Processing and/or receiving Authority Personal Data in Restricted Countries;

A1.7.1.4 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;

A1.7.2 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;

A1.7.3 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:

A1.7.3.1 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

A1.7.3.2 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 A1.7.3.1.

A1.8 The Service Provider and any sub-contractor (if any), acknowledge:

A1.8.1 the importance to Data Subjects and the Authority of safeguarding Authority Personal Data and Processing it only in accordance with the Authority's instructions and the Contract;

A1.8.2 the loss and damage the Authority is likely to suffer in the event of a breach of the Contract or negligence in relation to Authority Personal Data;

A1.8.3 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;

A1.8.4 notwithstanding Clause 26.1.1, if the Service Provider has committed a material breach under Clause A1.8.3 on two or more separate occasions, the Authority may at

its option:

A1.8.4.1 exercise its step in rights pursuant to Clause A16;

A1.8.4.1 withdraw authorisation for Processing by a specific sub-contractor by immediate written notice; or

A1.8.4.2 terminate the Contract in whole or part with immediate written notice to the Service Provider.

A1.9 Compliance by the Service Provider with this Clause A1 shall be without additional charge to the Authority.

A1.10 Following termination or expiry of this Contract, howsoever arising, the Service Provider:

A1.12.1 may Process the Authority 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 Clause A1.10.2);

A1.12.2 subject to Clause A1.10.1, shall;

A1.10.2.1 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; or A.10.2.2 in the absence of instructions from the Authority after 12 months from the expiry or termination of the Contract securely

destroy the Authority Personal Data.

A1.11 Authority Personal Data may not be Processed following termination or expiry of the Contract save as permitted by Clause A1.10.

A1.12 For the avoidance of doubt, and without prejudice to Clause A1.10, the obligations in this Clause A1 shall apply following termination or expiry of the Contract to the extent the Party concerned retains or Processes Authority Personal Data.

A1.13 The indemnity in Clause 18 shall apply to any breach of Clause A1 and shall survive termination or expiry of the Contract.

A1.14 The Parties' liability in respect of any breach of Clause 22.1 and this Clause A1 insofar as they relate to fines, court awards, settlements and legal costs shall be unlimited.