



*[SUBJECT TO CONTRACT]*

Contract Reference Number: tfl\_scp\_002004

Date: 07 February 2020

**Contract for Services**  
**between**  
**Transport for London**  
**and**  
**BLUECARSHARING SAS**

**Version: Generic December 2019**

**Contents**

CLAUSE	HEADING.....	PAGE
1.	<b>DEFINITIONS AND INTERPRETATION.....</b>	3
2.	<b>COMMENCEMENT AND DURATION.....</b>	11
3.	<b>THE SERVICES .....</b>	11
4.	<b>CHARGES.....</b>	12
5.	<b>PAYMENT PROCEDURES AND APPROVALS .....</b>	12
6.	<b>WARRANTIES AND OBLIGATIONS .....</b>	14
7.	<b>OPERATIONAL MANAGEMENT .....</b>	14
8.	<b>SERVICE PROVIDER’S PERSONNEL.....</b>	15
9.	<b>SUB-CONTRACTING AND CHANGE OF OWNERSHIP .....</b>	16
10.	<b>CONFLICT OF INTEREST .....</b>	18
11.	<b>ACCESS TO PREMISES AND ASSETS .....</b>	18
12.	<b>COMPLIANCE WITH POLICIES AND LAW .....</b>	19
13.	<b>LONDON LIVING WAGE .....</b>	27
14.	<b>CORRUPT GIFTS AND PAYMENT OF COMMISSION.....</b>	29
15.	<b>EQUIPMENT .....</b>	29
16.	<b>QUALITY AND BEST VALUE .....</b>	30
17.	<b>RECORDS, AUDIT AND INSPECTION .....</b>	30
18.	<b>SET-OFF .....</b>	31
19.	<b>INDEMNITY.....</b>	31
20.	<b>INSURANCE .....</b>	31
21.	<b>THE AUTHORITY’S DATA .....</b>	32
22.	<b>INTELLECTUAL PROPERTY RIGHTS .....</b>	32
23.	<b>PRIVACY, DATA PROTECTION AND CYBER SECURITY .....</b>	32
24.	<b>CONFIDENTIALITY AND ANNOUNCEMENTS.....</b>	32
25.	<b>FREEDOM OF INFORMATION AND TRANSPARENCY .....</b>	33
26.	<b>DISPUTE RESOLUTION.....</b>	35
27.	<b>BREACH AND TERMINATION OF CONTRACT .....</b>	36
28.	<b>CONSEQUENCES OF TERMINATION OR EXPIRY .....</b>	37
29.	<b>DECLARATION OF INEFFECTIVENESS AND PUBLIC PROCUREMENT TERMINATION EVENT .....</b>	38
30.	<b>SURVIVAL .....</b>	41
31.	<b>RIGHTS OF THIRD PARTIES.....</b>	41
32.	<b>CONTRACT VARIATION.....</b>	41
33.	<b>NOVATION.....</b>	42
34.	<b>NON-WAIVER OF RIGHTS.....</b>	42
35.	<b>ILLEGALITY AND SEVERABILITY .....</b>	42
36.	<b>NOTICES.....</b>	42
37.	<b>ENTIRE AGREEMENT.....</b>	43
38.	<b>COUNTERPARTS.....</b>	43
39.	<b>RELATIONSHIP OF THE PARTIES .....</b>	43

40.	<b>FURTHER ASSURANCE</b> .....	44
41.	<b>GOVERNING LAW</b> .....	44
	SCHEDULE 1 - KEY CONTRACT INFORMATION.....	46
	SCHEDULE 2 - SPECIAL CONDITIONS OF CONTRACT .....	49
	SCHEDULE 3 – SPECIFICATION .....	127
	SCHEDULE 4 – CHARGES .....	138
	SCHEDULE 5 - PROJECT PLAN.....	202
	SCHEDULE 6 - FORM FOR VARIATION .....	205
	SCHEDULE 7 - CONTRACT QUALITY, ENVIRONMENTAL & SAFETY CONSIDERATIONS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
	SCHEDULE 8 – RE-TENDER COOPERATION.....	208

**THIS CONTRACT** is made the 14<sup>th</sup> day of December 2020.

**BETWEEN:**

- (1) Transport for London ("**the Authority**"); and
- (2) BLUECARSHARING, SAS, a French limited liability company registered in France (Company Registration Number 528 872 625 RCS NANTERRE) whose registered office is at 23 Rue du Professeur Victor Pauchet, Vaucresson France 92420 ("**the Service Provider**").

**RECITALS:**

On 29<sup>th</sup> January, 2020, the Authority published a Contract Notice to advertise and inform TfL's call for competition for a Micromobility Management System Pilot, project reference number tfl\_scp\_002004. Using the Open Procedure, the Authority was seeking to appoint a provider to develop a system capable of ingesting data from Micromobility operators in London to provide TfL and participating London boroughs with near real time visibility of activity across London and informative analytics. Such a system will support network performance optimisation and long-term transport planning decisions in London.

- A. The Authority wishes the Service Provider to provide the Services and the Service Provider is willing to provide the Services to the Authority on the terms and conditions set out in the Contract.
- B. The Service Provider should be aware that the Authority does not offer any guarantee or minimum volume of the Services that may be delivered under this Contract and does not offer any exclusivity to the Service Provider.

**THE PARTIES AGREE THAT:**

**1. Definitions and Interpretation**

In the Contract (including the Recitals):

- 1.1 unless the context indicates otherwise the following expressions shall have the following meanings:

**"Affected Party"** has the meaning given to it in Clause 27.3;

**"Authority Assets"** means any assets (whether tangible or intangible), materials, resources, systems, networks, connectivity and other equipment, machinery and facilities owned by or licensed to the Authority or any member of the Authority Group;



**“Authority Group”**

shall mean where the Authority is:

- (a) TfL, TfL in its own right and as holding company of all its subsidiaries (as defined in section 1159 of the Companies Act 2006) from time to time together and reference to any **“member of the Authority Group”** shall refer to TfL or any such subsidiary; and
- (b) the Greater London Authority (GLA), the GLA, TfL, the Mayor’s Office for Policing and Crime, the London Fire Commissioner, London Legacy Development Corporation and the Old Oak and Park Royal Development Corporation (**“Functional Bodies”**) each in their own right and as holding companies of all of their subsidiaries (as defined in section 1159 of the Companies Act 2006) from time to time together and reference to any **“member of the Authority Group”** shall refer to the GLA, any Functional Body or any such subsidiary;

**“Authority Premises”**

any land or premises (including temporary buildings) owned or occupied by or on behalf of any member of the Authority Group;

**“Business Day”**

any day excluding Saturdays, Sundays or public or bank holidays in England;

**“Cessation Plan”**

a plan agreed between the Parties or determined by the Authority pursuant to Clauses 29.1 to 29.5 (inclusive) to give effect to a Declaration of Ineffectiveness or Clauses 29.6 to 29.10 (inclusive) to give effect to a Public Procurement Termination Event;

**“Charges”**

the charges payable by the Authority, in consideration of the due and proper performance of the Services in accordance with the Contract, as specified in or calculated in accordance with Schedule 4 as the same may be varied from time to time in accordance with Clause 27.6 or Clause 32;

<b>“Confidential Information”</b>	all information (whether written or verbal) that by its nature may reasonably be regarded as confidential to the Authority (or any member of the Authority Group) whether commercial, financial, technical or otherwise, and including information which relates to the business affairs, customers, suppliers, products, software, telecommunications, networks, trade secrets, know-how or personnel of the Authority Group);
<b>“Contract”</b>	this contract, including the Schedules and all other documents referred to in this contract;
<b>“Contract Commencement Date”</b>	the date for commencement of the Contract specified in Schedule 1;
<b>“Contract Information”</b>	(i) the Contract in its entirety (including from time to time agreed changes to the Contract) and (ii) data extracted from the invoices submitted pursuant to Clause 5 which shall consist of the Service Provider’s name, the expenditure account code, the expenditure account code description, the document number, the clearing date and the invoice amount;
<b>“Contract Manager”</b>	the person named as such in Schedule 1 or such other person as notified to the Service Provider by the Authority;
<b>“Data Protection Legislation”</b>	means: <ul style="list-style-type: none"> <li>(a) 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;</li> <li>(b) Directive (EU) 2016/680 (the Law Enforcement Directive);</li> <li>(c) 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;</li> <li>(d) any statutory codes of practice issued by the Information</li> </ul>

Commissioner in relation to such legislation; and

- (e) the Privacy and Electronic Communications (EC Directive) Regulations 2003;

**“Declaration of Ineffectiveness”**

a declaration of ineffectiveness in relation to this Contract made by a Court of competent jurisdiction pursuant to Regulation 98 of the Public Contracts Regulations 2015 or Regulations 113(2)(a) or 118(3) of the Utilities Contracts Regulations 2016;

**“Force Majeure Event”**

any of the following: riot, civil unrest, war, act of terrorism, threat or perceived threat of act of terrorism, fire, earthquake, extraordinary storm, flood, abnormal weather conditions or other natural catastrophe or strikes, lock-outs or other industrial disputes to the extent that such event has materially affected the ability of the Affected Party to perform its obligations in accordance with the terms of the Contract but excluding any such event insofar as it arises from or is attributable to the wilful act, omission or negligence of the Affected Party or the failure on the part of the Affected Party to take reasonable precautions to prevent such Force Majeure Event or its impact;

**“Holding Company”**

any company which from time to time directly or indirectly controls the Service Provider as set out by section 1159 of the Companies Act 2006;

**“Insolvency Event”**

any of the following:

- (f) either or both of the Service Provider or the Holding Company making any voluntary arrangement with its creditors or becoming subject to an administration order;
- (g) a receiver, administrative receiver, manager, or administrator being appointed over all or part of the business of either or both of the Service Provider or the Holding Company;

- (h) being a company, either or both of the Service Provider or the Holding Company having passed a resolution for its winding-up or being subject to a petition for its winding-up (except for the purposes of a voluntary amalgamation, reconstruction or other re-organisation without insolvency);
- (i) either or both of the Service Provider or the Holding Company ceasing or threatening to cease to carry on its business for any reason or being unable to pay its debts within the meaning of the Insolvency Act 1986;
- (j) being an individual or firm, the Service Provider becoming bankrupt or dying;
- (k) any similar event to those in (a) to (e) above occurring in relation to either or both of the Service Provider or the Holding Company under the law of any applicable jurisdiction for those purposes;

**“Intellectual Property Rights”**

any patent, know-how, trade mark or name, service mark, design right, copyright, rights in passing off, database right, rights in commercial or technical information, any other rights in any invention, discovery or process and any other intellectual property rights, in each case whether registered or unregistered and including applications for the grant of any such rights and all rights or forms of protection having equivalent or similar effect in each case in the United Kingdom and anywhere else in the world;

**“Key Personnel”**

the Service Provider’s key personnel named in Schedule 1;

**“Losses”**

all costs (including legal costs and costs of enforcement), expenses, liabilities (including any tax liability), injuries, direct, indirect or consequential loss (all three of which terms include pure economic loss, loss of profits, loss of business, depletion of goodwill and like loss), damages, claims, demands,

	proceedings and judgments;
<b>“Micromobility Operators”</b>	E-scooter and e-bike / dockless bike companies, as well as other mobility companies that operate within the City of London pursuant to a permit issued by the Authority and are under an obligation to share data within the MDS and / or GBFS or any other mobility data sharing standard, as the Service Provider is notified by the Authority.
<b>“Milestone”</b>	an event which is the completion of one or more of the specified activities as may be set out in the Project Plan;
<b>“Parties”</b>	the Authority and the Service Provider (including their successors and permitted assignees) and <b>“Party”</b> shall mean either of them as the case may be;
<b>“Personal Data”</b>	has the meaning given to it in the Data Protection Legislation;
<b>“Processing”</b>	has the meaning given to it in the Data Protection Legislation;
<b>“Procurement Manager”</b>	the person named as such in Schedule 1 and referred to in Clause 7 or such other person as notified to the Service Provider by the Authority;
	reserved
<b>“Project Plan”</b>	the plan (if any) for implementation including (without limitation) project delivery set out in Schedule 5, developed and agreed by the Parties in relation to the performance and timing of the Services under the Contract which may include Milestones;
<b>“Public Procurement Termination Event”</b>	has the meaning given to it in Clause 29.7;
<b>“Public Procurement Termination Grounds”</b>	any one or more of the grounds described either in Regulation 73(1) of the Public Contracts Regulations 2015 or Regulation 89(1) of the Utilities Contracts Regulations 2016;
<b>“Service Commencement”</b>	the date for commencement of the Services set out in Schedule 1;

<b>Date”</b>	
<b>“Service Provider Equipment”</b>	the equipment and materials of whatsoever nature used by the Service Provider in providing the Services which do not themselves form part of the Services and in which title is not intended to pass to the Authority under the Contract;
<b>“Service Provider’s Personnel”</b>	all such persons, including (without limitation) employees, officers, suppliers, sub-contractors and agents of the Service Provider, as are engaged in the performance of any of the Services and including the Key Personnel;
<b>“Services”</b>	<p>(a) subject to Clause 27.6 all or any part of the services to be provided to, or activities to be undertaken and completed for, the Authority by the Service Provider under the Contract as detailed in the Specification including any variations to such services or activities pursuant to Clause 32; and</p> <p>(b) any services, functions or responsibilities which may be reasonably regarded as incidental to the foregoing services or activities and which may be reasonably inferred from the Contract;</p>
<b>“Specification”</b>	the specification and other requirements set out in Schedule 3;
<b>“Supply Chain Finance Option”</b>	has the meaning given to it in paragraph 1 of Part B of Schedule 6;
<b>“Term”</b>	the period during which the Contract continues in force as provided in Clause 2 and Schedule 1;
<b>“TfL”</b>	Transport for London, a statutory corporation established under the Greater London Authority Act 1999;
<b>“Transparency Commitment”</b>	means the Authority’s commitment to publish its contracts, tender documents and data from invoices received in accordance with the Local Government Transparency Code 2015 and the Authority’s own published

transparency commitments;

**“VAT”**

means value added tax as provided for in the Value Added Tax Act 1994 and any tax replacing the same or of a similar nature.

- 1.2 a reference to the singular includes the plural and vice versa, and a reference to any gender includes all genders;
- 1.3 a reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended or re-enacted by any subsequent statute, enactment, order, regulation or instrument and shall include all statutory instruments or orders made pursuant to it whether replaced before or after the date of execution of the Contract;
- 1.4 a reference to any document other than as specified in Clause 1.3 and save as expressed otherwise shall be construed as a reference to the document as at the date of execution of the Contract;
- 1.5 headings are included in the Contract for ease of reference only and do not affect the interpretation or construction of the Contract;
- 1.6 references to Clauses and Schedules are, unless otherwise provided, references to clauses of, and schedules to, the Contract and any reference to a paragraph in any Schedule shall, in the absence of provision to the contrary, relate to the paragraph in that Schedule;
- 1.7 in the event, and only to the extent, of any conflict between the Clauses and the Schedules, the Clauses prevail, except where:
  - 1.7.1 the conflicting part of the Schedule is explicitly expressed to take precedence; or
  - 1.7.2 the conflict is with a provision in Schedule 2 (Special Conditions of Contract), in which case the provisions in Schedule 2 shall prevail;
- 1.8 the Schedules form part of the Contract and will have the same force and effect as if expressly set out in the body of the Contract;
- 1.9 the expression “person” means any individual, firm, body corporate, unincorporated association, partnership, government, state or agency of a state or joint venture; and
- 1.10 the words “including”, “includes” and “included” will be construed without limitation unless inconsistent with the context.

## **2. Commencement and Duration**

The Contract commences on the Contract Commencement Date and continues in force for the duration stated in Schedule 1 unless terminated earlier in accordance with Clause 27.

## **3. The Services**

### **3.1 The Service Provider:**

3.1.1 shall provide the Services to the Authority from the Service Commencement Date in accordance with the Contract;

3.1.2 acknowledges that it has sufficient information about the Authority and the Specification and that it has made all appropriate and necessary enquiries to enable it to perform the Services in accordance with the Contract;

3.1.3 shall neither be entitled to any additional payment nor excused from any obligation or liability under the Contract due to any misinterpretation or misunderstanding by the Service Provider of any fact relating to the Specification or otherwise to the Contract; and

3.1.4 shall comply with all lawful and reasonable directions of the Authority relating to its performance of the Services.

3.2 Notwithstanding anything to the contrary in the Contract, the Authority's discretion in carrying out its statutory duties shall not be fettered or otherwise constrained or affected by any provision of the Contract;

### **3.3 The Service Provider shall provide the Services:**

3.3.1 with the high degree of skill, care and diligence normally exercised by recognised professional firms or by highly skilled and experienced service providers providing services of a similar scope, type and complexity to the Services and with sufficient resources including project management resources;

3.3.2 in conformance in all respects with the Specification and so that they fulfil the purpose indicated by or to be reasonably inferred from the Specification;

3.3.3 in a safe manner and free from any unreasonable or avoidable risk to any person's health and well-being and in an economic and efficient manner; and

3.3.4 so that they are properly managed and monitored and shall immediately inform the Authority if any aspect of the Contract is not being or is unable to be performed.



- 3.4 Where in the reasonable opinion of the Authority the Service Provider has failed to provide the Services or any part of them in accordance with the Contract, the Service Provider shall, without prejudice to any of the Authority's other rights, re-perform the Services or part thereof as requested by the Authority at no additional cost and within such period of time as reasonably specified by the Authority.
- 3.5 Where reasonably requested to do so by the Authority and provided the Service Provider is willing to so contract, the Service Provider shall contract with such other member(s) of the Authority Group as on the terms of this Contract with only the necessary changes of Parties' details being made.
- 3.6 Throughout the term of the Contract the Service Provider shall when required give to the Authority such written or oral advice or information regarding any of the Services as the Authority may reasonably require.
- 3.7 Where a format for electronic receipt of orders by the Service Provider is set out in Schedule 1, the Service Provider shall, unless the Authority requires otherwise, receive orders in such format and shall maintain its systems to ensure that it is able to do so throughout the Term.

#### **4. Charges**

- 4.1 The Service Provider shall invoice the Authority in accordance with the procedures set out in Clause 5 and in consideration of, and subject to the due and proper performance of the Services by the Service Provider in accordance with the Contract, the Authority shall pay the Service Provider the Charges in accordance with those procedures and with the other terms and conditions of the Contract.
- 4.2 The Service Provider is not entitled to reimbursement for expenses unless such expenses are specified in Schedule 4 or have been incurred with the prior written consent of the Authority, in which case the Service Provider shall supply appropriate evidence of expenditure in a form acceptable to the Authority.
- 4.3 All Charges exclude any VAT which may be chargeable, which will be payable in addition to the sum in question at the rate and in the manner for the time being prescribed by law on delivery of a valid VAT invoice.

#### **5. Payment Procedures and Approvals**

- 5.1 The Service Provider shall invoice the Authority in respect of the Charges:
- 5.1.1 where no Milestones are specified in Schedule 4, at such dates or at the end of such periods as may be specified in Schedule 1; or

5.1.2 if specified in Schedule 4, on completion of each Milestone provided that any preceding Milestones have been completed in accordance with the Contract,

and shall not make any separate charge for submitting any invoice.

5.2 The Service Provider shall submit invoices to the postal address set out in Schedule 1 or via electronic invoicing, provided such electronic invoices comply with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870. Each such invoice shall contain all information required by the Authority including the Contract Reference Number, SAP order number, Service Provider's name, address and bank account details to which payment should be made, a separate calculation of VAT and a brief description of the Services provided. Invoices shall be clear, concise, accurate, and adequately descriptive to avoid delays in processing subsequent payment.

5.3 In the event of a variation to the Services in accordance with the Contract that involves the payment of additional charges to the Service Provider, the Service Provider shall identify these separately on the relevant invoices.

5.4 The Authority shall consider and verify each invoice, which is submitted by the Service Provider in accordance with this Clause 5, in a timely manner. If the Authority considers that the Charges claimed by the Service Provider in any invoice have:

5.4.1 been correctly calculated and that such invoice is otherwise correct, the invoice shall be approved and payment shall be made by bank transfer (Bank Automated Clearance System (BACS)) or such other method as the Authority may choose from time to time within 30 days of receipt of such invoice or such other time period as may be specified in Schedule 1;

5.4.2 not been calculated correctly or if the invoice contains any other error or inadequacy, the Authority shall notify the Service Provider and the Parties shall work together to resolve the error or inadequacy. Upon resolution, the Service Provider shall submit a revised invoice to the Authority.

The Authority shall not be entitled to treat any properly submitted invoice as disputed or incorrect solely due to its own undue delay in considering and verifying it.

5.5 No payment made by the Authority (including any final payment) or act or omission or approval by the Authority or Contract Manager or Procurement Manager (whether related to payment or otherwise) shall:

5.5.1 indicate or be taken to indicate the Authority's acceptance or approval of the Services or any part of them or any act or

omission of the Service Provider, or otherwise prejudice any rights, powers or remedies which the Authority may have against the Service Provider, or absolve the Service Provider from any obligation or liability imposed on the Service Provider under or by virtue of the Contract; or

- 5.5.2 prevent the Authority from recovering any amount overpaid or wrongfully paid including payments made to the Service Provider by mistake of law or fact. Without prejudice to Clause 18, the Authority shall be entitled to withhold such amount from any sums due or which may become due to the Service Provider or the Authority may recover such amount as a debt.
- 5.6 Except where otherwise provided in the Contract, the Charges shall be inclusive of all costs of staff, facilities, equipment, materials and other expenses whatsoever incurred by the Service Provider in discharging its obligations under the Contract.
- 5.7 Interest shall accrue at the rate of two percent (2%) above the base rate of the Bank of England from time to time on all sums due and payable under this Contract from the due date until the date of actual payment (both before and after judgement). All such interest shall be calculated on the basis of the actual number of days elapsed, over a three hundred and sixty five (365) day year and compounded at monthly intervals. The parties agree that this provision constitutes a substantial remedy for late payment of any sum payable under the Contract in accordance with s8(2) of the Late Payment of Commercial Debts (Interest) Act 1998.

## **6. Warranties and Obligations**

[not used – see Schedule 2]

## **7. Operational Management**

- 7.1 The Authority authorises the Contract Manager to act as the Authority's representative for the Contract.
- 7.2 The Service Provider shall deal with the Contract Manager (or his or her nominated representative) in respect of all matters arising under the Contract, except as set out below or unless otherwise notified by the Authority:
  - 7.2.1 variations to the Contract;
  - 7.2.2 any matter concerning the terms of the Contract; and
  - 7.2.3 any financial matter (including any issues in Schedule 4),which shall be referred to the Procurement Manager.

- 7.3 The Service Provider shall, at the Authority's request, provide promptly to the Authority at no additional cost such reports on the provision of the Services as the Authority may reasonably request.

**8. Service Provider's Personnel**

- 8.1 The Parties confirm that the Transfer of Undertakings (Protection of Employment) Regulations 2006 as amended do not apply on the Contract Commencement Date or the expiry or termination of this Contract.
- 8.2 Nothing in this Contract will render the Service Provider's Personnel, an employee, agent or partner of the Authority or Authority Group by virtue of the provision of the Services by the Service Provider under the Contract, and the Service Provider shall be responsible for making appropriate deductions for tax and national insurance contributions from the remuneration paid to the Service Provider's Personnel.
- 8.3 The Service Provider shall provide the Service Provider's Personnel as necessary for the proper and timely performance and management of the Services in accordance with the Contract. All personnel deployed on work relating to the Contract shall have the appropriate qualifications and competence, be properly managed and supervised and in these and any other respects be acceptable to the Authority.
- 8.4 Without prejudice to any of the Authority's other rights, powers or remedies, the Authority may (without liability to the Service Provider) deny access to any Service Provider's Personnel to any Authority Premises and/or require that any Service Provider's Personnel be immediately removed from performing the Services if such Service Provider's Personnel in the Authority's view have not been properly trained in any way required by this Contract, are otherwise incompetent, negligent, guilty of misconduct or could be a danger to any person. The Authority shall notify the Service Provider of such denial and/or requirement in writing and the Service Provider shall comply with such notice and provide a suitable replacement (with the Contract Manager's prior consent in the case of Key Personnel).
- 8.5 The Service Provider shall give the Authority, if so requested, full particulars of all persons who are or may be at any time employed on the Contract and shall take all reasonable steps to avoid changes to any of its staff designated in the Contract as Key Personnel. The Service Provider shall give the Authority reasonable notice of any proposals to change Key Personnel and Clause 8.3 shall apply to the proposed replacement personnel.
- 8.6 Notwithstanding Clause 8.1, the Service Provider shall indemnify, keep indemnified and hold harmless the Authority from and against all Losses which the Authority or other member of the Authority Group incur or suffer in relation to the Service Provider's Personnel or any

person who may allege to be the same (whenever such Losses may arise) or any failure by the Service Provider to comply with Clause 8.4.

- 8.7 The Service Provider shall pay to the Service Provider's Personnel not less than the amounts declared to the Authority (if any) as part of the tender process for the Contract and not less than the amounts to which the Service Provider's Personnel are contractually entitled.
- 8.8 The Service Provider shall provide training to the Authority's personnel (including its employees, officers, suppliers, sub-contractors and agents) as specified in Schedule 1.

## **9. Sub-Contracting and Change of Ownership**

- 9.1 The Service Provider shall not assign or sub-contract all or any part of the Services without the prior written consent of the Authority, which may be refused or granted subject to such conditions as the Authority sees fit.
- 9.2 Where the Service Provider sub-contracts all or any part of the Services to any person, the Service Provider shall:
  - 9.2.1 ensure that such person is obliged to comply with all of the obligations and duties of the Service Provider under the Contract insofar as they relate to the Services or part of them (as the case may be) which that sub-contractor is required to provide;
  - 9.2.2 be responsible for payments to that person;
  - 9.2.3 remain solely responsible and liable to the Authority for any breach of the Contract or any performance, non-performance, part-performance or delay in performance of any of the Services by any sub-contractor to the same extent as if such breach, performance, non-performance, part-performance or delay in performance had been carried out by the Service Provider;
  - 9.2.4 on or before the Contract Commencement Date or the Service Commencement Date (whichever is the earlier), notify the Authority in writing of the name, contact details and details of the legal representatives of any such sub-contractor (of any tier), to the extent that such information has not already been provided by the Service Provider to the Authority under the Contract;
  - 9.2.5 promptly notify the Authority in writing of any change to the information notified under Clause 9.2.4 and provide in writing the name, contact details and details of the legal representatives of each such sub-contractor (of any tier) who is

engaged after the Contract Commencement Date or the Service Commencement Date (whichever is the earlier);

9.2.6 without prejudice to the provisions of Clause 12, ensure compliance with the Bribery Act 2010 and any guidance issued by the Secretary of State under it when appointing any such sub-contractor;

9.2.7 include a term in each sub-contract (of any tier):

9.2.7.1 requiring payment to be made by the Service Provider or (in respect of a sub-contract below the first tier) the payer under the relevant sub-contract, to the sub-contractor within a specified period not exceeding 30 days from receipt of a valid and undisputed invoice as defined by the sub-contract requirements;

9.2.7.2 a requirement that any invoices for payment submitted by the sub-contractor are considered and verified by the Service Provider, or (in respect of a sub-contract below the first tier) the payer under the relevant sub-contract, in a timely manner and that any undue delay in doing so shall not in itself be sufficient justification for failing to treat an invoice as being valid and undisputed under the sub-contract requirements;

9.2.7.3 entitling the Service Provider or (in respect of a sub-contract below the first tier) the payer under the relevant sub-contract to terminate that sub-contract if the relevant sub-contractor fails to comply in the performance of its contract with legal obligations in the fields of environmental, social or labour law; and

9.2.7.4 a requirement that the sub-contractor includes a provision having the same effect as Clause 9.2.7.3 above in any sub-contract it awards.

9.3 The Service Provider shall give notice to the Authority within 10 Business Days where:

9.3.1 there is any change in the ownership of the Service Provider where such change relates to 50% or more of the issued share capital of the Service Provider; and

9.3.2 there is any change in the ownership of the Holding Company where such change relates to 50% or more of the issued share capital of the Holding Company; and

- 9.3.3 (in the case of an unincorporated Service Provider) give notice to the Authority if there is any change in the management personnel of the Service Provider, which alone or taken with any other change in management personnel not previously notified to the Authority, equates to a change in the identity of 50% or more of the management personnel of the Service Provider.

Upon the occurrence of any of the events referred to at Clauses 9.3.1 – 9.3.3 above, the Authority shall have the right to terminate the Contract.

## **10. Conflict of Interest**

- 10.1 The Service Provider warrants that it does not and will not have at the Contract Commencement Date or Service Commencement Date any interest in any matter where there is or is reasonably likely to be a conflict of interest with the Services or any member of the Authority Group, save to the extent fully disclosed to and approved by the Authority.
- 10.2 The Service Provider shall check for any conflict of interest at regular intervals throughout the Term and in any event not less than once in every six months and shall notify the Authority in writing immediately upon becoming aware of any actual or potential conflict of interest with the Services or any member of the Authority Group and shall work with the Authority to do whatever is necessary (including the separation of staff working on, and data relating to, the Services from the matter in question) to manage such conflict to the Authority's satisfaction, provided that, where the Authority is not so satisfied, it may terminate the Contract in accordance with Clause 27.1.4.

## **11. Access to Premises and Assets**

- 11.1 Subject to Clause 8.4 any access to either or both of any Authority Premises or Authority Assets made available to the Service Provider in connection with the proper performance of the Contract shall be free of charge and shall be used by the Service Provider solely for the purpose of performing the Services during the Term in accordance with the Contract provided, for the avoidance of doubt, the Service Provider shall be responsible for its own costs or travel including either or both of any congestion charging or low emission zone charging. The Service Provider shall:
- 11.1.1 have the use of such Authority Premises as licensee and shall not have or purport to claim any sole or exclusive right to possession or to possession of any particular part of such Authority Premises;

- 11.1.2 vacate such Authority Premises upon the termination or expiry of the Contract or at such earlier date as the Authority may determine;
  - 11.1.3 not exercise or purport to exercise any rights in respect of any Authority Premises in excess of those granted under this Clause 11.1;
  - 11.1.4 ensure that the Service Provider's Personnel carry any identity passes issued to them by the Authority at all relevant times and comply with the Authority's security procedures as may be notified by the Authority from time to time;
  - 11.1.5 not damage the Authority Premises or any assets on Authority Premises; and
  - 11.1.6 return immediately to the Authority in good working order and satisfactory condition (in the reasonable opinion of the Authority) all Authority Assets used by the Service Provider or the Service Provider's Personnel in the performance of the Services.
- 11.2 Nothing in this Clause 11 shall create or be deemed to create the relationship of landlord and tenant in respect of any Authority Premises between the Service Provider and any member of the Authority Group.
- 11.3 The Authority shall be under no obligation to provide office or other accommodation or facilities or services (including telephony and IT services) to the Service Provider except as may be specified in Schedule 1.

## **12. Compliance with Policies and Law**

- 12.1 The Service Provider, at no additional cost to the Authority:
- 12.1.1 undertakes to procure that all the Service Provider's Personnel comply with all of the Authority's policies and standards that are relevant to the performance of the Services, (including where the GLA is the Authority the Authority's Dignity at Work policy as updated from time to time and with the GLA's Code of Ethics as updated from time to time, and where TfL is the Authority, TfL's workplace harassment policy as updated from time to time (copies of which are available on request from TfL) and with TfL's Code of Conduct (which is available on TfL's website, [www.tfl.gov.uk](http://www.tfl.gov.uk))) including the provisions set out in Schedule 7 and those relating to safety, security, business ethics, drugs and alcohol and any other on site regulations specified by the Authority for personnel working at Authority Premises or accessing the Authority's computer systems. The Authority shall provide the Service Provider with copies of such policies and standards on request. In the event that the



Services are being provided to both the GLA and TfL, then the policies and standards of each of the GLA and TfL shall apply as appropriate;

- 12.1.2 shall provide the Services in compliance with and shall ensure that the Service Provider's Personnel comply with all requirements of all Acts of Parliament, statutory instruments, court orders, regulations, directives, European Community decisions (insofar as legally binding), bye-laws, treaties and other regulatory requirements relevant to either or both of the Service Provider's or the Authority's business, from time to time in force which are or may become applicable to the Services. The Service Provider shall promptly notify the Authority if the Service Provider is required to make any change to the Services for the purposes of complying with its obligations under this Clause 12.1.2;
- 12.1.3 without limiting the generality of Clause 12.1.2, shall comply with all relevant enactments in force from time to time relating to discrimination in employment and the promotion of equal opportunities;
- 12.1.4 acknowledges that the Authority is under a duty under section 149 of the Equality Act 2010 to have due regard to the need to eliminate unlawful discrimination on the grounds of sex, marital or civil partnership status, race, sexual orientation, religion or belief, age, pregnancy or maternity, gender reassignment or disability (a "**Relevant Protected Characteristic**") (as the case may be) and to promote equality of opportunity between persons who share a Relevant Protected Characteristic and persons who do not share it. In providing the Services, the Service Provider shall assist and cooperate with Authority where possible in satisfying this duty;
- 12.1.5 where possible, shall provide the Services in such a manner as to:
  - 12.1.5.1 promote equality of opportunity for all persons irrespective of their race, sex, disability, age, sexual orientation or religion;
  - 12.1.5.2 eliminate unlawful discrimination; and
  - 12.1.5.3 promote good relations between persons of different racial groups, religious beliefs and sexual orientation;
- 12.1.6 Where the GLA is the Authority the Service Provider shall:
  - 12.1.6.1 comply with policies developed by the Authority with regard to compliance with the Authority's duties

referred to in Clauses 12.1.4. - 12.1.5 as are relevant to the Contract and the Service Provider's activities;

- 12.1.6.2 obey directions from the Authority with regard to the conduct of the Contract in accordance with the duties referred to in Clauses 12.1.4. - 12.1.5;
  - 12.1.6.3 assist, and consult and liaise with, the Authority with regard to any assessment of the impact on and relevance to the Contract of the duties referred to in Clauses 12.1.4. - 12.1.5;
  - 12.1.6.4 on entering into any contract with a sub-contractor in relation to this Contract, impose obligations upon the sub-contractor to comply with this Clause 12.1.6 as if the sub-contractor were in the position of the Service Provider;
  - 12.1.6.5 provide to the Authority, upon request, such evidence as the Authority may require for the purposes of determining whether the Service Provider has complied with this Clause 12.1.6. In particular, the Service Provider shall provide any evidence requested within such timescale as the Authority may require, and cooperate fully with the Authority during the course of the Authority's investigation of the Service Provider's compliance with its duties under this Clause 12.1.6; and
  - 12.1.6.6 inform the Authority forthwith in writing should it become aware of any proceedings brought against it in connection with this Contract by any person for breach of the Equality Act 2010.
- 12.1.7 without prejudice to any other provision of this Clause 12.1 or the Schedules, where TfL is the Authority, comply with any provisions set out in the Schedules that relate to traffic management and shall comply with the reasonable instructions of TfL's Traffic Manager as may be made available to the Service Provider from time to time. For the purposes of this Clause 12.1.7, "**Traffic Manager**" means TfL's traffic manager appointed in accordance with section 17 of the Traffic Management Act 2004;
- 12.1.8 shall promptly notify the Service Provider's Personnel and the Authority of any health and safety hazards that exist or may arise in connection with the performance of the Services;

12.1.9 without limiting the generality of Clause 12.1.2, shall comply with the Bribery Act 2010 and any guidance issued by the Secretary of State under it; and

12.1.10 where applicable to the Service Provider and without limiting the generality of Clause 12.1.2, shall comply with the Modern Slavery Act 2015 and any guidance issued by the Secretary of State under it.

In all cases, the costs of compliance with this Clause 12.1 shall be borne by the Service Provider.

12.2 In providing the Services, the Service Provider shall (taking into account best available techniques not entailing excessive cost and the best practicable means of preventing, or counteracting the effects of any noise or vibration) have appropriate regard (insofar as the Service Provider's activities may impact on the environment) to the need to:

12.2.1 preserve and protect the environment and to the need to avoid, remedy and mitigate any adverse effects on the environment;

12.2.2 enhance the environment and have regard to the desirability of achieving sustainable development;

12.2.3 conserve and safeguard flora, fauna and geological or physiological features of special interest; and

12.2.4 sustain the potential of natural and physical resources and the need to safeguard the life-supporting capacity of air, water, soil and ecosystems.

### **Work Related Road Risk**

12.3 For the purposes of Clauses 12.3 to 12.12 (inclusive) of this Contract, the following expressions shall have the following meanings:

**“Alternative Scheme”** has the meaning given to it in Clause 12.4.1;

**“Approved Progressive Driver Training”** an ongoing programme of Drivers' training to ensure they have the appropriate knowledge, skills and attitude to operate safely on urban roads. This includes the training specific for the urban environment (including on-road experience from a cyclist's perspective), which is required to be completed at least once every 5 years;

**“Car-derived Van”** a vehicle based on a car, but with an interior that has been altered for the purpose of carrying larger amounts of goods and/or

	equipment;
<b>“Category N2 HGV”</b>	a vehicle designed and constructed for the carriage of goods having a MAM exceeding 3,500 kilograms but not exceeding 12,000 kilograms;
<b>“Category N3 HGV”</b>	a vehicle designed and constructed for the carriage of goods and having a MAM exceeding 12,000 kilograms;
<b>“CLOCS Standard”</b>	the Construction Logistics and Community Safety standard, which aims to eliminate risk of a collision between heavy goods vehicles servicing the construction sector and vulnerable road users by ensuring effective practice in the management of operations, vehicles, drivers and construction sites; further information can be found at: <a href="http://www.clocs.org.uk">www.clocs.org.uk</a> ;
<b>“Collision Report”</b>	a report detailing all collisions during the previous 12 months involving injuries to persons or fatalities;
<b>“Delivery and Servicing Vehicle”</b>	a HGV, a Van or a Car-derived Van;
<b>“Driver”</b>	any employee of the Service Provider (including an agency or contracted driver), who operates Delivery and Servicing Vehicles on behalf of the Service Provider while delivering the Services;
<b>“DVLA”</b>	Driver and Vehicle Licensing Agency;
<b>“Direct Vision Standard” or “DVS”</b>	Direct Vision Standard, a performance based assessment and rating tool, as updated from time to time that measures how much direct vision a Driver has from a Category N3 HGV cab in relation to other road users. Further information can be found at: <a href="http://www.tfl.gov.uk">www.tfl.gov.uk</a> ;
<b>“FORS”</b>	the Fleet Operator Recognition Scheme, which is an accreditation scheme for businesses operating commercial vehicles including vans, HGV, coaches and powered two wheelers. It offers impartial, independent advice and guidance to motivate companies to improve their

	compliance with relevant laws and their environmental, social and economic performance;
<b>“FORS Standard”</b>	the standard setting out the accreditation requirements for the Fleet Operator Recognition Scheme, a copy of which can be found at: <a href="http://www.fors-online.org.uk">www.fors-online.org.uk</a> ;
<b>“Gold Accreditation”</b>	the highest level of accreditation within the FORS Standard, the requirements of which are more particularly described at: <a href="http://www.fors-online.org.uk">www.fors-online.org.uk</a> ;
<b>“HGV”</b>	a vehicle with a MAM exceeding 3,500 kilograms;
<b>“MAM”</b>	the maximum authorised mass of a vehicle or trailer including the maximum load that can be carried safely while used on the road;
<b>“Silver Accreditation”</b>	the minimum level of accreditation within the FORS Standard acceptable for the contract schedule, the requirements of which are more particularly described at: <a href="http://www.fors-online.org.uk">www.fors-online.org.uk</a> ;
<b>“Van”</b>	a vehicle with a MAM not exceeding 3,500 kilograms; and
<b>“WRRR Self-Certification Report”</b>	has the meaning given to it in Clause 12.10.

#### **Fleet Operator Recognition Scheme Accreditation**

12.4 Where the Service Provider operates Delivery and Servicing Vehicles to provide the Services, it shall within 90 days of the Contract Commencement Date:

12.4.1 (unless already registered) register for FORS or a scheme, which in the reasonable opinion of the Authority, is an acceptable substitute to FORS (the “**Alternative Scheme**”); and

12.4.2 (unless already accredited) have attained the standard of Silver Accreditation (or higher) or the equivalent within the Alternative Scheme and shall maintain the standard of Silver Accreditation (or equivalent standard within the Alternative Scheme) by way of an annual independent audit in accordance with the FORS Standard or take such steps as may be

required to maintain the equivalent standard within the Alternative Scheme. Alternatively, where the Service Provider has attained Gold Accreditation, the maintenance requirements shall be undertaken in accordance with the periods set out in the FORS Standard.

### **Safety Features on HGVs**

- 12.5 The Service Provider shall ensure that every HGV, which it uses to provide the Services, shall be fitted with safety features consistent with the FORS Silver Accreditation.

### **Construction Logistics and Community Safety (CLOCS)**

- 12.6 Where applicable, for works contracts exceeding a value of £1m:
- 12.6.1 the Service Provider shall comply with the CLOCS Standard; and
  - 12.6.2 the Service Provider shall ensure that the conditions at all sites and locations where:
    - 12.6.2.1 the Services are being delivered; or
    - 12.6.2.2 in connection with the performance of the Services, any waste is being disposed of or supplies are being delivered to or from,
- are appropriate for each Category N3 HGV being used in the provision of the Services.

### **Direct Vision Standard (DVS)**

- 12.7 Where applicable, for contracts exceeding a value of £1m where the duration will exceed 12 months and a significant amount of the work will be conducted within the GLA boundaries:
- 12.7.1 the Service Provider shall comply with the DVS Schedule attached to this Contract; and
  - 12.7.2 the Service Provider shall ensure that:
    - 12.7.3 from and including 26 October 2019, all Category N3 HGVs used in the provision of the Services achieve a minimum of a one (1) star Direct Vision Standard rating; and
    - 12.7.4 from and including 26 October 2023, all Category N3 HGVs used in the provision of the Services achieve a minimum of three (3) star Direct Vision Standard rating.

### **Driver Training**

- 12.8 Where the Service Provider operates Delivery and Servicing Vehicles to provide the Services the Service Provider shall ensure that each of its Drivers attend the Approved Progressive Driver Training throughout the Term of the Contract.

### **Collision Reporting**

- 12.9 Where the Service Provider operates Delivery and Servicing Vehicles to deliver the Contract, the Service Provider shall within 15 days of the Contract Commencement Date, provide to the Authority a Collision Report. The Service Provider shall provide to the Authority an updated Collision Report within five Business Days of a written request from the Authority at any time.

### **Self-Certification of Compliance**

- 12.10 Where the Service Provider operates Delivery and Servicing Vehicles to provide the Services, within 90 days of the Contract Commencement Date, the Service Provider shall provide a written report to the Authority detailing its compliance with Clauses 12.4, 12.5, 12.6, 12.7, 12.8 and 12.9 (as applicable) of this Contract (the “**WRRR Self-Certification Report**”). The Service Provider shall provide updates of the WRRR Self-Certification Report to the Authority on each six month anniversary of its submission of the initial WRRR Self-Certification Report.

### **Obligations of the Service Provider Regarding Sub-contractors**

- 12.11 The Service Provider shall ensure that those of its sub-contractors who operate Category N2 HGVs, Category N3 HGVs, Vans and/or Car-derived Vans to provide the Services shall comply with the corresponding provisions of this Contract:

12.11.1 Clauses 12.4, 12.8, 12.9, 12.10; and

12.11.2 for Category N2 HGVs – Clause 12.5; and

12.11.3 for Category N3 HGVs – Clauses 12.5, and, where applicable 12.6, 12.7;

as if those sub-contractors were a party to this Contract.

### **Failure to Comply**

- 12.12 Without limiting the effect of any other clause of this Contract relating to termination, if the Service Provider fails to comply with Clauses 12.4, 12.5 (where applicable), 12.6 (where applicable), 12.7 (where applicable), 12.8, 12.9, 12.10 and 12.11;

12.12.1 the Service Provider has committed a material breach of this Contract; and

12.12.2 the Authority may refuse the Service Provider, its employees, agents and Delivery and Servicing Vehicles entry onto any property that is owned, occupied or managed by the Authority for any purpose (including but not limited to deliveries).

### 13. **London Living Wage**

For the purposes of this Clause 13, the following expressions have the corresponding meanings:

<b>“CCSL”</b>	the Centre for Civil Society Limited or any relevant replacement organisation as notified by the Authority from time to time;
<b>“London Living Wage”</b>	the London rate for the basic hourly wage as updated and published annually by the CCSL (or any relevant replacement organisation) on its website ( <a href="http://www.livingwage.org.uk">www.livingwage.org.uk</a> );
<b>“Subcontractor”</b>	a sub-contractor (of any tier) of the Service Provider.

13.1 The Service Provider acknowledges and agrees that the Mayor of London pursuant to section 155 of the Greater London Authority Act 1999 has directed that members of the Authority Group ensure that the London Living Wage be paid to anyone engaged by any member of the Authority Group who is required to discharge contractual obligations (whether as a direct contractor or a sub-contractor (of any tier) of that direct contractor) on the Authority’s estate in the circumstances set out in Clause 13.3.1.

13.2 Without prejudice to any other provision of this Contract, the Service Provider shall:

13.2.1 ensure that its employees and procure that the employees of its Sub-contractors engaged in the provision of the Services:

13.2.1.1 for two (2) or more hours of work in any given day in a week, for eight (8) or more consecutive weeks in a year; and

13.2.1.2 on the Authority’s estate including (without limitation) premises and land owned or occupied by the Authority,

be paid an hourly wage (or equivalent of an hourly wage) equivalent to or greater than the London Living Wage;



13.2.2 ensure that none of:

13.2.2.1 its employees; nor

13.2.2.2 the employees of its Sub-contractors,

engaged in the provision of the Services be paid less than the amount to which they are entitled in their respective contracts of employment;

13.2.3 provide to the Authority such information concerning the London Living Wage as the Authority or its nominees may reasonably require from time to time, including (without limitation):

13.2.3.1 all information necessary for the Authority to confirm that the Service Provider is complying with its obligations under Clause 13; and

13.2.3.2 reasonable evidence that Clause 13 has been implemented;

13.2.4 disseminate on behalf of the Authority to:

13.2.4.1 its employees; and

13.2.4.2 the employees of its Sub-contractors,

engaged in the provision of the Services such perception questionnaires as the Authority may reasonably require from time to time and promptly collate and return to the Authority responses to such questionnaires; and

13.2.5 cooperate and provide all reasonable assistance in monitoring the effect of the London Living Wage including (without limitation):

13.2.5.1 allowing the CCSL to contact and meet with the Service Provider's employees and any trade unions representing the Service Provider's employees;

13.2.5.2 procuring that the Service Provider's Sub-contractors allow the CCSL to contact and meet with the Subcontractors' employees and any trade unions representing the Sub-contractors' employees,

in order to establish that the obligations in Clause 13.3.1 have been complied with.

13.3 For the avoidance of doubt the Service Provider shall:

13.3.1 implement the annual increase in the rate of the London Living Wage; and

13.3.2 procure that its Sub-contractors implement the annual increase in the rate of the London Living Wage,

on or before 1 April in the year following the publication of the increased rate of the London Living Wage.

13.4 The Authority reserves the right to audit (acting by itself or its nominee(s)) the provision of the London Living Wage to the Service Provider's staff and the staff of its Sub-contractors.

13.5 Without limiting the Authority's rights under any other termination provision in this Contract, the Service Provider shall remedy any breach of the provisions of this Clause 13 within four (4) weeks' notice of the same from the Authority (the "**Notice Period**"). If the Service Provider remains in breach of the provisions of this Clause 13 following the Notice Period, the Authority may by written notice to the Service Provider immediately terminate this Contract.

#### 14. **Corrupt Gifts and Payment of Commission**

The Service Provider shall not, and shall ensure that its employees, agents and sub-contractors do not, pay any commission, fees or grant any rebates to any employee, officer or agent of any member of the Authority Group nor favour any employee, officer or agent of any member of the Authority Group with gifts or entertainment of significant cost or value nor enter into any business arrangement with employees, officers or agents of any member of the Authority Group other than as a representative of the Authority, without the Authority's prior written approval.

#### 15. **Equipment**

15.1 Risk in:

15.1.1 all Service Provider Equipment shall be with the Service Provider at all times; and

15.1.2 all other equipment and materials forming part of the Services (title to which will pass to the Authority) ("**Materials**") shall be with the Service Provider at all times until completion of the Services in accordance with the Contract,

regardless of whether or not the Service Provider Equipment and Materials are located at Authority Premises.

15.2 The Service Provider shall ensure that all Service Provider Equipment and all Materials meet all minimum safety standards required from time to time by law.

16. **Quality and Best Value**

- 16.1 The Service Provider acknowledges that the Authority is a best value authority for the purposes of the Local Government Act 1999 and as such the Authority is required to make arrangements to secure continuous improvement in the way it exercises its functions (having regard to a combination of economy, efficiency and effectiveness) and, as such, the Service Provider shall, where reasonably requested by the Authority, participate in any relevant best value review.
- 16.2 Where the GLA is the Authority then in accordance with the statutory requirement set out in section 61(3) of the Greater London Authority Act 1999, the Service Provider shall send such representatives as may be requested to attend the Greater London Assembly for questioning in relation to the Contract. The Service Provider acknowledges that it may be liable to a fine or imprisonment if it fails to comply with a summons to attend.

17. **Records, Audit and Inspection**

- 17.1 The Service Provider shall, and shall procure that its sub-contractors shall:
- 17.1.1 maintain a complete and correct set of records pertaining to all activities relating to the performance of the Services and the Service Provider's obligations under the Contract and all transactions entered into by the Service Provider for the purposes of the Contract (including time-sheets for the Service Provider's Personnel where such records are material to the calculation of the Charges) ("**Records**"); and
  - 17.1.2 retain all Records during the Term and for a period of not less than 6 years (or such longer period as may be required by law), except Records containing Personal Data (as defined in Data Protection Legislation) which shall only be retained for as long as necessary, following termination or expiry of the Contract ("**Retention Period**").
- 17.2 The Authority and any person nominated by the Authority has the right to audit any and all Records at any time during the Retention Period on giving to the Service Provider what the Authority considers to be reasonable notice (whether in writing or verbally) and at any reasonable time to inspect any aspect of the Service Provider's performance of the Services (including compliance with Clause 12.1) and the Service Provider shall give all reasonable assistance to the Authority or its nominee in conducting such inspection, including making available documents and staff for interview.

18. **Set-Off**

All damages, costs, charges, expenses, debts, sums or other amounts owing (contingently or otherwise) to or incurred by the Authority arising out of or attributable to this Contract or any other contract between the Authority and the Service Provider may be deducted by the Authority from monies due or which may become due to the Service Provider under this Contract or under any other contract with any member of the Authority Group may recover such amount as a debt.

19. **Indemnity**

19.1 Subject to Clause 19.2, the Service Provider is responsible for and shall indemnify, keep indemnified and hold harmless each of the Authority and all other members of the Authority Group (including their respective employees, sub-contractors and agents) ("**the Indemnified Party**") against all Losses which the Indemnified Party incurs or suffers as a consequence of any breach or negligent performance of the Contract by the Service Provider (or any of the Service Provider's Personnel) (including in each case any non-performance or delay in performance of the Contract) or of any breach of statutory duty, misrepresentation or misstatement by the Service Provider (or any of its employees, agents or sub-contractors).

19.2 The Service Provider is not responsible for and shall not indemnify the Authority for any Losses to the extent that such Losses are caused by any breach or negligent performance of any of its obligations under the Contract by the Authority or any other member of the Authority Group including by any of their respective employees, agents or sub-contractors.

20. **Insurance**

20.1 The Service Provider will at its sole cost maintain employer's liability and motor insurance cover as required by law and insurance cover in the sum of not less than £5 million per claim (in terms approved by the Authority) in respect of the following to cover the Services (the "**Insurances**") and will ensure that the Authority's interest is noted on each and every policy or that any public liability, product liability or employer's liability insurance includes an Indemnity to Principal clause:

20.1.1 public liability to cover injury and loss to third parties;

20.1.2 insurance to cover the loss or damage to any item related to the Services;

20.1.3 product liability; and

20.1.4 professional indemnity or, where professional indemnity insurance is not available, a "financial loss" extension to the public liability insurance referred to in Clause 20.1.1 or, if

applicable, the product liability insurance referred to in Clause 20.1.3. Any professional indemnity insurance or “financial loss” extension shall be renewed for a period of 6 years (or such other period as the Authority may stipulate) following the expiry or termination of the Contract.

- 20.2 The insurance cover will be maintained with a reputable insurer.
- 20.3 The Service Provider will produce evidence to the Authority on reasonable request of the insurance policies set out in Clause 20.1 and payment of all premiums due on each policy.
- 20.4 The Service Provider warrants that nothing has or will be done or be omitted to be done which may result in any of the insurance policies set out in Clause 20.1 being or becoming void, voidable or unenforceable.
- 20.5 In the event that any of the Insurances are cancelled or not renewed, the Service Provider shall immediately notify the Authority and shall at its own cost arrange alternative Insurances with an insurer or insurers acceptable to the Authority.

21. **The Authority’s Data**

[not used – see Schedule 2]

22. **Intellectual Property Rights**

[not used – see Schedule 2]

23. **Privacy, Data Protection and Cyber Security**

[not used – see Schedule 2]

24. **Confidentiality and Announcements**

- 24.1 Subject to Clause 25, the Service Provider will keep confidential:

24.1.1 the terms of this Contract; and

24.1.2 any and all Confidential Information that it may acquire in relation to the Authority.

- 24.2 The Service Provider will not use the Authority’s Confidential Information for any purpose other than to perform its obligations under this Contract. The Service Provider will ensure that its officers and employees comply with the provisions of Clause 24.1.

- 24.3 The obligations on the Service Provider set out in Clause 24.1 will not apply to any Confidential Information:

- 24.3.1 which either of the Parties can demonstrate is in the public domain (other than as a result of a breach of this Clause 24);
  - 24.3.2 which a Party is required to disclose by order of a court of competent jurisdiction but then only to the extent of such required disclosure; or
  - 24.3.3 to the extent that such disclosure is to the Secretary for Transport (or the government department responsible for public transport in London for the time being) the Office of Rail Regulation, or any person or body who has statutory responsibilities in relation to transport in London and their employees, agents and sub-contractors.
- 24.4 The Service Provider shall keep secure all materials containing any information in relation to the Contract and its performance.
- 24.5 The Service Provider shall not communicate with representatives of the general or technical press, radio, television or other communications media in relation to the existence of the Contract or that it is providing the Services to the Authority or in relation to any matter under or arising from the Contract unless specifically granted permission to do so in writing by the Authority. The Authority shall have the right to approve any announcement before it is made.
- 24.6 The provisions of this Clause 24 will survive any termination of this Contract for a period of 6 years from termination.
25. **Freedom of Information and Transparency**
- 25.1 For the purposes of this Clause 25:
- 25.1.1 **“FOI Legislation”** means the Freedom of Information Act 2000, all regulations made under it and the Environmental Information Regulations 2004 and any amendment or re-enactment of any of them and any guidance or statutory codes of practice issued by the Information Commissioner, the Ministry of Justice or the Department for Environment Food and Rural Affairs (including in each case its successors or assigns) in relation to such legislation;
  - 25.1.2 **“Information”** means information recorded in any form held by the Authority or by the Service Provider on behalf of the Authority; and
  - 25.1.3 **“Information Access Request”** means a request for any Information under the FOI Legislation.
- 25.2 The Service Provider acknowledges that the Authority:

- 25.2.1 is subject to the FOI Legislation and agrees to assist and cooperate with the Authority to enable the Authority to comply with its obligations under the FOI Legislation; and
  - 25.2.2 may be obliged under the FOI Legislation to disclose Information without consulting or obtaining consent from the Service Provider.
- 25.3 Without prejudice to the generality of Clause 25.2, the Service Provider shall and shall procure that its sub-contractors (if any) shall:
  - 25.3.1 transfer to the Contract Manager (or such other person as may be notified by the Authority to the Service Provider) each Information Access Request relevant to the Contract, the Services or any member of the Authority Group that it or they (as the case may be) receive as soon as practicable and in any event within two (2) Business Days of receiving such Information Access Request; and
  - 25.3.2 in relation to Information held by the Service Provider on behalf of the Authority, provide the Authority with details about and copies of all such Information that the Authority requests and such details and copies shall be provided within five (5) Business Days of a request from the Authority (or such other period as the Authority may reasonably specify), and in such forms as the Authority may reasonably specify.
- 25.4 The Authority shall be responsible for determining whether Information is exempt from disclosure under the FOI Legislation and for determining what Information will be disclosed in response to an Information Access Request in accordance with the FOI Legislation.
- 25.5 The Service Provider shall not itself respond to any person making an Information Access Request, save to acknowledge receipt, unless expressly authorised to do so by the Authority.
- 25.6 The Service Provider acknowledges that the Authority is subject to the Transparency Commitment. Accordingly, notwithstanding Clause 24.1 and Clause 25, the Service Provider hereby gives its consent for the Authority to publish the Contract Information to the general public.
- 25.7 The Authority may in its absolute discretion redact all or part of the Contract Information prior to its publication. In so doing and in its absolute discretion the Authority may take account of the exemptions/exceptions that would be available in relation to information requested under the FOI Legislation.
- 25.8 The Authority may in its absolute discretion consult with the Service Provider regarding any redactions to the Contract Information to be published pursuant to Clause 25.6. The Authority shall make the final

decision regarding both publication and redaction of the Contract Information.

**26. Dispute Resolution**

- 26.1 The Authority and the Service Provider shall use all reasonable endeavours to negotiate in good faith and settle any dispute or difference that may arise out of or relate to the Contract ("**Dispute**") before resorting to litigation.
- 26.2 If the Dispute is not settled through discussion between the Contract Manager and a representative of the Service Provider within a period of seven (7) Business Days of the date on which the Dispute arose, the Parties may refer the Dispute in writing to a director or chief executive (or equivalent) ("**Senior Personnel**") of each of the Parties for resolution.
- 26.3 If the Dispute is not resolved within 14 Business Days of referral to the Senior Personnel, the Parties shall attempt in good faith to resolve the Dispute through entry into a structured mediation or negotiation with the assistance of a mediator. Either Party may give notice to the other Party ("**Notice**") to commence such process and the Notice shall identify one or more proposed mediators.
- 26.4 If the Parties are unable to agree on a mediator, or if the agreed mediator is unable or unwilling to act within 28 Business Days of the service of the Notice, either Party may apply to the Centre for Effective Dispute Resolution ("**CEDR**") in London to appoint a mediator. The costs of that mediator shall be divided equally between the Parties or as the Parties may otherwise agree in writing.
- 26.5 Where a dispute is referred to mediation under Clause 26.3, the Parties will attempt to settle such Dispute by mediation in accordance with the model mediation procedures published by CEDR or such other procedures as the mediator may recommend.
- 26.6 If the Parties reach agreement on the resolution of the Dispute, such agreement shall be recorded in writing and once signed by the Parties' authorised representatives, shall be final and binding on the Parties.
- 26.7 If either Party refuses at any time to participate in the mediation procedure and in any event if the Parties fail to reach agreement on the Dispute within 40 Business Days of the service of the Notice either Party may commence proceedings in accordance with Clause 41.
- 26.8 For the avoidance of doubt, the Service Provider shall continue to provide the Services in accordance with the Contract and without delay or disruption while the Dispute is being resolved pursuant to this Clause 26.



- 26.9 Neither Party shall be prevented from, or delayed in, seeking any order for specific performance or for interim or final injunctive relief as a result of the provisions of this Clause 26 and Clause 26 shall not apply in respect of any circumstances where such remedies are sought.

**27. Breach and Termination of Contract**

- 27.1 Without prejudice to the Authority's right to terminate at common law, the Authority may terminate the Contract immediately upon giving notice to the Service Provider if:

27.1.1 In addition and without prejudice to Clauses 27.1.2 to 27.1.6 (inclusive), the Service Provider has committed any material or persistent breach of the Contract and in the case of such a breach that is capable of remedy fails to remedy that breach within 10 Business Days (or such other timeframe as specified in writing by the Authority) from the date of written notice to the Service Provider giving details of the breach and requiring it to be remedied;

27.1.2 the Service Provider is subject to an Insolvency Event;

27.1.3 in the event that there is a change of ownership referred to in Clause 9.3 or the Service Provider is in breach of Clause 9.3;

27.1.4 the Authority is not satisfied on the issue of any conflict of interest in accordance with Clause 10;

27.1.5 the Service Provider or any of its officers, employees or agents commits any act of bribery described in the Bribery Act 2010; or

27.1.6 the Service Provider commits any of the money laundering related offences listed in the Public Contracts Regulations 2015; or

27.1.7 the Service Provider fails to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law.

- 27.2 Without prejudice to any of the Authority's other rights, powers or remedies (whether under the Contract or otherwise) if the Service Provider is in breach of any of its warranties, or obligations either under Clause 6 or any other provision of this Contract, the Service Provider shall, if required to do so by the Authority, promptly remedy and/or re-perform the Services or part of them at its own expense to ensure compliance with such warranties and obligations. Nothing in this Clause 27.2 shall prevent the Authority from procuring the provision of any Services or any remedial action in respect of any Services from an alternative contractor and, where the Authority so procures any Services or any remedial action, the Authority shall be

entitled to recover from the Service Provider all additional cost, loss and expense incurred by the Authority and attributable to the Authority procuring such Services or remedial action from such alternative contractor.

- 27.3 Neither Party shall be deemed to be in breach of the Contract, or otherwise liable to the other Party in any manner whatsoever, for any failure or delay in performing its obligations under the Contract to the extent that such failure or delay is due to a Force Majeure Event. If a Force Majeure Event has continued for more than 8 weeks from the date on which that Force Majeure Event first arose and is having a material adverse effect on either Party's performance of its obligations under the Contract ("**the Affected Party**"), then for as long as such Force Majeure Event continues and has that effect, the Party not affected by such Force Majeure Event ("**Innocent Party**") may terminate the Contract immediately upon giving notice to the Affected Party. If the Contract is terminated in accordance with this Clause 27.3 then without prejudice to any rights and liabilities which accrued prior to termination the Affected Party shall not be liable to the Innocent Party by reason of such termination.
- 27.4 Without prejudice to the Authority's right to terminate the Contract under Clause 27.1 or to terminate at common law, the Authority may terminate the Contract at any time without cause subject to giving the Service Provider written notice of the period specified in Schedule 1, provided that this Clause 27.4 may be disapplied by notice to that effect in Schedule 1.
- 27.5 Without prejudice to the Authority's right to terminate the Contract under Clauses 27.1, 27.4 or at common law, the Authority may terminate the Contract at any time following a Declaration of Ineffectiveness in accordance with the provisions of Clause 29.
- 27.6 To the extent that the Authority has a right to terminate the Contract under this Clause 27 then, as an alternative to termination, the Authority may by giving notice to the Service Provider require the Service Provider to provide part only of the Services with effect from the date specified in the Authority's notice ("**Change Date**") whereupon the provision of the remainder of the Services will cease and the definition of "the Services" shall be construed accordingly. The Charges applicable with effect from the Change Date will be adjusted proportionately or if in the Authority's opinion a proportionate adjustment would not be reasonable in such manner as the Authority may determine.
28. **Consequences of Termination or Expiry**
- 28.1 Notwithstanding the provisions of Clause 24, wherever the Authority chooses to put out to tender for a replacement service provider some or all of the Services, the Service Provider shall disclose to tenderers such information concerning the Services as the Authority may require

for the purposes of such tender and shall also comply with all requirements as are set out at Schedule 8. The Service Provider may impose upon any recipient of such information such obligations of confidentiality as it may require.

28.2 The termination or expiry of the Contract shall not prejudice or affect any right, power or remedy which has accrued or shall accrue to either Party prior to or after such termination or expiry.

28.3 Upon expiry or termination of the Contract (howsoever caused):

28.3.1 the Service Provider shall, at no further cost to the Authority:

28.3.1.1 take all such steps as shall be necessary to agree with the Authority a plan for the orderly handover of Services to the Authority (or its nominee), such that the Services can be carried on with the minimum of interruption and inconvenience to the Authority and to effect such handover; and

28.3.1.2 on receipt of the Authority's written instructions to do so (but not otherwise), arrange to remove all electronically held information by a mutually agreed date, including the purging of all disk-based information and the reformatting of all disks.

28.3.2 the Authority shall (subject to Clauses 18, 28.1 and 28.4 and the provisions of any security for due performance supplied by the Service Provider) pay the Service Provider any Charges remaining due in relation to any Services properly performed in accordance with the Contract up to the date of termination or expiry calculated so far as is possible in accordance with Schedule 4 or otherwise reasonably determined by the Authority.

28.4 On termination of all or any part of the Contract, the Authority may enter into any agreement with any third party or parties as the Authority thinks fit to provide any or all of the Services and (save where terminated under Clause 27.4) the Service Provider shall be liable for all additional expenditure reasonably incurred by the Authority in having such services carried out and all other costs and damages reasonably incurred by the Authority in consequence of such termination. The Authority may deduct such costs from the Charges or otherwise recover such costs from the Service Provider as a debt.

## **29. Declaration of Ineffectiveness and Public Procurement Termination Event**

29.1 In the event that a court makes a Declaration of Ineffectiveness, the Authority shall promptly notify the Service Provider. The Parties agree that the provisions of Clause 28 and Clauses 29.1, 29.2, 29.4 to 29.6

(inclusive) and 29.12 shall apply as from the time when the Declaration of Ineffectiveness is made.

- 29.2 The Declaration of Ineffectiveness shall not prejudice or affect any right, liability or remedy which has accrued or shall accrue to either Party prior to or after such Declaration of Ineffectiveness in respect of the period prior to the Declaration of Ineffectiveness, save as otherwise expressly provided to the contrary in Clauses 29.1 to 29.6 inclusive.
- 29.3 During any court proceedings seeking a Declaration of Ineffectiveness, the Authority may require the Service Provider to prepare a Cessation Plan in accordance with this Clause 29.3 by issuing a notice in writing. As from the date of receipt by the Service Provider of such notification from the Authority, the Parties (acting reasonably and in good faith) shall agree or, in the absence of such agreement, the Authority shall reasonably determine an appropriate Cessation Plan with the object of achieving:
- 29.3.1 an orderly and efficient cessation of the Services or (at the Authority's request) a transition of the Services to the Authority or such other entity as the Authority may specify; and
  - 29.3.2 minimal disruption or inconvenience to the Authority or to customers of the Services or to public passenger transport services or facilities,
- in accordance with the provisions of Clauses 29.2 to 29.6 (inclusive) and which the Parties agree would have effect in the event that a Declaration of Ineffectiveness is made.
- 29.4 Where there is any conflict or discrepancy between the provisions of Clause 28 and Clauses 29.2 to 29.6 (inclusive) and 29.12 or the Cessation Plan, the provisions of these Clauses 29.2 to 29.6 (inclusive) and 29.12 and the Cessation Plan shall prevail.
- 29.5 The Parties will comply with their respective obligations under the Cessation Plan (as agreed by the Parties or, where agreement cannot be reached, as reasonably determined by the Authority) in the event that a Declaration of Ineffectiveness is made.
- 29.6 The Authority shall pay the Services Provider's reasonable costs in assisting the Authority in preparing, agreeing and complying with the Cessation Plan. Such costs shall be based on any comparable costs or Charges agreed as part of this Contract or as otherwise reasonably determined by the Authority. Provided that the Authority shall not be liable to the Service Provider for any loss of profit, revenue, goodwill or loss of opportunity as a result of the early termination of this Contract pursuant to any Declaration of Ineffectiveness.

- 29.7 Without prejudice to the Authority's rights of termination implied into the Contract by Regulation 73(3) of the Public Contracts Regulations 2015 or Regulation 89(3) of the Utilities Contracts Regulations 2016, in the event that the Authority exercises its right to terminate pursuant to this Clause 29.7 (a "**Public Procurement Termination Event**"), the Authority shall promptly notify the Service Provider and the Parties agree that:
- 29.7.1 the provisions of Clause 28 and these Clauses 29.7 to 29.12 (inclusive) shall apply as from the date of receipt by the Service Provider of the notification of the Public Procurement Termination Event; and
- 29.7.2 if there is any conflict or discrepancy between the provisions of Clause 28 and these Clauses 29.7 to 29.12 or the Cessation Plan, the provisions of these Clauses 29.7 to 29.12 and the Cessation Plan shall prevail.
- 29.8 Termination on the Public Procurement Termination Grounds shall not prejudice or affect any right, liability or remedy which has accrued or shall accrue to either Party prior to or after such termination on Public Procurement Termination Grounds, in respect of the period prior to such termination, save as otherwise expressly provided in Clauses 29.7 to 29.11 inclusive.
- 29.9 As from the date of receipt by the Service Provider of the notification of the termination on Public Procurement Termination Grounds, the Parties (acting reasonably and in good faith) shall agree or, in the absence of such agreement, the Authority shall reasonably determine an appropriate Cessation Plan with the object of achieving:
- 29.9.1 an orderly and efficient cessation or (at the Authority's election) a transition to the Authority or such other entity as the Authority may specify of: (i) the Services; or (at Authority's election), (ii) the part of the Services which are affected by the Public Procurement Termination Grounds; and
- 29.9.2 minimal disruption or inconvenience to the Authority or to customers of the Services or to public passenger transport services or facilities,
- in accordance with the provisions of these Clauses 29.7 to 29.11 (inclusive) and to take account of the circumstances of the Public Procurement Termination Grounds.
- 29.10 Upon agreement, or determination by the Authority, of the Cessation Plan the Parties will comply with their respective obligations under the Cessation Plan.
- 29.11 The Authority shall pay the Service Provider's reasonable costs in assisting the Authority in preparing, agreeing and complying with the

Cessation Plan. Such costs shall be based on any comparable costs or Charges agreed as part of this Contract or as otherwise reasonably determined by the Authority, provided that the Authority shall not be liable to the Service Provider for any loss of profit, revenue, goodwill or loss of opportunity as a result of the early termination of this Contract as a result of Public Procurement Termination Grounds.

- 29.12 For the avoidance of doubt, the provisions of this Clause 29 (and applicable definitions) shall survive any termination of the Contract following a Declaration of Ineffectiveness or termination on Public Procurement Termination Grounds.

30. **Survival**

The provisions of Clauses 1, 3.1.3, 4, 5, 6.1.4, 8.1, 9.2.2, 9.2.3, 11.1.1, 11.1.2, 11.1.5, 11.2, 15, 17-21 (inclusive), 22.2, 23-26 (inclusive), 28, 29-32 (inclusive), 34-41 (inclusive) and any other Clauses or Schedules that are necessary to give effect to those Clauses shall survive termination or expiry of the Contract. In addition, any other provision of the Contract which by its nature or implication is required to survive the termination or expiry of the Contract shall do so.

31. **Rights of Third Parties**

- 31.1 Save that any member of the Authority Group has the right to enforce the terms of the Contract in accordance with the Contracts (Rights of Third Parties) Act 1999 ("**Third Party Act**"), the Parties do not intend that any of the terms of the Contract will be enforceable by virtue of the Third Party Act by any person not a party to it.
- 31.2 Notwithstanding Clause 31.1, the Parties are entitled to vary or rescind the Contract without the consent of any other person including any member of the Authority Group.

32. **Contract Variation**

Save where the Authority may require an amendment to the Services and/or this Contract is amended pursuant to the Service Provider's exercise of any Supply Chain Finance Option, the Contract may only be varied or amended with the written agreement of both Parties. Save for any variations or amendments to reflect the Service Provider's exercise of any Supply Chain Finance Option (the mechanism for which is set out at Part B of Schedule 6) the details of any variations or amendments shall be set out in such form as the Authority may dictate and which may be substantially in the form set out in Part A of Schedule 6 and shall not be binding upon the Parties unless completed in accordance with such form of variation.

33. **Novation**

33.1 The Authority may novate or otherwise transfer the Contract (in whole or in part).

33.2 Within 10 Business Days of a written request from the Authority, the Service Provider shall at its expense execute such agreement as the Authority may reasonably require to give effect to any such transfer all or part of its rights and obligations under the Contract to one or more persons nominated by the Authority.

33.3 Subject to Clause 9, the Contract is personal to the Service Provider who shall not assign the benefit or delegate the burden of the Contract or otherwise transfer any right or obligation under the Contract without the prior written consent of the Authority.

34. **Non-Waiver of Rights**

No waiver of any of the provisions of the Contract is effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with the provisions of Clause 36. The single or partial exercise of any right, power or remedy under the Contract shall not in any circumstances preclude any other or further exercise of it or the exercise of any other such right, power or remedy.

35. **Illegality and Severability**

If any provision of the Contract (in whole or in part) is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed from the Contract and the remaining provisions shall continue in full force and effect as if the Contract had been executed without the invalid, illegal, or unenforceable provision. In the event that in the Authority's reasonable opinion such a provision is so fundamental as to prevent the accomplishment of the purpose of the Contract, the Authority and the Service Provider shall immediately commence good faith negotiations to remedy such invalidity.

36. **Notices**

Any notice, demand or communication in connection with this Contract will be in writing and may be delivered by hand, prepaid recorded delivery first class post or by email addressed as follows:

If to TFL:

[REDACTED]

[REDACTED] at [REDACTED] [REDACTED]

If to Service Provider:

██████████ at ██████████ and

██████████ at ██████████

The notice, demand or communication will be deemed to have been duly served:

if delivered by hand, at the time of delivery;

if delivered by post, two (2) Business Days after being posted or in the case of Airmail 14 Business Days after being posted; or

if delivered by email, the next business day after the day when the email was sent.

### 37. **Entire Agreement**

#### 37.1 Subject to Clause 37.2:

37.1.1 the Contract and all documents referred to in the Contract, contains all of the terms which the Parties have agreed relating to the subject matter of the Contract and such documents and supersedes and extinguishes any prior drafts, agreements, undertakings, representations, warranties and arrangements of any nature whatsoever, whether or not in writing relating to the provision of the Services. Neither Party has been induced to enter into the Contract by a statement which the Contract does not contain; and

37.1.2 without prejudice to the Service Provider's obligations under the Contract, the Service Provider is responsible for and shall make no claim against the Authority in respect of any misunderstanding affecting the basis of the Service Provider's tender in respect of the Contract or any incorrect or incomplete information howsoever obtained.

37.2 Nothing in this Clause 37 excludes any liability which one Party would otherwise have in respect of any statement it has made fraudulently to the other Party.

### 38. **Counterparts**

This Contract may be executed in any number of counterparts or duplicates, each of which shall be an original, and such counterparts or duplicates shall together constitute one and the same agreement.

### 39. **Relationship of the Parties**

Nothing in the Contract constitutes, or shall be deemed to constitute, a partnership between the Parties. Except as expressly provided in the Contract, neither Party shall be deemed to be the agent of the other, nor shall either Party hold itself out as the agent of the other.



40. **Further Assurance**

Each Party will do or procure the doing of all acts and things and execute or procure the execution of all such documents as the other Party reasonably considers necessary to give full effect to the provisions of the Contract.

41. **Governing Law**

The Contract shall be governed by and construed in accordance with the law of England and Wales. Without prejudice to Clause 26, the courts of England will have exclusive jurisdiction to settle any dispute which may arise out of or in connection with the Contract provided that the Authority has the right in its absolute discretion to enforce a judgment and take proceedings in any other jurisdiction in which the Service Provider is incorporated or in which any assets of the Service Provider may be situated. The Parties agree irrevocably to submit to that jurisdiction.

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

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]

## SCHEDULE 1 - KEY CONTRACT INFORMATION

1. **Contract Reference Number:** tfl\_scp\_002004
2. **Name of Service Provider:** Bluecarsharing, SAS
3. **Commencement:**
  - (a) **Contract Commencement Date:** December 14, 2020
  - (b) **Service Commencement Date:** December 15<sup>th</sup>, 2020
4. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
5. **Payment (see Clauses 5.1 and 5.4):**  
[REDACTED]  
receiving an invoice;  
  
[REDACTED] front within 30 days after receiving an invoice;  
  
[REDACTED] subject to the number of total vehicles connected to the Platform (license fee and platform hosting).  
  
Please refer to Schedule 4 "Charges" for the full pricing schedule.  
  
[insert alternative (shorter\*) period]  
Where no alternative is listed, payment must be made within 30 days of receipt of invoices.  
  
**\* the period cannot exceed 30 days**
6. **The preferred method – E-invoicing (EDI):**  
Transport for London  
<https://tfl.gov.uk/corporate/publications-and-reports/procurement-information>

### Accounts Payable:

TfL will accept invoices by email but they must be in PDF format. Each invoice must be a separate PDF and with a unique file reference

[invoices@tfl.gov.uk](mailto:invoices@tfl.gov.uk)

# Transport for London

To avoid a delay in payment, it's important for your invoice to be legally compliant. The following checklist will help to avoid payment delays.

Contact FSC for all Accounts Payable-related queries on: 0343 222 5100, or email: [accountspayable@tfl.gov.uk](mailto:accountspayable@tfl.gov.uk).

## 7. Time for payment where not 30 days (see Clause 5.4):

## 8. Details of the Authority's Contract Manager

Name: [REDACTED]

Address: 11th Floor, Palestra, 197 Blackfriars Road, London SE1 8NJ

Tel : 07725 [REDACTED]

[REDACTED] [REDACTED]

## 9. Details of the Authority's Procurement Manager

Name: [REDACTED]

[REDACTED] SE1 8NJ

Tel : [REDACTED]

Email: [REDACTED]

[REDACTED]

## 10. Service Provider's Key Personnel:

Name & Position	Contact Details	Area of Responsibility
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]	Overall success of the project and delivery and maintenance of the platform in London
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]	Communication with TFL on a frequent basis regarding needs, requests and user experience and satisfaction,

## Transport for London

		<div></div> <div></div>
<div></div> <div></div>	<div></div> <div></div> <div></div>	<div></div> <div></div>

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

\_\_\_\_\_

[REDACTED]

[REDACTED]

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

- 13. Office facilities to be provided to the Service Provider in accordance with Clause 11.3:** *[Need to be clear about any telephony, IT etc.]*

Not applicable

- 14. Training to be provided by the Service Provider in accordance with Clause 8.8:**

During the launch phase, a comprehensive training schedule will be set up for all users of the Platform. Training sessions and demos will take place over a video call as opposed to in-person meetings. A demo of each new functionality, use case or feature will be conducted as these new developments are released. All users will also receive a detailed user guide and online tutorial videos. These training materials will be kept up to date and will remain accessible throughout the project for any new user.

## SCHEDULE 2 - SPECIAL CONDITIONS OF CONTRACT

### Definitions

The following definitions are used in this Schedule:

<b>“Authority Data”</b>	Means Micromobility Operators’ data, including trip data, provided to the Service Provider by each Micromobility Operator on behalf of the Authority via an Operator’s application programming interface (API) pursuant to the Authority regulations, boroughs’ regulations and other applicable regulations, to enable the Service Provider to deliver the Services to the Authority.
<b>“Hardware”</b>	means items of hardware or equipment to be supplied, recommended and installed by the Service Provider under this Contract as specified in <b>Error! Reference source not found.</b> 3 (Specification), if any, which may include computer equipment, telecommunications equipment or other equipment;
<b>“Software”</b>	means Service Provider Software and the Third Party Software;
<b>“System”</b>	means Hardware and the Software;
<b>“Third Party”</b>	means any person, partnership, company or any other undertaking not being the Service Provider or a Authority Group Member and <b>“Third Parties”</b> shall be construed accordingly;
<b>“Third Party Software”</b>	means Third Party software to be provided to the Authority under this Contract which is specified as Third Party Software in <b>Error! Reference source not found.</b> 3 (Specification), as may be updated, replaced or amended from time to time;

### 1. The Software

- 1.1 The Service Provider shall provide the Software to the Authority in accordance with this Contract and the relevant Project Plan.

#### **Risk**

- 1.2 Risk in the media on which the Software is recorded shall pass to the Authority on delivery of such media to the Authority or Acceptance of the Software (whichever is the latter).

## ***Licence(s)***

- 1.3 Prior to commencing work on the System and procuring and developing the Software, the Service Provider shall specifically identify any applicable:

1.3.1 Service Provider IPR and Service Provider Software intended for supply or used in the System and, for the duration of the Term, grant the Authority a royalty free, worldwide and transferable only to another authority within London City limits, upon the Service Provider's prior written approval, licence of the same which permits the Authority to use, and sub-licence only to another authority within London City limits upon the Service Provider's prior written approval, of all Intellectual Property Rights in the Service Provider IPR and Service Provider Software for the benefit of the Authority and any Successor Authority and the Authority's agents with effect from the date of delivery in a form reasonably acceptable to the Authority; and

1.3.2 subject to clause 1.3.3, Third Party Software intended for supply or used in the System, agreeing with the Authority in advance (at the Authority's option) whether the Authority or the Service Provider is to obtain the licences necessary to use such Third Party Software and the terms upon which such licence should be granted to use such Third Party Software.

1.3.3 Unless otherwise agreed in writing, the Service Provider shall obtain all written licences required for such Third Party Software on the basis of a royalty free worldwide and transferable licence for the duration of the Term which permits the Authority to use, copy, adapt, translate and sub-licence all Intellectual Property Rights in the Third Party Software or parts thereof for the benefit of the Authority, and, where the Authority requires it, the Authority and/or any Successor Authority and its agents. Should this not be possible the Service Provider shall consult with the Authority with regards to alternative licence terms or alternative third party suppliers.

- 1.4 For the avoidance of doubt, any fees associated with the licences granted in clauses 1.3.1 and 1.3.2 shall be included in the Charges detailed in 4 (Charges).

## **2. Warranties and Obligations**

- 2.1 Without prejudice to any other warranties expressed elsewhere in the Contract or implied by law, the Service Provider warrants, represents and undertakes to the Authority that:

## 2.1.1 the Service Provider:

2.1.1.1 has full capacity and authority and all necessary licences, permits, permissions, powers and consents (including, where its procedures so require, the consent of its Holding Company) to enter into and to perform the Contract; and

2.1.1.2 is aware of the purposes for which the System and the Services are required and acknowledges that the Authority is reliant upon the Service Provider's expertise and knowledge in the provision of the Services; and

2.1.1.3 is entering into this Contract as principal and not as agent for any person and that it shall act as an independent contractor in carrying out its obligations under this Contract;

2.1.2 the Contract is executed by a duly authorised representative of the Service Provider;

2.1.3 all materials, equipment and goods used or supplied by the Service Provider in connection with the Contract shall be of satisfactory quality within the meaning of the Sale of Goods Act 1979 (as amended), sound in design and in conformance in all respects with the Specification;

2.1.4 all documents, drawings, computer software and any other work prepared or developed by the Service Provider or supplied to the Authority under the Contract shall not infringe any Intellectual Property Rights or any other legal or equitable right of any person;

2.1.5 each part of the System shall, on the date on which it is supplied in accordance with the Contract and for the Warranty Period thereafter, fulfil the Authority's requirements and comply with the Specification, and that if any part of the System materially fails to comply in accordance with this clause 2.1.5 at any time during the Warranty Period and the Service Provider shall comply with clause 2.3;

2.1.6 the System (whether supplied or recommended for purchase by the Authority in connection with this Contract) shall be fully compatible with the Authority's computer and system infrastructures (including its operating environment set out in the Specification) or notified to the Service Provider in writing from time to time;



- 2.1.7 the Service Provider shall fully co-operate with the Authority's agents, representatives or contractors (including other suppliers of computing products and services) and supply them with such information, materials and assistance as the Authority may reasonably request or authorise from time to time;
- 2.1.8 all of the Service Provider's liabilities, responsibilities, and obligations shall be fulfilled in compliance with all applicable laws, enactments, orders, regulations, codes of practice, licences, waivers, consents, registrations, approvals, and other authorisations of competent authorities ("**Applicable Laws**") and that the Authority Group's possession and/or use of the System and/or its receipt of the benefit of the Services shall not place the Service Provider or any of those persons so named in this clause in breach of any Applicable Laws, provided that the Service Provider shall have no liability under this clause in respect of any breach of such Applicable Laws to the extent such breach is caused by the negligent, wilful or fraudulent act and/or omission of the Authority. For the avoidance of doubt, clause **Error! Reference source not found.** of the Contract shall apply in the event that a Change in Law requires Changes to the System to be implemented by the Service Provider where the Changes are peculiar to the business of the Authority;
- 2.1.9 the media on which any System is supplied shall be free from material defects in materials and workmanship under normal use;
- 2.1.10 if and to the extent that software is being provided as part of the System or the Services, the Service Provider shall not and shall ensure that the Service Provider's Personnel and Sub-contractor's do not, without the Authority Contract Manager's prior written consent, include any Third Party software code which materially conforms to either (a) the then current Open Source definition laid down by the Open Source Initiative; or (b) any generally accepted replacement for or alternative to such Open Source definition at the relevant time;
- 2.1.11 the Service Provider shall ensure that the System and any software, electronic or magnetic media, hardware or computer system recommended by the Service Provider for use in connection with this Contract shall:
- 2.1.11.1 not have its functionality or performance affected, or be made inoperable or be more difficult to use by reason of any data related input or processing in or on any part of such

software, electronic or magnetic media, hardware or computer system;

2.1.11.2 not cause any damage to, loss of or erosion to or interfere adversely or in any way with the compilation, content or structure of any data, database, software or other electronic or magnetic media, hardware or computer system used by, for or on behalf of any of the Authority Group and/or any Third Party, on which it is used or with which it interfaces or comes into contact; and

2.1.11.3 comply with the Government's open standards principles as documented at <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>, and any variations, enhancements or actions undertaken by the Service Provider in respect of such software, electronic or magnetic media, hardware or computer system shall not affect the Service Provider's compliance with this clause 2.1.11;

2.1.12 subject to clause 2.1.8, in all cases, the costs of compliance with clause 2.1.11 shall be borne by the Service Provider; and

2.1.13 the Service Provider shall:

2.1.13.1 not introduce into any of the Authority's computer systems anything, including any computer program code, Virus, authorisation key, licence control utility or software lock, which is intended by any person to, is likely to, or may:

(a) impair the operation of the System or any other computer systems or programs in the possession of the Authority or impair the receipt of the benefit of the Services; or

(b) cause loss of, or corruption or damage to, any program or data held on the Authority's computer systems,

and this clause 2.1.13.1 shall apply notwithstanding that any such things are purported to be used for the purposes of protecting the Service Provider's IPR, Third Party IPR, the Service

Provider's contractual rights or other rights or not damaging the reputation of the Authority.

- 2.2 The Service Provider shall ensure that the benefit of any and all warranties which it receives in respect of any and all Hardware and Third Party Software are passed on to the Authority such that the Authority can enforce those warranties directly against such Third Party Software licensors and Hardware vendors.
- 2.3 Without prejudice to any other rights, powers or remedies the Authority may have, in the event of any breach(es) of the warranties set out at clauses **Error! Reference source not found.** of the Contract and 2.1.3 to 2.1.12 of this Schedule, the Service Provider shall promptly (and, if applicable, in accordance with any relevant KPI or PI) supply such services as are necessary to remedy such breach(es) and to prevent the re-occurrence of such breach(es) in the future. To the extent that any such breach(es) re-occurs (notwithstanding, in relation to the limited warranty contemplated in clause 2.1.5, the fact that the relevant Warranty Period may have ended) then, subject to the cause of the said re-occurrence being the same or similar to that which caused the initial breach(es), the Service Provider shall forthwith supply such further Services as are necessary to remedy such breach(es) and to prevent any further re-occurrence thereof. Any Services required to be performed pursuant to this clause 2.3 shall be performed at no additional cost to the Authority.
- 2.4 Each warranty and obligation in this clause 2 shall be construed as a separate warranty or obligation (as the case may be) and shall not be limited or restricted by reference to, or reference from, the terms of any other such warranty or obligation or any other term of the Contract.

### 3. The Authority's Data

- 3.1 The Parties agree that the Service Provider has no ownership of and, except as stated this Contract, acquires no rights in Authority Data. As between the Parties, the Authority retains all right of ownership, title, and interest in and to Authority Data, including all intellectual property rights therein.
- 3.2 Subject to the confidentiality obligations and the other terms of this Contract, the Authority grants the Service Provider a non-transferable (except to the affiliate entity within the Service Provider's Group), non-exclusive, and revocable license to use, analyze, create derivative works based on, host, store, display and process Authority Data for the purpose of performing, maintaining and improving the Services under this Contract for the duration of the Term. Additionally, the Service Provider may use De-identified Authority Data including performance metrics, statistics, and usage data to improve its Services or offer new products and services to the Authority. The Service Provider shall not use, analyze, host, store, or process Authority Data for any other purpose. "De-identified" shall mean aggregated data such that no

individual Micromobility Operator can reasonably be identified or associated with the data. The Service Provider may also display the Authority logo within designated areas of its Software.

- 3.3 The Service Provider shall also receive data from Micromobility Operators in a sandbox testing environment to test any modifications in the data feed from Micromobility Operators and improve existing features and functionalities and develop for the Authority new features and functionalities of the Software.
- 3.4 In furtherance of transparency, at Micromobility Operators' request and pursuant to a separate agreement with each interested Operator, the Service Provider may give access to the datasets of that particular Operator only, representing information the Authority has available on that Micromobility Operator through the Software.
- 3.5 The Authority agrees that with respect to any suggestions and feedback the Authority may have with regard to the Software, the Service Provider may, in its discretion and for any purpose, use, modify and incorporate into its products and services and license and sublicense the suggestions and feedback without any obligation to the Authority.
- 3.6 The Service Provider acknowledges the Authority Group's ownership of Intellectual Property Rights which may subsist in the Authority Group's data. The Service Provider shall not delete or remove any copyright notices contained within or relating to the Authority Group's data.
- 3.7 The Service Provider and the Authority shall each take reasonable precautions (having regard to the nature of their other respective obligations under the Contract) to preserve the integrity of the Authority Group's data and to prevent any corruption or loss of the Authority Group's data.

## 4. Intellectual Property Rights

- 4.1 Except for any of the Service Provider's Software, the Third Party Software, the Service Provider's IPR and Third Party IPR, all Intellectual Property Rights of whatever nature in the System and the Services ("the **Authority Rights**") whether created by the Service Provider or any of the Service Provider's Personnel shall or shall on creation of the same be and remain vested in the Authority. Prior to such vesting, the Service Provider grants each member of the Authority Group a royalty-free, worldwide and transferable licence for the duration of the Term to use, adapt, translate, support and sublicense the Authority Rights to the extent necessary for the Authority, the Authority Group and its other authorised agents to receive its rights under this Contract, including with respect to the right to Test the System and Software. The Service Provider shall do all such acts and execute all such deeds and documents as shall be necessary or

desirable to perfect the right, title and interest of the Authority in and to such Intellectual Property Rights, including ensuring that the Service Provider's Personnel assign all such Intellectual Property Rights owned by them either direct to the Authority or to the Service Provider to enable the Service Provider to comply with its obligations hereunder and waive any moral rights they may otherwise have, in each case at no cost to the Authority.

- 4.2 Nothing in this clause 4 shall prevent the Service Provider from using data processing techniques, ideas and know-how gained during the performance of this Contract in the furtherance of its normal business, to the extent that this does not constitute or relate to a disclosure of Confidential Information or an infringement by the Service Provider of any Intellectual Property Right.
- 4.3 To the extent that any Authority Group member provides the Service Provider with any materials in which any member of the Authority Group owns (or is licensed by a Third Party to use) the IPR ("the **Authority Deliverables**") for the purpose of or in connection with the provision of the Services or supply of the System, the Service Provider acknowledges and agrees that nothing in this Contract grants to the Service Provider any right, title or interest in such materials other than a limited non-exclusive right to use those materials solely for the purposes of supplying the System and providing the Services. All Intellectual Property Rights in such materials are and shall remain the exclusive property of the Authority Group or (if applicable) its Third Party licensors.
- 4.4 The Service Provider warrants and shall ensure that the possession and/or use by the Authority Group of the System, and the performance by the Service Provider of the Services shall not constitute any infringement or misappropriation of any Intellectual Property Rights or any other legal or equitable right of any person and that the Service Provider owns or has obtained valid licences to or of all such Intellectual Property Rights and other rights which are necessary for the performance of its obligations under this Contract.
- 4.5 If any Third Party claims that the possession and/or use of the System and/or the receipt of the Services ("**Indemnified Deliverables**") by any Authority Group member and/or the provision by the Service Provider of any Indemnified Deliverable under or in connection with this Contract constitutes an infringement or misappropriation of any Intellectual Property Rights or other right of that Third Party ("**IPR Claim**"), the Service Provider shall indemnify, keep indemnified and hold harmless the Authority Group Members (including its respective employees, Sub-contractors and agents) against all Losses arising from or incurred by reason of any such IPR Claim (including the defence and any settlement of such IPR Claim).
- 4.6 In the event of a claim pursuant to clause 4.5:

- 4.6.1 the Authority shall promptly notify the Service Provider of the claim;
  - 4.6.2 the Service Provider shall, at its own cost and expense, control the defence of such IPR Claim and any related proceedings or settlement negotiations, except that the Authority shall be entitled to take any action which it deems necessary if the Service Provider fails to take action, or (in the Authority's reasonable opinion) delays taking action, in defending or settling any such IPR Claim and such failure or delay may, in the reasonable opinion of the Authority, prejudice the interests of the Authority Group; and
  - 4.6.3 at the cost and expense of the Service Provider, the Authority shall take all reasonable steps to co-operate with the Service Provider in the defence or settlement of such IPR Claim.
- 4.7 If any Indemnified Deliverable becomes the subject of any IPR Claim and, as a result of such IPR Claim, a court of competent jurisdiction grants an injunction preventing the use by the Service Provider or any Authority Group member of any of such Indemnified Deliverable or there is substantial risk of such injunction being granted or the IPR Claim is settled on the basis that the Indemnified Deliverable cannot be used, the Service Provider shall at its expense as soon as possible following (and in any event within thirty (30) days of) such event occurring:
- 4.7.1 obtain for the Authority Group members the right to continue to possess, use and/or receive the benefit of the relevant Indemnified Deliverable(s); or
  - 4.7.2 replace or modify the relevant Indemnified Deliverable(s) so that it becomes non-infringing without detracting from the functionality or performance of the overall System or Service and provided that any such replacement or modification shall not prevent the Service Provider's compliance with the warranties contained at **clause 2**.
- 4.8 The Service Provider shall have no liability under or in connection with this Contract for any infringement caused solely and directly by:
- 4.8.1 the combination of the relevant Indemnified Deliverable with other products, data or information not supplied by the Service Provider unless the combination was made or approved by the Service Provider;
  - 4.8.2 the modification of the Indemnified Deliverable unless the modification was made or approved by the Service Provider;
  - 4.8.3 the supply by or on behalf of the Authority of any of the materials specified at clause 4.3; or



- 4.8.4 breach by the Authority of any of the terms of this Contract and/or any licence terms in respect of the Indemnified Deliverable to which the Authority is subject pursuant to the terms of this Contract.
- 4.9 If any Third Party claims that the possession and/or use by the Service Provider of any of the Authority Deliverables constitutes an infringement or misappropriation of any Intellectual Property Rights or other right of that Third Party, the Authority shall indemnify keep indemnified and hold harmless the Service Provider (including their respective employees, Sub-contractors and agents) and keep the Service Provider indemnified against all claims, demands, actions, costs, expenses (including legal costs and disbursements on a full indemnity basis) and damages awarded by a court of competent jurisdiction or agreed to be paid by way of settlement of such claim provided that:
  - 4.9.1 the Service Provider promptly notifies the Authority of such claim;
  - 4.9.2 the Authority shall, at its own cost and expense, be entitled to control the defence of such claim and any related proceedings or settlement negotiations; and
  - 4.9.3 at the cost and expense of the Authority, the Service Provider takes all reasonable steps to co-operate with the Authority in the defence or settlement of such claim.
- 4.10 The Authority shall not be liable under 4.9 or otherwise for any infringement:
  - 4.10.1 caused by the combination of the relevant the Authority Deliverables with other products, data, or information not supplied by the Authority;
  - 4.10.2 caused by any use by the Service Provider of any the Authority Deliverables other than strictly for the purpose of the Service Provider performing its obligations under this Contract; or
  - 4.10.3 caused by breach by the Service Provider of any of the terms of this Contract.
- 4.11 If any Authority Deliverables become the subject of any claim as described in clause 4.9 and, as a result of such claim, a court of competent jurisdiction grants an injunction preventing the Authority Group's and/or the Service Provider's use of any such the Authority Deliverables or there is substantial risk of such injunction being granted or the claim is settled on the basis that the Authority Deliverables cannot be used, the Authority shall at its expense as soon as possible following (and in any event within thirty (30) days of) such event occurring:

- 4.11.1 obtain for the Service Provider the right to continue to possess and/or use the relevant the Authority Deliverables;
  - 4.11.2 with all such assistance from the Service Provider (including the provision of Additional Services) as may be agreed in accordance with the Change Control Procedure, replace or modify the relevant the Authority Deliverables so that it becomes non-infringing without detracting from the functionality or performance of the Authority Deliverables so as to prevent the Service Provider from complying with its obligations under this Contract; or
  - 4.11.3 if it is not commercially reasonable to perform either of the above options, the Authority and the Service Provider shall cease use of the infringing the Authority Deliverables in which case the Parties' representatives shall meet and, in good faith, explore all possible amendments to the Services which are required as a result of such cessation of use. Any such amendments shall be considered and (where applicable) agreed in accordance with the Change Control Procedure.
- 4.12 The Service Provider shall have no right (save where expressly permitted under the Contract or with the Authority's prior written consent) to use any trade marks, trade names, logos or other Intellectual Property Rights of the Authority.
- 4.13 The Service Provider shall ensure that all royalties, licence fees or similar expenses in respect of all Third Party IPR used in connection with the Contract have been paid and are included within the Charges.
- 4.14 This clause 4 shall survive termination of this Contract.

## 5. Privacy, Data Protection and Cyber Security

- 5.1 The Service Provider shall comply with all of its obligations under Data Protection Legislation and, if Processing Personal Data on behalf of the Authority, shall only carry out such Processing for the purposes of providing the Services in accordance with **Error! Reference source not found..**
- 5.2 The Service Provider shall comply with the requirements of Appendix 2 - Cyber Security.

## 6. Source Code, Escrow and Verification Services

**– this section (Section 6. Source Code, Escrow and Verification Services) is currently not applicable. Save where the Authority may require an amendment to the Services, if any source code or software development process is added to the contract; this shall be submitted to TfL for approval in accordance with the Variation procedure set out in this Agreement Section 6 may apply.**



- 6.1 The Service Provider shall supply to the Authority, the source code to any Software in which the Intellectual Property Rights are, or are to be, owned by the Authority, together with any programmers' notes and other documentation reasonably required to operate the source code in object code form and to maintain and adapt the source code, when that part of the System is supplied to the Authority ("the **Authority Materials**").
- 6.2 The Service Provider shall ensure that the source code to any Software forming part of the Service Provider's IPR and/or Third Party IPR, together with any programmers' notes and other documentation reasonably required to operate the source code in object code form and to maintain and adapt the source code ("the **Escrow Materials**") shall, where requested by the Authority in **Error! Reference source not found. (Key Contract Information)**, be subject to source code deposit arrangements and verification services to be entered into, on such terms as are reasonably acceptable to the Authority, within thirty (30) days of the Authority's request to do so (whether in relation to part or all of the Software) for the benefit of the Authority and its authorised agents with either NCC International Limited ("**NCC**") (on NCC's then standard terms) or any other reputable escrow agent agreed to by the Authority and providing for the release of the source code of such Software in the event of insolvency (or analogous events) of the Service Provider, inadequate performance of support or maintenance obligations (if any) or cessation of trade by Service Provider.
- 6.3 Where requested by the Authority, the Service Provider shall procure that NCC (or such other escrow agent as the Authority considers appropriate) enters into the escrow/verification agreement. The charges payable to NCC or other escrow agent shall be borne by the Authority.
- 6.4 The Service Provider shall at all times ensure that the Escrow Materials deposited with NCC or other escrow agent are capable of being used to generate and maintain and adapt the latest version of the Software and the Service Provider shall deliver to NCC or other escrow agent an updated copy of the Escrow Materials as and when necessary for this purpose or when requested to do so by the Authority.
- 6.5 This clause 6 shall survive termination of the whole or part of the Contract.

## 7. **Loss of Software and Data Security**

- 7.1 Without prejudice to its other obligations under this Contract, the Service Provider shall, during the term of this Contract and in the

course of performing the Services, provide all measures necessary in respect of the prevention of unauthorised access to any Authority Group member's computer systems, software and data, the prevention of the introduction of known Viruses and shall provide the capability to restore the systems, software and data in the event that the loss of the systems, software or data arises directly or indirectly from any act or omission of the Service Provider (including the Service Provider's Personnel) or whilst such systems, software or data is in the custody, control or otherwise interfaced with or accessed by the Service Provider.

- 7.2 The Service Provider shall not, without the consent of the Authority, be entitled to delete any software or data belonging to the Authority Group to which the Service Provider has access in performance of its obligations under this Contract.
- 7.3 The Service Provider shall, upon receipt of the Authority Group's software or data and during any collection, processing, storage and transmission by the Service Provider of the Authority Group's software or data, take all necessary precautions to preserve the integrity of such software and data and to prevent any corruption or loss thereof, including such precautions as are specified by the Authority from time to time.
- 7.4 In the event that any of the Authority Group's software or data is corrupted or lost or so degraded as to be unusable due to any act or omission of the Service Provider after its receipt or creation by the Service Provider or during any collection, processing, storage or transmission by the Service Provider of the Authority Group's software or data or otherwise as a result of any default by the Service Provider then, in addition to any other remedies that may be available to the Authority under this Contract or otherwise:
- 7.4.1 the Service Provider shall promptly, at the Service Provider's expense, restore or procure the restoration of the Authority Group's software and data to the Authority Group's reasonable satisfaction, as notified in writing, such that the Service Provider has made good the corruption, loss or degradation of the software and data; and
- 7.4.2 in the event that the Authority itself has to restore or procure the restoration of the Service Provider's software or data, then the Authority shall require the Service Provider to repay the Authority's reasonable costs and expenses incurred in carrying out such restoration.
- 7.5 In the event that any of the Authority Group's software or data is corrupted or lost or sufficiently degraded as to be unusable otherwise than due to a default by the Service Provider, the Service Provider shall nevertheless carry out such remedial actions to restore the Authority Group's software and data or such other actions as may be

necessary to restore the Authority Group's software and data as the Authority may request in writing and the reasonable agreed cost of the remedial actions or such other actions shall be borne by the Authority.

7.6 Without prejudice to the generality of **clauses 7.1** and 7.3, the Service Provider shall:

7.6.1 before performing any actions in respect of the Authority Group's software or data, ensure that it has performed back-ups of such software or data as set out in **Error! Reference source not found. (Key Contract Information)** or agreed in writing from time to time or, where none are agreed, as are reasonable in the circumstances; and

7.6.2 perform its obligations in conformance with the Security Policy.

Nothing in this Contract shall relieve the Service Provider's obligations in this regard.

7.7 The Service Provider shall fully indemnify the Authority and the Authority Group for any and all Losses incurred or suffered by the Authority which results from a breach by the Service Provider of its obligations under this **clause 7**.

7.8 This clause 7 shall survive termination of this Contract.

## **8 Option to Extend Duration**

8.1 The Authority has an option, exercisable at its sole discretion, to extend the duration of the Contract for a further period or periods up to a total of one year by notice in writing to the Service Provider provided that such notice is served at least one month prior to the expiry of the initial duration of the Contract or the expiry of any previous extension, if later.

## Appendix 1 - Privacy and Data Protection

For the purposes of this Appendix, 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>	an assessment by the Data Controller of the impact of the envisaged Processing on the protection of Personal Data;
<b>“Data Protection Legislation”</b>	<p>Protection means:</p> <ul style="list-style-type: none"><li>(a) 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;</li><li>(b) Directive (EU) 2016/680 (the Law Enforcement Directive);</li><li>(c) 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;</li><li>(d) any statutory codes of practice issued by the Information Commissioner in relation to such legislation; and</li><li>(e) the Privacy and Electronic Communications (EC Directive) Regulations 2003;</li></ul>
<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 Request”</b>	a request made by or on behalf of a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation including the right (i) to be informed, (ii) of access, (iii) to rectification, (iv) to erasure, (v) to restrict processing, (vi) to data portability, (vii) to object and (viii) to automated decision making including profiling.
A1.1	With respect to the Parties' rights and obligations under the Contract, the Parties acknowledge that the Authority is a Data Controller solely responsible for determining the purposes and manner in which Authority Personal Data is to be Processed, and that the Service Provider is a Data Processor.
A1.2	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:  <b>End users of shared mobility services</b>
A1.2.2	The Authority Personal Data to be Processed includes the following types of Personal Data and/or Sensitive Personal Data:  <b>Data includes details of the use of shared mobility services – e.g. date/time of trips made, trip start and end points (GPS data), etc.</b>
A1.2.3	The Authority Personal Data is to be Processed for the following purpose(s):  <b>To enable the assessment of shared mobility services.</b>

# Transport for London

A1.2.4 Clause deleted – data not to be processed in any restricted countries.

A1.2.5 The subject matter of the Authority Personal Data to be Processed is:

**The processing is necessary to allow the Service Provider to effectively deliver the contract to provide a Micromobility Management system (pursuant to the Invitation to Tender No. tfl\_scp\_002004).**

A1.2.6 The duration of the Processing shall be:

**For as long as this Agreement is in effect beginning on the Effective Date – as set out in Schedule 1 Key Contract Information - and ending 18 months thereafter, with the possibility to extend the duration by additional 6 months at the sole discretion of TFL.**

A1.2.7 The nature of the Processing is:

**The Software of the Service Provider, commonly known as Blue Systems Mobility Manager, will enable the Authority to view, monitor, regulate and analyze Authority Data.**

**There is no intention to identify individuals from any data processed on the system, and both Parties must not use the data to identify natural persons. Steps will be taken to mitigate the risk of re-identification, including, but not limited to, data minimisation.**

A1.3 Without prejudice to the generality of Clause 5, the Service Provider shall:

A1.3.1 process the Authority Personal Data only in accordance with written 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, assist the Authority in carrying 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);

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 which are appropriate to protect against unauthorised or unlawful Processing of Authority Personal Data and against accidental loss, destruction of, or damage to such Authority Personal Data which the Authority may reasonably reject (but failure to reject shall not amount to approval by the Authority of the adequacy of the measures);

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 Request (or purported Subject Request); or

A1.3.11.1.2 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; and
    - A1.3.12.2 where applicable, such assistance as is reasonably requested by the Authority to enable it to comply with the Subject Request within the relevant timescales set out in Data Protection Legislation;
  - 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. The Service Provider shall provide the Authority with such information regarding the proposed sub-contractor as the Authority may reasonably require. The Service Provider shall only share Authority Personal Data with a sub-contractor where there is a written contract in place between the Service Provider and the sub-contractor which requires the sub-contractor to:

# Transport for London

- A1.4.1 only Process Authority Personal Data in accordance with the Authority's written 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, 17.1, 17.2, 19.1, 21.2, 23 and 24).
- 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 written 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 written 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 written 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 27.1.1, 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 The Service Provider shall remain fully liable for all acts or omissions of any sub-contractor.
- A1.11 Following termination or expiry of this Contract, howsoever arising, the Service Provider:
  - A1.11.1 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 A1.11.3;
  - A1.11.2 where Clause A1.11.1 does not apply, may Process the Authority Personal Data only for such duration as agreed in Clause A1.2.6 above and following this will then comply with Clauses A1.11.3 and A1.11.4;
  - A1.11.3 subject to Clause A1.11.1, shall 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

# Transport for London

A.1.11.4 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.

A1.12 Authority Personal Data may not be Processed following termination or expiry of the Contract save as permitted by Clause A1.11.

A1.13 For the avoidance of doubt, and without prejudice to Clause A1.11, 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.

A1.14 The indemnity in Clause 19 shall apply to any breach of Clause A1 and shall survive termination or expiry of the Contract.

A1.15 The Parties' liability in respect of any breach of Clause 23.1 and this Clause A1 insofar as they relate to fines, court awards, settlements and legal costs shall be unlimited.

## Appendix 2 – Cyber Security

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

<b>“Cloud”</b>	A type of internet-based computing service where organisation can have aspects of their IT infrastructure managed by external providers, normally as a Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) basis
<b>“Cyber Essentials Scheme”</b>	is a UK government scheme encouraging organisations to adopt good practice in information security, focussing mainly on technical controls rather than governance, risk, and policy
<b>“Cyber Security Policy / Policies”</b>	The high level Cyber Security requirements for all IT and Operational technology and data owned by TfL or operated and supported by third parties for on behalf of TfL.
<b>“Cyber Security Standard(s)”</b>	The technical detail behind the implementation of the high level cyber security requirements as set out in the Cyber Security Policies.
<b>“Data”</b>	means data created, generated or collected, during Providing the Services (or any part thereof), including Personal Data and data supplied to TfL and members of the TfL Group.
<b>“Good Industry Practice”</b>	means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of undertaking under the same or similar circumstances.
<b>HMG Information Security Assurance Standards</b>	the meaning and definition as well as relevant policy documents and standards can be found at <a href="https://www.gov.uk/government/collections/government-security">https://www.gov.uk/government/collections/government-security</a> <u><a href="#">or any updated link</a></u> ;
<b>“Information</b>	means a register of all information assets relating to the

# Transport for London

<b>Asset Register”</b>	<i>services</i> as detailed in paragraph 2.2(c)
<b>“Information Security Management System” or “ISMS”</b>	a framework of governance models, policies and procedures, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security in accordance with the requirements of Paragraph 15
<b>ISO/IEC 27001</b>	is an information security standard specification for an information security management system (ISMS), with an emphasis on measuring and evaluating how well an organisation's ISMS is performing.
<b>“IT Services”</b>	means the IT services that support the delivery of the Services;
<b>“Malicious Software”</b>	means any software that brings harm to a computer system. Commonly known as malware can be in the form of worms, viruses, trojans, spyware, and adware which steal protected data, delete documents or add software not approved by a user.
<b>“Operational Technology”</b>	means any hardware or software which monitors and/or operates a physical process.
<b>“Outline Security Management Plan”</b>	means the security plan provided by the <i>Contractor</i> as part of their tender submission
<b>“Removable Media”</b>	any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives
<b>“Security Incident”</b>	a potential or actual event or attempted breach of security affecting the confidentiality, integrity or availability of the Services, IT Services or Networks which process or hold Data
<b>“Security</b>	means the <i>Contractor's</i> security plan developed and



# Transport for London

<b>Management Plan”</b>	revised pursuant to Paragraph 14
<b>“Security Policy”</b>	means any TfL security policies as amended by TfL from time to time;
<b>“Security Risk”</b>	meaning all Risks associated with the security of the Services which may have a negative impact upon the agreed security posture, including information security and any risks identified pursuant to the Security Management Schedule.
<b>“Security Risk Register”</b>	means a register of Security Risks produced and maintained as detailed in paragraph 2.2(b)
<b>“Service Assets”</b>	means all information technology assets and rights including all physical assets, Software, IPR, as well as spares and components whether in storage, repair or on sites, used by the <i>Contractor</i> to Provide the Services.
<b>“The Contractor’s people”</b>	means all employees, agents, consultants and contractors of the <i>Contractor</i> or of any Sub-Contractor
<b>“Contractor Premises”</b>	means any land or building where the <i>Contractor</i> carries out any part of this contract
<b>“TfL Information Security Controls Framework”</b>	means a hierarchy of IT security documents consisting of the high level Information Management Security Policy and ten security principles (Information Security Controls Framework).
<b>“TfL Network(s)”</b>	means the network infrastructure and services owned or used by TfL to support the delivery of the IT Services.
<b>“TfL Personnel ”</b>	means all employees, agents, consultants and contractors of TfL
<b>“TfL</b>	as defined in the TfL Information Security Classification

**Restricted”** Standard (listed in Annex 5)

**“TfL Sites”** means all TfL premises where the services are delivered

## 1. **PURPOSE**

1.1 The purpose of this appendix to the Scope is to set out:

- (a) the principles of protective security to be applied by the *Contractor* in Providing the Service;
- (b) the *Contractor's* wider security obligations relating to Providing the Service;
- (c) the *Contractor's* requirements to test and audit Providing the Service including any Information Security Management System paragraph 3, to ensure compliance with the security requirements set out in this appendix to the Scope;
- (d) the *Contractor's* obligations in the event of a Security Incident;
- (e) the principles for the *Contractor's* development, implementation, operation, maintenance and continual improvement of the Security Management Plan;
- (f) the principles for the *Contractor's* development, implementation, operation, maintenance and continual improvement of the Information Security Management System;
- (g) any obligations for certification against Providing the Service including but not limited to ISO/IEC 27001, the Cyber Essentials Scheme or HMG Information Security Assurance Standards;
- (h) any requirements to Provide the Service in accordance with the CESG Commercial Product Assurance (CPA) Scheme
- (i) the requirements on the *Contractor* when Providing the Service, which are aligned with the 10 Steps to Cyber security set out by the Government (see Annex 5) and
- (j) the *Contractor's* obligation to comply with the Operations Technology Cyber Security Standards (see Annex 5).

## 2. **SECURITY PRINCIPLES**

- 2.1 The *Contractor* acknowledges that security, data protection and confidentiality are of fundamental importance in relation to its provision of the service and TfL's ability to retain public confidence. The *Contractor* shall at all times comply with the security principles set out in Paragraph 3 in Providing the Service.
- 2.2 In recognition of the importance that the Parties place on security, data protection and confidentiality, the *Contractor* shall ensure that a director or relevant individual, as agreed by TfL, is made aware of the risks set out in the Security Management Plan and is assigned overall responsibility for ensuring that:
- (a) appropriate members of the *Contractor* people take responsibility for managing the different levels of security risk and promote a risk management culture;
  - (b) a Security Risk Register is produced and maintained and that all Security Risks are documented in an appropriate manner and is included in any contract risk register if one is in place. This Security Risk Register must be available for audit when reasonably required by TfL as set out in Clause 7 of this Schedule.
  - (c) an Information Asset Register is produced and maintained and that all information technology assets are documented in an appropriate manner in the Information Asset Register and shall identify the criticality of the relevant Service Assets in the delivery of the Services. This register must be available for audit when reasonably required by TfL as stated in Paragraph 7 of this Schedule and when a Security Incident occurs.
  - (d) supporting policies are implemented (where relevant) and communicated with the *Contractor's* people.
- 2.3 The *Contractor* shall, at all times ensure that:
- (a) security threats to the service are minimised and mitigated;
  - (b) delivery of the service shall fully comply at all times with:
    - (i) any security requirements set out in Annex 3;
    - (ii) the agreed Outline Risk Management Processes and approach set out in Annex 2; and
    - (iii) Good Industry Practice.
- 2.4 The *Contractor* must notify TfL of any instances where software, applications, services or processes are hosted or run from the cloud that are not part of Providing the Service, and that host, process or

connect with any of TfL Operational or IT technology, Data and Networks or handle TfL Data. The *Contractor* is responsible for ensuring that any such cloud services comply with this Cyber Security Management Schedule.

### 3. **ACCESS CONTROLS AND SECURE CONFIGURATION OF SYSTEMS**

3.1 The *Contractor* shall comply with all obligations relating to the patching and configuration management of Service Assets as set out in Annex 4 in addition to any specific obligations set out in Annex 4, the *Contractor* shall ensure that:

- (a) security patches are applied to Service Assets as soon as possible in line with vendor recommendations in accordance with overall risk management;
- (b) account management and configuration control processes are implemented to ensure that access to Service Assets by the *Contractor's* people is limited to the extent required for them to fulfil their roles in supporting of Providing the Service.
- (c) when the *Contractor's* people change roles or no longer support Providing the service, access rights are revoked or reviewed;
- (d) any system administration functionality is strictly controlled and restricted to those people who need to have access to such functionality and that the ability of the *Contractor's* people to change the configuration of the Service Assets is appropriately limited and fully auditable;
- (e) *The Contractor's* people are informed of what constitutes acceptable access of operational or IT technology, Data and Networks and the consequences of non-compliance;
- (f) any preconfigured passwords delivered with any Service Assets are changed prior to their implementation for use in Providing the Service;
- (g) the Service Assets have appropriate devices, tools or applications in place to filter traffic or separate connections, such as industry standard firewalls and malicious software protection, to all public or private networks which are not controlled by or on behalf of TfL;
- (h) all wireless functionality is secure; and
- (i) software upgrades and patching must be managed appropriately and access to any software shall be granted using the principle of least privilege.

## 5. THE CONTRACTOR'S PEOPLE

- 5.1 The *Contractor* shall, appoint a member of the *Contractor's* people to be the security manager who shall be responsible for the development, monitoring, enforcement, maintenance and enhancement of all security measures set out in this appendix to the Scope (the "**Security Manager**").
- 5.2 The *Contractor* shall ensure that all of *it's people* are security screened or vetted and shall provide TfL within five (5) working days of the *starting* date, and every twelve (12) months thereafter, written confirmation that this obligation has been complied with.
- 5.3 The *Contractor* shall immediately notify the *Service Manager* if it becomes aware of any security clearance issues in relation to the *it's* people and the *Contractor* shall undertake any action requested by the *Service Manager* in relation to mitigating the impact of any such security clearance issues.

## 6. TRAINING

- 6.1 The *Contractor* shall ensure that all of the *Contractor's* people have undergone suitable security awareness training prior to their deployment and such security awareness training shall cover, as a minimum; account usage, malicious software, home and mobile working, use of removable media, audit and inspection and Security Incident reporting and data handling. The *Contractor* shall implement an up-to-date on-going programme of security awareness training for the *Contractor's* people throughout the *service period*.
- 6.2 The *Contractor* shall provide additional training to its people, which may be required following a Security Incident, the application of a patch or update, or any relevant change to the Scope.
- 6.3 The *Contractor* shall ensure that all of *it's* people are familiar with their responsibilities under applicable law and policies including, as a minimum, the Data Protection Legislation, the Security Policies set out in Paragraph 1 of this appendix to the Scope and policies in relation to the handling of protectively marked materials both during their employment and following the termination of or change to the terms of their employment.

## 7. TESTING & AUDIT

- 7.1 The *Contractor* shall conduct regular automated vulnerability scans the Service Assets, as agreed in the Risk Management Process and ensure that any identified vulnerabilities are appropriately mitigated or patched in line with the TfL Security Patching Standard (Annex 5), taking into consideration the risk posed to the Client and Providing the Service.

- 7.2 The Contractor shall conduct security tests, including ethical hacking and penetration tests, to assure compliance with the Security Incident Management Process, the security provisions in this appendix to the Scope, the Security Management Plan. The Contractor shall conduct security testing in accordance with the Security Management Plan. The Contractor shall conduct such security tests, as a minimum, every twelve (12) months from the starting date and shall include security penetration testing of the Service Assets and the associated technical infrastructure. Wherever the Service Assets are accessible from the internet or other such public network, the Contractor shall carry out security penetration tests from the internet or the public network.
- 7.3 The Contractor shall, within one (1) week of completion of the security provide a report to the *Service Manager* setting out the outcome of such security tests including all identified vulnerabilities and it's plans to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this appendix to the Scope.
- 7.4 The *Contractor* shall implement its plans to each identified vulnerability in accordance with the report delivered pursuant to Paragraph 7.2 save to the extent directed by the *Service Manager* in writing.
- 7.5 The *Contractor* shall, upon request by TfL, following a Security Incident, carry out such additional security testing over and above the obligations set out in Paragraph 7.2.
- 7.6 The *Client* shall be entitled to send a representative to witness the conduct of any audit or security tests carried out by or on behalf of the *Contractor*. The *Contractor* shall provide the *Service Manager* with the results of such audits (in a form agreed in advance) as soon as practicable after the completion of each audit or test.
- 7.7 In addition to complying with this document, PCI DSS where applicable and other relevant industry standards and Good Industry Practice, the *Contractor* shall at least once during each twelve (12) month period starting from the Service Commencement Date, engage an appropriately skilled third party to conduct a formal audit of the Service Assets against the then current versions of the:
- (a) security controls, processes and procedures required pursuant to this appendix to the Scope;
  - (b) Data Protection Legislation (using BS10012 or another standard as agreed with TfL), where applicable; and
  - (c) Security Management Plan.

The *Contractor* shall inform the *Service Manager* of actual or potential security issues which impact or could impact Providing the Service within five (5) days of becoming aware of them and shall keep the

*Service Manager* up to date as the it investigates the nature and impact of such issue. Within five (5) days of the finalisation of audit findings, the *Contractor* shall provide the *Service Manager* a copy of all such findings which are relevant.

- 7.8 Without prejudice to any other right of audit or access granted to the *Client* pursuant to this appendix to the *Scope* or at law, the *Service Manager* or other representatives of the *Client* may carry out such audits in relation to security matters as are reasonably required to assess the *Contractor's* compliance with the Information Security Management System and the Security Management Plan.
- 7.9 If any test or audit carried out reveals any non-compliance with this appendix to the *Scope* or vulnerability (and, in the case of a TfL audit, TfL has informed the *Contractor* thereof), the *Contractor* shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this appendix to the *Scope*. The *Contractor* shall implement its plans to remedy each identified vulnerability in accordance with such report save to the extent directed by the *Service Manager*.

## **8. SECURITY INCIDENT MANAGEMENT PROCESS**

- 8.1 The *Contractor* shall:
- (a) establish, document and provide to the *Service Manager* a process to identify and respond to Security Incidents and mitigate the impact of such Security Incidents on Providing the Service, including assigning clearly defined roles and responsibilities to specific *Contractor* people;
  - (b) record each Security Incident and corresponding severity level in the *Contractor's* ISMS; and
  - (c) without limitation to the other provisions of this appendix to the *Scope*, follow TfL's reasonable instructions in relation to the identification and resolution of any Security Incident.
- 8.2 The *Contractor* shall notify and ensure that the *Service Manager* is aware as soon as possible and in any event no later than within **one (1) hour**, upon becoming aware of any Security Incident or of any potential Security Incident.
- 8.3 The *Contractor* will additionally provide notification with all relevant details reasonably available of any actual or suspected breach of security in relation to any *Client* personal data including unauthorised or unlawful access or processing of, or accidental loss, destruction or damage.
- 8.4 If a Security Incident occurs, the *Contractor* shall:



# Transport for London

- (a) immediately take steps to assess the extent of the Data compromised or affected including, but not limited to, the amount of affected;
- (b) immediately take the steps necessary to remedy or protect the integrity of the Service Assets against any such Security Incident;
- (c) securely collect and preserve evidence, including logs, to support the Security Incident Management Process and share with the *Service Manager* such evidence;
- (d) handle any information pertaining to the Security Incident according to the handling requirements for TfL RESTRICTED information defined in TfL's Information Security Classification Standard;
- (e) promptly escalate the Security Incident to the Service Manager;
- (f) when requested by TfL:
  - a. provide such information in relation to the Security Incident (including, if necessary, by collating such information from its and its Sub-contractors' systems and the *Contractor Personnel*);
  - b. provide the *Client's* representative with supervised access (or, if the Parties agree, direct access) to any relevant systems, *Contractor Premises* and people in order to investigate the Security Incident; and
  - c. follow the *Client's* directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Service Assets; and
- (g) as soon as reasonably practicable develop and provide TfL with a copy of its remediation plan for the Security Incident which sets out full details of the steps taken and to be taken by the *Contractor* to:
  - a. correct, make good, reinstate, replace and remediate all deficiencies and vulnerabilities, loss and/or damage to the Service Assets, Data, and/or Services in connection with the Security Incident; and
  - b. perform or re-perform any security tests or alternative tests relating to the security of the Service Assets and/or Services as appropriate and within the timescales specified by TfL, to assure TfL that the Security Incident has been addressed and its effects mitigated,



provided that any such remediation must be implemented in accordance with this appendix to the Scope. The *Contractor* shall fully implement and comply with any such remediation plan unless otherwise instructed by the Service Manager.

- 8.5 The *Contractor* shall provide a detailed report to TfL within two (2) days of the resolution of the Security Incident, a report to detail:
- (a) the nature of the Security Incident;
  - (b) the causes and consequences of the Security Incident;
  - (c) the actions undertaken and length of time taken by the *Contractor* to resolve the Security Incident; and
  - (d) the actions undertaken by the *Contractor* to prevent recurrence of the Security Incident.
- 8.6 If there is a suspected security event up to and including a Security Incident, the *Contractor* shall to the extent requested by the TfL CISO (or any duly authorised delegate):
- (a) provide information in relation to the Services which is relevant collating, if necessary, relevant information from Sub-contractors' systems and the *Contractor* Personnel;
  - (b) provide relevant TfL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, *Contractor* Sites and *Contractor* Personnel in order to investigate the security incident; and
  - (c) follow TfL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Services; and
  - (d) work with TfL to identify any lessons learnt which could mitigate any gaps in process, policy or controls.

and TfL shall reimburse the *Contractor's* reasonable, demonstrable costs and expenses in relation to the *Contractor's* compliance with such request.

## **9. SECURITY LOGGING AND MONITORING**

- 9.1 The *Contractor* shall ensure that the Security Management Plan sets out its monitoring strategy to monitor its own performance of its obligations under this appendix to the Scope. The *Contractor* shall update its monitoring strategy as necessary throughout the *service period* in response to:
- (a) changes to applicable laws, regulations and standards;
  - (b) changes to Good Industry Practice;

- (c) any relevant change to the Scope or this appendix to the Scope;
  - (d) any Security Incident; and
  - (e) any instruction by the Service Manager.
- 9.2 The monitoring strategy should include, as a minimum, processes for monitoring and logging (as appropriate):
- (a) networks and host systems to detect attacks originating both on an internal private network or from public networks (e.g. internet);
  - (b) instances of misuse of the Service Assets, *Contractor* systems used in Providing the Services and data by the Parties people, including attempts at such misuse;
  - (c) wireless access points to ensure that all wireless networks are secure and no unauthorised access points are available;
  - (d) malicious software on the *Contractor* systems used in Providing the Services and the Service Assets;
  - (e) access to and movement of Data, including internal access to such Data; and
  - (f) traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attempt or actual attack.
- 9.3 The *Contractor* shall ensure that access to system logs and monitoring information is strictly restricted to those people who need to access these to Provide the Service and protect the integrity of the Service Assets.
- 9.4 The *Contractor* shall ensure that any monitoring process complies with the monitoring strategy developed in accordance with Paragraphs 9.1 and 9.2 and all of its legal and regulatory obligations pursuant to applicable law.
- 9.5 The *Contractor* shall maintain a log of:
- (a) all instances of the *Contractor's* people accessing Data;
  - (b) all Service Recipient, TfL people and *Contractor* people logon attempts, successful and failed, to the Service Assets or any elements of the *Contractor* Solution requiring authentication;
  - (c) all actions taken by Service Recipients, TfL people or *Contractor* people with administrative privileges;
  - (d) all instances of accounts being created for Service Recipients, TfL people or *Contractor* people and their relevant privileges;

- (e) all records of formal staff induction or certification required by *Contractor* people to operate systems and handle TFL RESTRICTED Data (where required);
  - (f) all instances of accounts for Service Recipients, TfL people, or *Contractor* Personnel being deleted;
  - (g) *Contractor* people system access group memberships in relation to relevant Service Assets;
  - (h) Service Recipient and group privilege changes against each of the system resources;
  - (i) unauthorised use of input and output devices and removable media; and
  - (j) all access to log files and audit systems.
- 9.6 The logs required must be raw logs, which are provided in a structured text format and the schema for such logs will need to be provided.
- 9.7 The *Contractor* shall implement recording mechanisms to identify the Parties people and their actions when cases of misuse are being investigated and shall ensure that any such recording mechanisms are protected against manipulation and disruption.
- 9.8 The *Contractor* shall regularly review logs to identify anomalies, suspicious activity and suspected Security Incidents. The *Contractor* shall notify the Service Manager of such findings in accordance with Paragraph 8.2.
- 9.9 The *Contractor* shall provide copies of any log data collected by the *Contractor* whilst Providing the Service (system audit log data) at the *Service Manager's* request in a human readable electronic format such as comma-separated value or Microsoft Excel.

## **10. MALICIOUS SOFTWARE**

- 10.1 The *Contractor* shall throughout the Term, use the latest versions of anti-malware solutions and software available from an industry accepted vendor (unless otherwise agreed by the Service Manager) to check for, contain the spread of, and minimise the impact of Malicious Software in the IT Services.
- 10.2 Notwithstanding Clause 10.1, if Malicious Software is detected within services provided by the *Contractor*, the *Contractor* shall ensure the effect of the Malicious Software is mitigated and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Data, restore the Service Assets to their desired operating efficiency.

10.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Clause 10.2 shall be borne by the Parties as follows:

- (a) by the *Contractor* if the Malicious Software originates from the *Contractor* Software, the Third Party Software supplied by the *Contractor* (except where TfL has waived the obligation set out in Clause 10.11) or TfL Data (whilst TfL Data was under the control of the *Contractor*) unless the *Contractor* can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by TfL when provided to the *Contractor*; and
- (b) otherwise by TfL.

## 11. **REMOVABLE MEDIA**

11.1 The *Contractor* may only use Removable Media to support Providing the Service if it has obtained prior written consent of the Service Manager and has implemented appropriate controls to ensure that the use of any input or output devices and removable media is restricted strictly to that needed to supply and support Providing the Service.

11.2 If Removable Media is approved for use by the Service Manager, the *Contractor* shall ensure that it deploys suitable anti-virus and anti-malware checking solutions to actively scan for the introduction of Malware onto systems and networks through all Data imports and exports from removable media and that the removable media is encrypted to a suitable standard agreed in advance with the Service Manager.

11.3 The *Contractor* shall report any loss or interception of Data as a result of the use of removable media to TfL in accordance with Section 8 of this appendix to the Scope. The *Client* reserves the right in such instances to rescind its approval in relation to the *Contractor's* continued use of Removable Media.

## 12. **MOBILE AND HOME WORKING**

12.1 The *Contractor* may only use mobile and home working to support Providing the Service if it has obtained prior written consent of TfL.

12.2 If such consent is granted but the *Contractor* does not have a home and mobile policy for *its* people, TfL's Home and Mobile Working Cyber Security Policy shall apply to the *Contractor* and its people.

12.3 If the *Contractor* has a home and mobile working policy in relation to its people, the *Contractor* shall ensure through this policy that:

# Transport for London

- (a) data is protected and suitably encrypted in line with Cyber Security Policy (see Annex 5), when stored outside of the *service areas*;
  - (b) data is protected when accessed, imported or exported through a connection other than one which is accessed at the *service areas*; and
  - (c) Security Incident management plans acknowledge the increased risk posed by home and mobile working such as theft or loss of Data and/or devices.
- 12.4 The *Contractor* shall report any loss or interception of Data as a result of home or mobile working to the *Service Manager* in accordance with Clause 8.

## 13. **DISPOSALS**

- 13.1 The *Contractor* shall not reuse any Service Asset or Removable Media used in Providing the Service unless such items have been wiped securely in accordance with a standard approved by the *Service Manager*.
- 13.2 The *Contractor* shall securely dispose of and delete Data from Service Assets used for Providing the Service to a standard approved by the Service Manager upon the termination or expiry of the contract or when such Service Assets are no longer required, whichever is sooner, and shall document the disposal and deletion accordingly.
- 13.3 The *Contractor* shall ensure that the disposal of any Service Asset is accurately reflected in the Information Asset Register.

## 14. **SECURITY MANAGEMENT PLAN**

- 14.1 The Outline Security Management Plan as at the *starting date* is set out at Annex 1 (*Outline Security Management Plan*).
- 14.2 The *Contractor* shall within fifteen (15) days of the *starting date* submit to the Service Manager for approval, a draft Security Management Plan which at minimum will:
- (a) set out the security measures to be implemented and maintained by the *Contractor* in relation to all aspects of the Service Assets and all processes associated with Providing the Service and shall at all times comply with and specify security measures and procedures which are sufficient to ensure the Service Assets comply with this appendix to the Scope;
  - (b) reference and comply with the security requirements set out in Annex 3;

- (c) state any other cyber security industry standards over and above those set out in this appendix to the Scope which are applicable to the Service Assets or Providing the Service;
- (d) state all applicable law which relates to the security of the Service Assets; and
- (e) set out how the *Contractor* will comply with any other security requirements the *Client* may reasonably request from time to time.

When the Security Management Plan is approved by the *Service Manager* the approved plan will replace the Outline Security Management Plan in Annex 1.

14.3 The *Contractor* shall review and update the Security Management Plan at least annually and as required in response to:

- (a) changes to the Cyber Security Standards;
- (b) emerging changes in Good Industry Practice;
- (c) any relevant change to the Scope;
- (d) any new perceived or changed security threats; and
- (e) an instruction by the Service Manager.

14.4 The *Contractor* shall submit any amendments to the Security Management Plan to the Service Manager for approval.

## **15. INFORMATION SECURITY MANAGEMENT SYSTEM**

15.1 The *Contractor* shall develop, implement, operate, maintain the ISMS and shall within fifteen (15) Working Days of the Effective Date submit a draft ISMS to TfL. The *Contractor* shall ensure that the ISMS includes the Security Incident Management Process, dealing with, among other matters, Security Incident management.

15.2 The ISMS shall, unless otherwise specified by TfL in writing, be designed to protect all aspects of:

- (a) the Services;
- (b) all processes associated with the delivery of the Services; and
- (c) TfL Sites, the *Contractor* Solution and any information and Data (including TfL Confidential Information and TfL Data) to the extent used by TfL or the *Contractor* in connection with this Agreement.

- 15.3 The *Contractor* shall make any document referenced in the ISMS available to TfL upon request.
- 15.4 If the investigation of a Security Incident reveals weaknesses or flaws in the ISMS, then any change to the ISMS to remedy the weakness or flaw shall be submitted to TfL for approval in accordance with the Variation procedure set out in this Agreement for the avoidance of doubt, if a change needs to be made to the ISMS to address an instance of non-compliance with the Security Management Plan or security requirements, the change to the ISMS shall be at no cost to TfL.
- 15.5 The ISMS will be fully reviewed in accordance with ISO/IEC 27001 by the *Contractor* at least annually, or from time to time as agreed with TfL, in response to:
- (a) changes to Good Industry Practice;
  - (b) any relevant Operational Changes or Variations or proposed Operational Changes or Variations to the Services and/or associated processes;
  - (c) any new perceived or changed security threats; and
  - (d) any reasonable request by TfL.
- 15.6 The *Contractor* shall provide the results of such reviews to TfL (together with such related information as TfL may reasonably request) as soon as reasonably practicable after their completion. The results of the review should include, without limitation:
- (a) suggested improvements to the effectiveness of the ISMS;
  - (b) updates to the risk assessments;
  - (c) proposed modifications to the procedures and controls that affect the ability to respond to events that may impact on the ISMS; and
  - (d) suggested improvements in measuring the effectiveness of controls.

## **16. COMPLIANCE WITH ISO/IEC 27001**

- 16.1 The *Contractor* shall obtain certification from a UKAS registered organisation of the ISMS to ISO/IEC 27001 for any aspects of the business that is necessary to support the Services. The *Contractor* shall obtain such certification within twelve (12) months of the Effective Date and shall maintain such certification throughout the Term.
- 16.2 If certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27001 and Schedule 2.3 (*Standards*) the *Contractor* shall promptly notify TfL of this.



- 16.3 Without prejudice to any other audit rights set out in this Agreement TfL may carry out, or appoint an independent auditor to carry out, such regular security audits as may be required in accordance with Good Industry Practice in order to ensure that the ISMS maintains compliance with the principles and practices of ISO/IEC27001.
- 16.4 If on the basis of evidence provided by such audits, TfL, acting reasonably, considers that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the *Contractor*, then TfL shall notify the *Contractor* of the same and the *Contractor* shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such non-compliance as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement.

## **17. APPROVED PRODUCTS**

- 17.1 The *Contractor* shall ensure that all Service Assets providing security enforcing functionality are certified under the CESG Commercial Product Assurance (CPA) Scheme, to the appropriate grade, as defined with Annex 3 “Security Requirements”, provided that relevant certified products are available in the market.
- 17.2 If a product is not assured under the CPA scheme, TfL reserves the right to require bespoke assurance of that product under a recognised scheme such as CESG Tailored Assurance Service (CTAS).



**ANNEX 1 – OUTLINE SECURITY MANAGEMENT PLAN/SECURITY  
MANAGEMENT PLAN** See *Blue Systems Data Security Policy attached to  
the Tender*

**Blue Systems**

**(a BLUECARSHARING brand)**

## **DATA SECURITY POLICY**

**January 2020**

*Confidential*

1



## 2. [REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED] ■ [REDACTED]  
[REDACTED]

[REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]

\_\_\_\_\_

[REDACTED]

[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.2 [redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

[redacted]

[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

[redacted]  
[redacted]  
[redacted]

[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

[redacted]

[redacted]  
[redacted]

[Redacted text block]

- [Redacted text block]
- [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]

- [Redacted text block]
- [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]
  - [Redacted list item]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

1.7 [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted] [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
  
[Redacted]  
[Redacted]  
[Redacted]  
  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted] [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[REDACTED]

[REDACTED]

## 7. [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



# Transport for London

1.1

The service users' accounts are managed by Blue Systems  
Application access is protected

The underlying infrastructure is managed by Blue Systems

- [Redacted]
- [Redacted]

1.13

## 8. [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

- [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]  
[REDACTED]
- [REDACTED];
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.16

[REDACTED]

1.18

[REDACTED]

■

- [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

1.19

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

- [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

1.22 [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

[REDACTED]:

- [REDACTED]  
[REDACTED]
- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]  
[REDACTED]

- [REDACTED]

[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED] ■ [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]
  - [REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]



## Transport for London

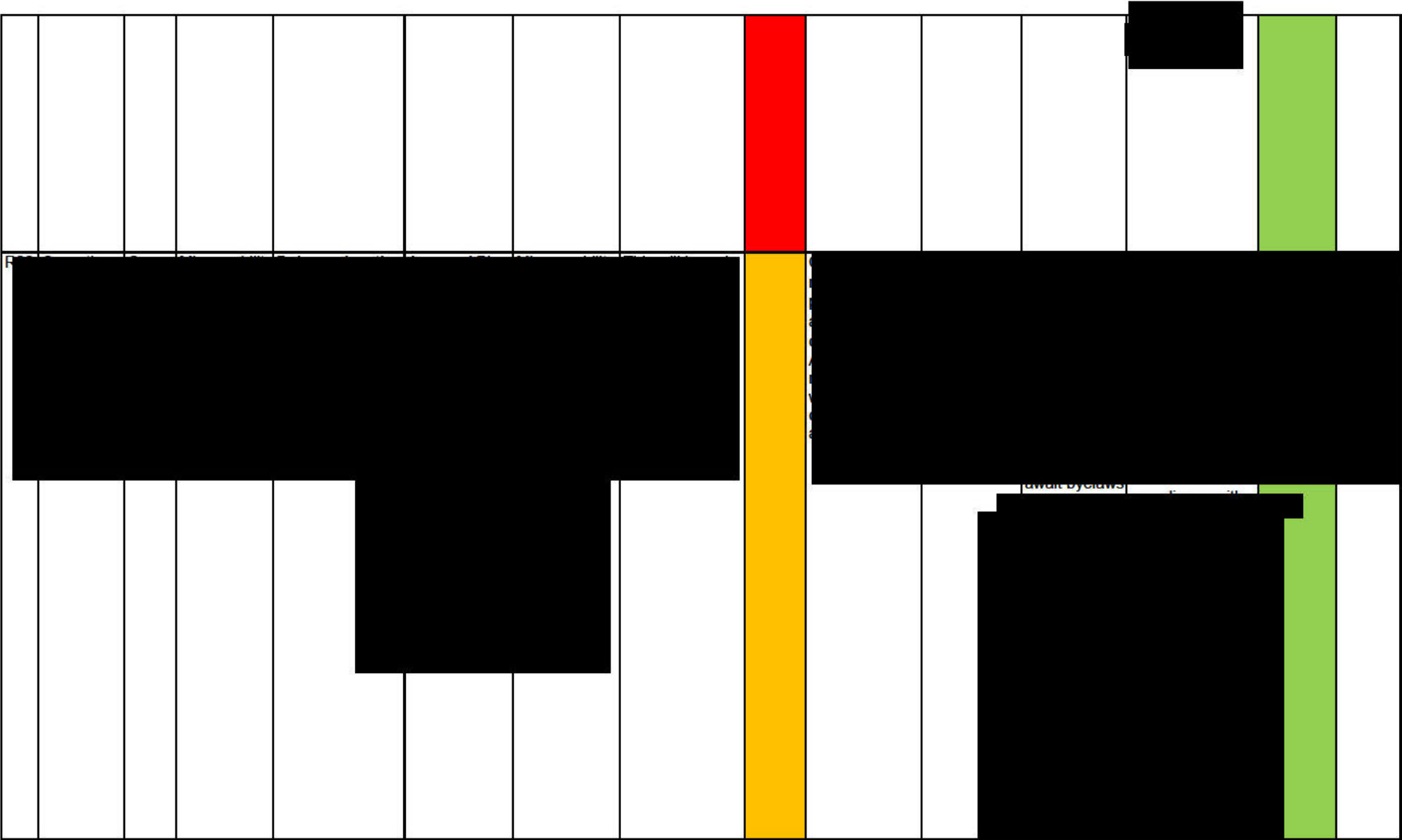
## ANNEX 2 – OUTLINE RISK MANAGEMENT PROCESS

**See Annex 1 Blue Systems Data Security Policy as well as Risk Mitigation Plan attached to the Tender**

Transport for London – Invitation to Tender										Project Reference Number: tfl scp 002004					
Risk No	Type	Risk Status	Risk Owner	Risk Title	Cause	Event	Impact	Current Rating	Best Case	Most Likely Case	Worst Case	Mitigation Action	Post-Mitigation Rating	Action Owner	



Transport for London



# Transport for London

[illegible]

## Transport for London

[illegible]

## Transport for London



## Transport for London

Date	Time	Location	Observer	Weather	Wind	Temp	Humidity	Pressure	Visibility	Clouds	Moon	Stars	Planets	Other	Observations	
															Notes	Sketches
1950-01-01	00:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	01:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	02:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	03:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	04:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	05:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	06:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	07:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	08:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	09:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	10:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	11:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	12:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	13:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	14:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	15:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	16:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	17:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	18:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	19:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	20:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	21:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	22:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2	10	0	0	0	0	0	Star visible at 100°E, 10°N	
1950-01-01	23:00	100°E, 10°N	W. H. L.	Clear	0	25.0	75	1013.2								

## ANNEX 3 – SECURITY REQUIREMENTS

Ref	Item	Guidance for Completion
1	Cloud Service	Details of the Tenderer's proposed cloud service and provider to be used for this contract: name of the proposed provider; and length of contract with the cloud provider.
2	Cloud Provider Service	Details of the Tenderer's service with the proposed cloud provider; and details of whether a SaaS, IaaS or PaaS service will be used.
3	Cloud Provider Audit	Details on the frequency of audits on the proposed cloud provider (e.g. annually, six monthly); details of the organisation(s) appointed by the Tenderer to conduct audits, including the rationale for selecting such organisations; details of the Tenderer's audit processes on the proposed cloud provider; and details of how audit findings will be reported.
4	Data Centres	Details of the Tenderer's data centres for the contract including their location.

## Transport for London

5	Penetration ("pen") Test	Details of who will conduct the pen tests; how often the pen tests will be conducted on the proposed cloud service (note: A CREST/TIGER approved provider must be used); and as applicable, details of the following activities: cyber security factory acceptance testing; cyber security site acceptance testing; cyber security functional testing; pen testing; vulnerability scanning and code reviews; and cyber security verification and validation activities.	
---	--------------------------	---	--

Ref	Item	Guidance for Completion	Response
6	Administrative Controls	Details of the Tenderer's administrative controls for the proposed cloud service, including: timeout systems; break glass protocol (i.e. processes implemented to provide a quick means for an individual to access privileged information); and administrative control processes for new joiners and leavers.	

## Transport for London

7	Subcontractor Access	Details of the service the Tenderer's Subcontractor will be providing; details of the Tenderer's Subcontractor's access to their proposed cloud and potential impacts to TfL data and systems for the proposed contract; details of what control measures the Tenderer will implement on their Subcontractors and them accessing TfL's data; and details about whether the Subcontractors are part of the Tenderer's proposed solution.	
8	Service Changes & Compromised Data	Details of the Tenderer's change controls and processes in providing the service; details of how system changes will be detected and dealt with; and details of the Tenderer's communication and reporting procedures when system changes are detected.	
9	Encryption Level	Details of the Tenderer's proposed encryption levels for data in transit and at rest; and encryption levels that will adhere to TfL's Cyber Security policies.	

Ref	Item	Guidance for Completion	Response
-----	------	-------------------------	----------



## Transport for London

10	Password Controls	Details of the Tenderer's proposed password controls and the rationale for these controls (e.g. how often do passwords need to be changed and how passwords are reset); details of any additional measures the Tenderer will implement to make access to its systems more secure; and how Tenderer's will ensure adherence to TfL's Cyber Security policies.	[REDACTED]
11	MFA (Multi Factor Authentication)	Details of whether the Tenderer will enable MFA for the proposed contract, including: where MFA will be enabled; who will use MFA; and the MFA change policy.	[REDACTED]
12	Information Risk Management	Positive information risk management program attributes include: establishes a governance framework; determines the organisation's risk appetite; maintains the board's engagement with information risk; produces supporting policies; adopts a lifecycle approach to information risk management; applies recognised standards; makes use of endorsed assurance schemes; educates users and maintains their awareness; promotes a risk management culture; reference to the National Cyber Security Centre guidance; and provides copies of certificates (e.g. ISO, PCI DSS (Payment Card Industry Data Security Standards), cyber essentials, clearly stating dates, names and reference numbers).	[REDACTED]

# Transport for London

Ref	Item	Guidance for Completion	Response
13	Secure Configuration	Positive attributes include: uses vendor supported software; develops and implements policies to update and patch systems; creates and maintains hardware and software inventories; hardens systems and software; conducts regular vulnerability scans; establishes configuration control and management; disables unnecessary peripheral devices and removable media access; implements application whitelisting and execution control; limits user ability to change configuration; limits privileged user functionality; reference to the National Cyber Security Centre guidance; and provides copies of certificates (e.g. ISO, PCI DSS (Payment Card Industry Data Security Standards), cyber essentials, clearly stating dates, names and reference numbers).	

## Transport for London

14	Network Security	Positive attributes include: uses firewalls (including nextgeneration firewalls where appropriate); uses intrusion protection/detection tools; prevents malicious content both at the network perimeter and internally; implements network segregation; segregates production and management networks; manages the solution via jump servers; scures wireless devices; enables secure administration; configures exception handling processes; provides a network monitoring capability; conducts regular penetration tests; reference to the National Cyber Security Centre guidance; and provides copies of certificates (e.g. ISO, PCI DSS (Payment Card Industry Data Security Standards), cyber essentials, clearly stating dates, names and reference numbers).
----	------------------	---

Ref	Item	Guidance for Completion
15	Managing User Privileges	Positive attributes include: establishes effective account management processes; establishes policy and standards for user identification and access control; limits user privileges; limits the number and use of privileged accounts; monitors user activity; limits access to the audit system and the system activity logs; educates users and maintain their awareness of acceptable account use; and reference to the National Cyber Security Centre guidance.

# Transport for London

16	User Education and Awareness	Positive attributes include: produces a user security policy; establishes a staff induction process; maintains user awareness of the cyber risks faced by the organisation; supports the formal assessment of security skills; monitors the effectiveness of security training; promotes an incident reporting culture; establishes a formal disciplinary process for breaches of security; and reference to the National Cyber Security Centre guidance.	
----	------------------------------	---	--

Ref	Item	Guidance for Completion	
-----	------	-------------------------	--


## Transport for London

17	Security Incident Management	Positive attributes include: establishes an incident response capability; provides specialist training (i.e. where necessary to ensure that the incident response team have the specialist knowledge and expertise required); defines the required roles and responsibilities of those who will handle ICT incidents; establishes a data recovery capability; tests the incident management plan; decides what information will be shared and with whom; collects and analyses post-incident evidence; conducts a lessons learnt review; educates users and maintains their awareness (i.e. of their responsibilities in relation to reporting security weaknesses or incidents as soon as possible (without fear of recrimination)); reports criminal incidents to relevant organisations (e.g. law enforcement agencies); reference to the National Cyber Security Centre guidance; and provides copies of certificates (e.g. ISO, PCI DSS (Payment Card Industry Data Security Standards), cyber essentials, clearly stating dates, names and reference numbers).	
----	------------------------------	--	--

Ref	Item	Guidance for Completion	Response
-----	------	-------------------------	----------



## Transport for London

18	Malware Prevention	Positive attributes include: develops and implements malware prevention policies to stop cyber attacks; manages all data import and export; blacklists malicious or potentially malicious websites, blocking access to users; provides dedicated removable media scanning machines; establishes appropriate malware defences across the organisation; educates users and maintain their awareness; reference to the National Cyber Security Centre guidance; and provides copies of certificates (e.g. ISO, PCI DSS (Payment Card Industry Data Security Standards), cyber essentials, clearly stating dates, names and reference numbers).	
----	--------------------	---	---

## Transport for London

Ref	Item	Guidance for Completion	
19	Security Monitoring	Positive attributes include: establishes a monitoring strategy and supporting policies; monitors all systems; monitors network traffic; monitors user activity; tests compliance with policies and procedures to ensure monitoring processes are legally compliant and/or comply with regulatory constraints; fine-tunes monitoring systems; establishes a centralised collection and analysis capability; provides resilient and synchronised timing; trains the security personnel in how to monitor the systems; aligns security monitoring policies and practices with incident management policies and practices; conducts a lessons learnt reviews; reference to the National Cyber Security Centre guidance; and provides copies of certificates (e.g. ISO, PCI DSS (Payment Card Industry Data Security Standards), cyber essentials, clearly stating dates, names and reference numbers).	

Ref	Item	Guidance for Completion	Response
-----	------	-------------------------	----------

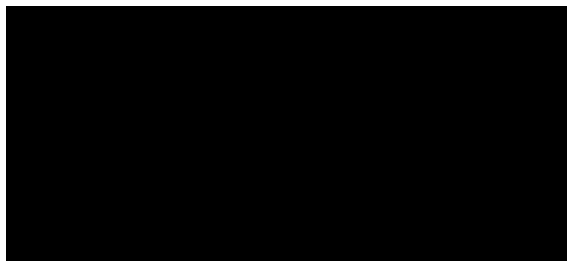
# Transport for London

20	Removable Media	Positive attributes include: produces and evidences corporate policies, processes and solutions to control the use of removable media for the import and export of information; limits the use of removable media to only essential use (where no other option is available); scans all media for malware; formally issues media to users; audits media holdings regularly; encrypts the information held on the media; locks down access to media drives; monitors the use of removable media; actively manages the reuse and secure disposal of removable media; educates users on the use of removable media and maintain their awareness; and reference to the National Cyber Security Centre guidance.	[REDACTED]
21	Home and Mobile Working	Positive attributes include: assesses the risks and creation of a mobile working security policy; educates users and maintains their awareness on these policies; applies the secure baseline build; protects data at rest when mobile working; protects data in transit when mobile working; incorporates home and mobile working in incident management; and reference to the National Cyber Security Centre guidance.	[REDACTED]



## ANNEX 4 – CONFIGURATION MANAGEMENT OF SERVICE ASSETS

[REDACTED]



## ANNEX 5 – LIST OF RELEVANT POLICIES

### TO BE PROVIDED BY TFL UPON REQUEST

- **Network Security Policy** defines the requirements for securing TfL networks as well as the information and network specific devices on them.
- **System Access Control Policy** defines the requirements for managing user and system account access to applications and technology such as allowing them to sign in to OneLondon or SAP.
- **Cyber Security Incident Management Policy** defines how we will handle cyber security incidents and the requirements for reporting and managing those incidents.
- **Malware Prevention Policy** defines the requirements for helping to prevent malware (malicious software e.g. computer viruses) from infecting our systems and networks.
- **Security Logging, Monitoring and Audit Policy** details the requirements for security logging and monitoring of access to our technology and data and the audit capabilities.
- **Removable Media Policy** details the requirements for using removable media such as USBs, CDs or portable hard drives.
- **Home and Mobile Working Cyber Security Policy** details the requirements for allowing and supporting secure home and mobile working.
- **Third Party Cyber Security Policy** defines the rules governing how the security of third party custodians of TfL information, technology and third party connections to TfL systems will be ensured.
- **TfL Information Security Classification Standard** details the information security classification scheme covering information and records, in all formats, and the minimum requirements for managing such information
- **10 Steps to Cyber Security** can be found at <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary>
- **Cyber Essentials Scheme** can be found at <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>

# Transport for London

- **Security Patching Standard** details the requirements for applying security-related updates ('security patches') in order to help secure TTL systems and applications in line with the secure builds and configurations policy.
- **Operations Technology Cyber Security Standard** describes the cyber security requirements for operational technology assets throughout their lifecycle

## SCHEDULE 3A – SPECIFICATION

# **SURFACE TRANSPORT INVITATION TO TENDER**

**FOR**

## **Micromobility Management System Pilot VOLUME 2 SPECIFICATION**

---

**Project Reference Number: tfl\_scp\_002004**

---

*Copyright on the whole and every part of this document is owned by Transport for London. No reproduction of the whole or any part of this document is to be made without the authority of Transport for London.*

# Transport for London

## Table of Contents

<b>1.</b>	<b>ORGANISATIONAL OVERVIEW .....</b>	<b>129</b>
1.1.	Transport for London (TfL)	129
1.2.	Business Unit	129
<b>2.</b>	<b>INTRODUCTION.....</b>	<b>129</b>
2.1.	Background	129
2.2.	Objectives	130
<b>3.</b>	<b>SCOPE 131</b>	
3.1.	General Requirement	131
<b>4.</b>	<b>DELIVERABLES / MILESTONES .....</b>	<b>133</b>
<b>5.</b>	<b>SERVICE LEVEL AGREEMENTS (SLAS).....</b>	<b>135</b>
5.1.	SLAs	135
5.2.	General requirements	135
<b>6.</b>	<b>PROJECT PLAN/TIMESCALES .....</b>	<b>136</b>
	<b>APPENDIX 1 - SUMMARY OF REQUIREMENTS .....</b>	<b>137</b>

# Transport for London

## 1. ORGANISATIONAL OVERVIEW

### 1.1. Transport for London (TfL)

TfL was created in 2000 as the integrated body responsible for London's transport system. TfL is a functional body of the Greater London Authority. Its primary role is to implement the Mayor of London's Transport Strategy and manage transport services to, from and within London.

TfL manages London's buses, the Tube network, Docklands Light Railway, Overground and Trams. TfL also runs Santander Cycles, London River Services, Victoria Coach Station, the Emirates Air Line and London Transport Museum. As well as controlling a 580km network of main roads and the city's 6,000 traffic lights, TfL also regulates London's taxis and private hire vehicles and the Congestion Charge scheme.

Further background on what TfL does can be found on the TfL website here: <https://tfl.gov.uk/corporate/about-tfl/what-we-do>

### 1.2. Business Unit

The Transport Innovation Directorate sits within Surface Transport. Our role is to make sure transport in London is ready for the future. We actively seek out and assess new ideas and developments in the transport world, helping TfL to determine which new business models or services could help us address the challenges facing our city. We engage with market innovators, test how new ideas could work for London and set the policy frameworks to ensure new innovations are integrated and work for all.

The Transport Innovation Directorate sits within the Surface Transport Unit which has overall responsibility for the road and bus network and is responsible for delivering contracted transport services including buses, trains and trams. This unit also leads efforts to make London's streets and transport safe and secure, including the organisation's [Vision Zero](#) commitment to eliminate all deaths and serious injuries, increase active travel, and reduce congestion and emissions, including the Ultra Low Emission Zone. It is essential that all areas of Surface Transport work holistically both from a data and an operations stand-point.

## 2. INTRODUCTION

### 2.1. Background

TfL and London boroughs have limited information on trips made by dockless cycles, and limited influence on dockless rental companies despite operators being reliant on public infrastructure. TfL and boroughs need a dynamic view of

how new modes of transport such as dockless rental bikes and e-bikes could help to effectively deliver the Mayor's Transport Strategy goals and avoid the potential dis-benefits of thousands of mobile assets moving around London and causing obstructions in the public realm.

Understanding the impact that dockless cycles have on journeys (whether they are replacing car journeys, complementing public transport journeys or impacting active travel) is necessary to influence investment and policy decisions and promote safety. Data on dockless cycles (such as aggregating origin and destination data and routes taken) could influence decisions in areas like expanding cycle routes/infrastructure, investments in junction safety and influencing operators to expand into areas in need of better active transport options. Two-way data sharing with operators would help TfL understand the current situation, react intelligently, understand what is really going on and communicate up to date network information to operators to ensure that highways are kept clear and safe for all users.

Given the number of providers working with other cities across the world to ingest data from micromobility operators, we now want to develop and deliver a pilot system for London, before considering a longer-term solution.

## 2.2. Objectives

TfL is seeking to deliver proof of concept for a micromobility management system for a number of reasons:

### **To enable Network Performance Managers to prioritise and smooth traffic flows in line with the Mayor's Transport Strategy**

Providing the Network Management Control Centre with near real-time data of where all dockless hire vehicles are in London will vastly increase the amount of information they have about how these vehicles are being used in the city. This will inform decision-making to the benefit of cyclists, pedestrians and other road users.

### **To complement existing aggregated and anonymous data sets that TfL and boroughs use to inform long-term planning, policy and investment decisions**

TfL doesn't have much information about how people use rental bicycles in London. Data on how people use dockless hire bikes would allow TfL to analyse route choices, popular locations for hiring and ending hires, etc. and use this data to inform future policy decisions in relation to cycling, and planning and investment on cycling infrastructure, junction safety etc.

## **To allow TfL and London boroughs to ensure compliance with the Greater London Dockless Vehicle Byelaws, and therefore ensure responsible parking of dockless vehicles**

Access to real-time data from micromobility operators will allow TfL and boroughs to see the locations of dockless vehicles all over London and validate compliance with the parking requirements in the Byelaws. The Byelaws are due to come into force mid-2020. This data will facilitate informed discussions with operators. Ultimately, being better informed about where these vehicles are parked is essential for TfL and boroughs being able to ensure responsible parking and keeping streets clear and safe for all users.

## **To support enforcement teams and relieve the burden of new vehicles on enforcement officers**

Real-time operator data and the ability to see where dockless vehicles are on a map of London will allow for a more targeted approach to enforcement. This will help reduce the impact for enforcement teams of an unlimited number of dockless bikes and the potential legalisation of e-scooters, which would likely see a large increase in the number of dockless vehicles on London's streets.

## **To support TfL's ongoing relationship with operators, and ensure that TfL and boroughs have access to the data they need as data needs evolve**

There is also an opportunity to explore other new transport business models as they appear.

### **3. SCOPE**

#### **General Requirement**

This contract is for a provider to deliver an 18-month data-sharing pilot between micromobility operators in London and TfL, with several London boroughs participating as users.

The Provider shall develop the necessary Application Programming Interface (APIs) to enable two-way data sharing between micromobility operators on the one hand, and TfL and London boroughs on the other.

The Provider shall ingest from operator's data such as verifiable near real-time data (up to one minute latency) on the locations of all dockless micromobility hire vehicles in London (with unique identifiers, vehicle type and propulsion type for each vehicle), their statuses (available for hire/out of service), and journey start and journey end data. The Provider's solution shall share this near real-time data with TfL and the participating boroughs. The Provider's solution shall include functionality to allow TfL and boroughs to download and store historical data for analytical purposes. The Provider's solution shall



# Transport for London

enable TfL and London boroughs to communicate with operators and supply operational information (e.g. network availability information and policy updates).

The Provider's solution and processes must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 or any amendment or re-enactment from time to time or national replacement of such legislation. This includes, but is not limited to, the obligation for 'data minimisation'. The Provider will need to work with TfL in defining the specific scope of data collected from operators and aligning this with clear purposes of use, to ensure we only collect the minimum data required.

The Provider's solution shall include a front-end dashboard mapping data over London, with access provided to TfL, the London boroughs, the City of London, and other public authorities that TfL may nominate during the course of the contract. TfL will use this dynamic view of micromobility vehicles in London to help target resources and on-street activity.

The Provider's solution shall allow users to filter historic and real-time data by operator, by vehicle type, by propulsion type, by borough, by time and by other categories as request by TfL/boroughs over the course of the contract. The Provider shall ensure that each individual user is required to complete a secure log-in process to gain access to the system, and shall implement role-based access controls, to ensure users only access information which they are authorised to do so.

Over the course of the contract new operators, micromobility modes or other new transport solutions may arrive in London, or TfL may want to be able to collect data on other measures. This could include new data sets that become available as technology develops, such as the ability to ingest and share 'swerve' data should vehicles be fitted with gyroscopes or other technology capable of communicating such data. The Provider's solution should be scalable and come with the option of adding further standard features or developing customised features.

The Provider shall bring their experience working with a large and complex city like London, with multiple levels of government. London has one Mayor and a strategic transport authority (Transport for London), but it also has 33 individual boroughs, and those boroughs are highways authorities for their own road networks. TfL is leading this pilot but has invited boroughs to register interest in taking part as users. The Provider shall support TfL in onboarding boroughs to the pilot and providing technical support to all users throughout the pilot.

During this pilot, the Provider shall obtain the required data such as Mobility Data Specification (MDS) or General Bikeshare Feed Specification (GBFS) data) from operators and share it with TfL and all participating boroughs in a way that is compliant with data protection legislation, including the GDPR, and agreed security standards, always carefully balancing the privacy of micromobility service users with TfL and borough data needs. Over the course of the pilot, the Provider shall support TfL's ongoing relationship with operators, and ensure that TfL and boroughs have access to the data they need as data needs evolve.

The Provider's solution should be compatible with a range of devices, including desktops, laptops, tablets, and smartphones.

The Provider shall provide training to TfL and borough users upon deployment of the solution, as new users are added, and as required for any new features, updates or other changes.

Appendix 1 contains a summary of requirements.

## **4. DELIVERABLES / MILESTONES**

The pilot will run for 18 months. We expect to go live in May/June 2020.

The initial period after the contract commences will be important for mobilisation. Within 14 days of the Contract Date the Provider shall have appointed an account manager, produced a programme plan and have presented it to TfL.

Within six weeks of the Contract Date the Provider shall:

- Have overlaid a dashboard/platform over a map of London that is consistent with those used by TfL and our partners and have started to ingest data from existing micromobility operators
- Have gone live with the following standard features: view of fleet by operator including the real-time locations, unique identifiers, vehicle types and propulsion types of those vehicles, journey start and end locations and vehicle status (available for hire/out-of-use).
- Have onboarded the boroughs that will be taking part in the pilot
- Have agreed workflows with TfL analysts/data experts and borough nominees, which TfL will facilitate.
- Have provided a data management report (exact requirements to be agreed but to include the number of ping data points, number of derived data points, data quality (source) and data quality (sent to TfL/boroughs))

# Transport for London

- Once TfL is satisfied that the provider has delivered a minimum viable product (including having enabled data-sharing with existing TfL systems) on a daily basis the Provider shall refresh any data that is not real-time.

On a monthly basis after month one the Provider shall:

- Produce a report showing monthly summaries and trends. TfL will define the exact requirements of these reports before the first report is due and will refine the requirements subject to business need over the course of the contract.

After three months the Provider shall:

- In partnership with TfL, have identified and resolved any issues in data-sharing agreements with micromobility operators

Over the course of the 18-month pilot the Provider shall:

- Have the ability to add further standard features or develop customised features
- Have the ability to ingest and share with TfL/boroughs data from additional dockless bike operators, or any operators of a new transport solution that TfL wants to be able to collect MDS-standard or similar data from.

## 5. SERVICE LEVEL AGREEMENTS (SLAS)

### 5.1. SLAs

Over the course of the pilot, for the purposes of tracking and monitoring progress, a number of SLAs are envisaged. They are likely to include:

Description	Service Level
Regularity of receiving data from operators	<ul style="list-style-type: none"><li>• Daily refreshing of data that isn't real-time for analytical purposes</li></ul>
Agreed response and repair times if the system experiences issues/bugs	<ul style="list-style-type: none"><li>• Technical support response times and channels to be agreed before contract is signed</li><li>• Ongoing support to be available</li></ul>
Advance notice of deploying any service impacting modifications (excluding emergency patches/fixes).	<ul style="list-style-type: none"><li>• Notification period to be agreed within 7 days of the Contract Date</li></ul>
Advance notice of releasing any major improvements or enhancements to the System, including a description of the intended improvements or enhancements.	<ul style="list-style-type: none"><li>• Notification period to be agreed within 7 days of the Contract Date</li></ul>
A regular meeting/call with the account manager.	<ul style="list-style-type: none"><li>• Weekly</li></ul>

TfL expects a minimum viable product to be fully functional within six weeks of the Contract Date.

The precise nature of SLAs and their reporting frequencies will be subject to the exact solution that is procured and will be subject to agreement within 7 days of the Contract Date, with the possibility for review during the course of the pilot (with the first review point at 6 months).

### 5.2. General requirements

As well as SLAs such as those set out above, the Provider will be subject to service requirements such as:

# Transport for London

Description	Measure
Ongoing compliance with all data protection legislation and agreed security standards including GDPR	<ul style="list-style-type: none"><li>• To be regularly reviewed with the account manager and TfL's privacy team.</li><li>• Regularity to be agreed within 7 days of the Contract Date</li></ul>
Reporting meetings	<ul style="list-style-type: none"><li>• Account manager, TfL policy and relevant technical experts to be in attendance.</li><li>• Regularity and exact requirements to be agreed within 7 days of the Contract Date</li></ul>

## 6. PROJECT PLAN/TIMESCALES

TfL anticipates regular meetings between the account manager and the policy and technical leads in TfL, and regular reports on findings/trends/issues. The regularity and specific details of these meetings will be agreed within 7 days of the Contract Date.

*May/June 2021:* consider the long-term legacy of the pilot and agree transitional arrangements. We expect the Provider to be part of this review process.

*November/December 2021:* pilot ends and transitional arrangements are in place. The Provider shall produce an end of pilot review report, the exact requirements of which will be determined by TfL before the end of the pilot.



## APPENDIX 1 - SUMMARY OF REQUIREMENTS

- Develop Application Programming Interface (APIs) to enable two-way data sharing between micromobility operators and TfL/London borough users.
- Solution must be able to ingest as near as possible to real-time data and share this with TfL/boroughs within one minute of receiving the data.
- Required data from operators:
  - locations of all dockless micromobility hire vehicles
  - unique vehicle identifiers
  - vehicle type for each vehicle
  - propulsion type for each vehicle
  - vehicle status (available for hire/out of service)
  - journey start data
  - journey end data
- Develop a front-end dashboard displaying this data to users. Users shall be provided with secure, role-based access and shall be able to filter historic and real-time data by:
  - operator
  - vehicle type
  - propulsion type
  - borough
  - time
  - any other categories as request by TfL/boroughs over the course of the contract.
- Data can be downloaded and stored by TfL and boroughs as needed for analytical purposes.
- TfL and London boroughs able to communicate with operators and supply operational information (e.g. network availability information and policy updates)
- The solution should be scalable and come with the option of adding further standard features or developing customised features.
- The Provider shall support TfL in onboarding boroughs to the pilot and providing technical support to all users throughout the pilot.
- The Provider shall support TfL's ongoing relationship with operators and ensure that TfL and boroughs have access to the data they need as data needs evolve.
- The Provider should use a standard data format such as Mobility Data Specification (MDS) or General Bikeshare Feed Specification (GBFS)
- The Provider's solution should be compatible with a range of devices, including desktops, laptops, tablets, and smartphones.

# Transport for London

- The Provider shall provide training to TfL and borough users at the start of the contract, as new users are added, and as required for any new features, updates or other changes.
- Compliance with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 or any amendment or re-enactment from time to time or national replacement of such legislation.
- 'Data minimisation': The Provider will need to work with TfL in defining the specific scope of data collected from operators and aligning this with clear purposes of use, to ensure collection of the minimum data required.



tfl\_scp\_002004

## SCHEDULE 3B – SUPPLIER'S RESPONSE

Transport for London – Invitation to Tender

Project Reference Number:

Micro mobility Management System Pilot

Name, address and the phone number of the company	Bluecarsharing SAS d/b/a Blue Systems 23, rue du Professeur Victor Pauchet 94420 Vaucresson - France
Contact Person	[REDACTED] [REDACTED] [REDACTED]
Phone number and email address of the contact person	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

“This page intentionally left blank”



## Table of Contents

INTRODUCTION.....	142
ABOUT BLUE SYSTEMS.....	143
BLUE SYSTEMS EXPERTISE .....	144
OUR REFERENCES .....	145
OUR COMPETITIVE ADVANTAGE .....	146
QUALITY TENDER SUBMISSION.....	147
<b>1. Methodology and Approach</b>	14
a. Working with TfL, local authorities and other stakeholders	14
b. Shaping and sustaining an operating model:	14
c. Development of new features in response to user needs	15
d. Added value to other cities and TfL	15
e. Other possible applications:	15
f. Capability and relevant experience of the key personnel	15
<b>2. Mobilisation</b>	15
a. Work programme overview	15
b. Top 3 key risks (out of 4) potentially encountered during mobilisation	15
c. Mitigation plan for the key risks identified above	15
d. TFL participation to support our mobilisation plan	15
<b>3. Systems and Processes</b>	15
a. Legacy systems and data integration	15
b. Compliance with regulations and best practices	15
c. Use of different data formats	15
d. Different data analytics activity	15
e. Use of an agile process so the system is deployed at speed	15
<b>4. Operator engagement</b>	16
a. Our approach to working with operators	16
b. Our engagement model with the operators, challenges and experience	16
c. Our approach to agreements between cities and operators, and our role	16
<b>5. Demonstration</b>	16
a. Effective user experience for TfL and borough users	16
b. Alignment with data requirements	18
c. Multi-jurisdictional access	18
d. Development of customized features	18
e. Scalability of the solution	19
<b>6. Cyber Security</b>	19
<b>7. Privacy and Data Protection</b>	19

“This page intentionally left blank”

# Introduction

We are pleased to offer Transport for London and our data analytics platform (the “Platform”) as a response to the Invitation to tender #tfl\_scp\_002004 for monitoring micro-mobility providers.

We believe we understand exactly what you are looking to achieve, and the good news is – we have done it before! We have successfully integrated a very similar Platform in cities in the United States and Europe, and now we are eager to share our expertise and experience with Transport for London.

Our fully MDS compliant Mobility Manager platform is now operational in the cities of Los Angeles, and Grand Lyon (France), and about to launch in San Jose, Calif., and we have extensive experience working with mobility operators to obtain data for compliance analytics. We can ensure that we will meet or exceed all your requirements, including:

- [illegible]

## Smart Mobility for Smarter Cities

Blue Systems is a global leader in urban mobility. As an expert in smart mobility and smart city solutions, we provide services and products to empower cities to shape a sustainable future.

Our Platform is a smart city tool that collects real-time information from all micro-mobility providers and suggests ways to regulate operators instantly. At the same time, it also allows the City to analyze past data and create smart policies based on this analysis. It can also be used as a foundation for a Mobility as a Service (MaaS) platform. It can be expanded to monitor and regulate all TNCs, shared bikes, ride-hailing companies, car sharing, freight

# Transport for London

companies and public transportation, as well as emerging technologies like delivery drones and autonomous vehicles.

## *Monitor, Analyze, Plan*

[Redacted]

[Redacted]

[Redacted]

## *Gain Control and Regulate the Entire Mobility Ecosystem*

We are committed to helping Transport for London in its mission to have London become a shared, autonomous, active, safe and sustainable city. We understand that these areas are of critical importance as we develop solutions for urban mobility in the digital age.

The stakes could not be higher, and the time to address these issues is now. The Blue Systems team is excited to put our collective knowledge and expertise to work for you.

Thank you for your consideration.

Sincerely,

**Blue Systems Team**

## **About Blue Systems**

Blue Systems is a global leader in urban mobility and a subsidiary of the Bolloré Group.

# Transport for London

Founded in 1822, the Bolloré Group is one of the 500 largest companies in the world. Blue Systems is one of the three divisions of the Bolloré Group. Blue Systems as a company is part of the Blue Systems division which gathers many companies (“Blue Systems Division”).



Today, the Bolloré Group employs 80,500 employees spread across 143 countries in five continents. Blue Systems has offices in London, Los Angeles, Santa Monica, Indianapolis, Paris, Turin and Singapore.

## Blue Systems Expertise

Having developed a top-notch carsharing services platform that is now in use worldwide, we have built upon this experience by designing a complete Software-as-a-Service platform for the management of shared assets. Today, we offer a wide range of products and services in the field of smart mobility.



# Transport for London

In addition to our smart mobility solutions, we provide consulting services and end-to-end assistance in project management and innovation. We have participated in many ambitious Smart City projects. From consulting to data analytics, we have a very experienced team to meet all of our customers' needs.



We are now working extensively with cities in Europe, the US and around the world to promote MDS and are actively participating in the MDS evolution as one of the very first technology member of the Open Mobility Foundation (“OMF”). We are also a member of UITP – the international organization for public transport authorities, operators and policy makers.



From transportation operator to technology provider and innovation advisor, Blue Systems has turned ideas into innovative products for both its own activities and for other organizations' projects and for DOTs of the largest cities in the world (Los Angeles, London, Paris, Singapore).

## Our References

- Micro-mobility MDS platforms in Europe and the US
- Smart Parking platform, mobility data analytics, enforcement and billing software – (100+ cities, including *Paris, Lille, Strasburg, Lyon, Los Angeles, Singapore, London*)
- Electric shared mobility platform in several cities worldwide – (Los Angeles, Indianapolis, Paris, Lyon, Turin, Singapore, London)
- Electric vehicle charging points and parking platform in all London Boroughs aggregating and managing over 20 mobility operators – (*Source London*)
- Yearly value of all transactions processed by our platforms is over \$700 million   6 million daily active users worldwide

# Transport for London



Today, Blue Systems platforms aggregate and process data from 200,000+ shared vehicles and 400,000+ road assets (parking meters, parking spots, charge points) worldwide.

## Our competitive advantage

Blue Systems team is excited to present to Transport for London, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## Quality Tender Submission

### 1.23 1. Methodology and Approach

#### 1.24 a. Working with TfL, local authorities and other stakeholders

[REDACTED]

[REDACTED]

[REDACTED]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**Power to act operationally:** Mobility Manager allows authorities to act operationally in terms of [REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

In turn, TfL will directly benefit from all these positive developments and achievements in other cities. We know exactly what to do to bring real benefit in terms of improving micromobility operations in London.

[REDACTED]

To achieve this, **first**, the Platform is already capable of collecting data within the MDS framework from TNCs, [REDACTED]

**Second.**

**Third**, Mobility Manager is actually just one of the three modules of our comprehensive Smart City Platform. The second module is Smart Parking, allowing the city to centralize and control parking operations within the city generating additional revenue and optimizing fine payments for Londoners. Finally, the third module is Smart Patrol which will enable TfL to effectuate smart planning, efficient dispatch and cost-effective parking and micro-mobility enforcement, again generating additional revenue for the city. We will be thrilled to demonstrate all capabilities of the Platform to TfL and discuss scaling once the Pilot begins.

1.29 f. Capability and relevant experience of the key personnel  
We will staff this Project with well-trained team of project and product managers, interface developers, data security and management specialists and other staff to deliver and maintain Mobility Manager Platform for TfL. In fact, the team who will work on this Project has designed and implemented the same platform for Los Angeles, San José and Lyon and has benefited from user feedback in those cities. The same team has also worked on other large scale public and private mobility data projects (Paris, Source London, Lyon, Los Angeles etc.). Therefore, the team is well equipped to anticipate and effectively address and resolve any issues as they may arise during the project implementation. **See engagement team bios, experience and organizational chart in Appendix 6 - Screenshots (figures 3 & 4).**

## 1.30 2. Mobilisation

### 1.31 a. Work programme overview

We are committed to align our deliverables and milestones with the timetable set by TfL. Please see our proposed work programme overview attached as **Appendix 1 – Work Programme Proposal.**

1.32 b. Top 3 key risks (out of 4) potentially encountered during mobilisation

(1) [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

## Appendix 1 – Work Programme Proposal.

### 1.35 3. Systems and Processes

1.36 a. Legacy systems and data integration  
Mobility Manager allows for a two-way integration with legacy systems:

Legacy to Mobility Manager: On request, [REDACTED]

[REDACTED]

[REDACTED]

Mobility Manager to legacy: All the data and analysis available in Mobility Manager [REDACTED]

[REDACTED]

[REDACTED] and best practices

As detailed in the **section 6 - Cyber Security** and **section 7 - Privacy and Data Protection**, our Mobility Manager and all corresponding services

# Transport for London

are fully compliant with cyber security, data protection, and privacy regulations and best practices:

- Our infrastructures are hosted on ISO27001 certified facilities.
- [REDACTED]
- Our offices are [REDACTED]
- A [REDACTED]  
[REDACTED]  
[REDACTED]
- Mobility data [REDACTED]  
[REDACTED]  
[REDACTED]
- Blue Systems will never use TfL and boroughs' data for any other purpose than those needed for the operation of the Platform.

Please see our Data Security Policy ([\*\*Appendix 4 - Data Security Policy\*\*](#)) and our data breach response plan ([\*\*Appendix 5 - Data Breach Response Plan\*\*](#)).

## 1.38 c. Use of different data formats

Our Mobility Manager is fully compatible with:

- ~~Mobility Data Specifications (MDS) format~~ [REDACTED]  
[REDACTED]  
[REDACTED] – [REDACTED] with full compliance;
- ~~The Google Data 1.0 - 1.0 File Specification (GDFS) format~~ [REDACTED]  
[REDACTED]

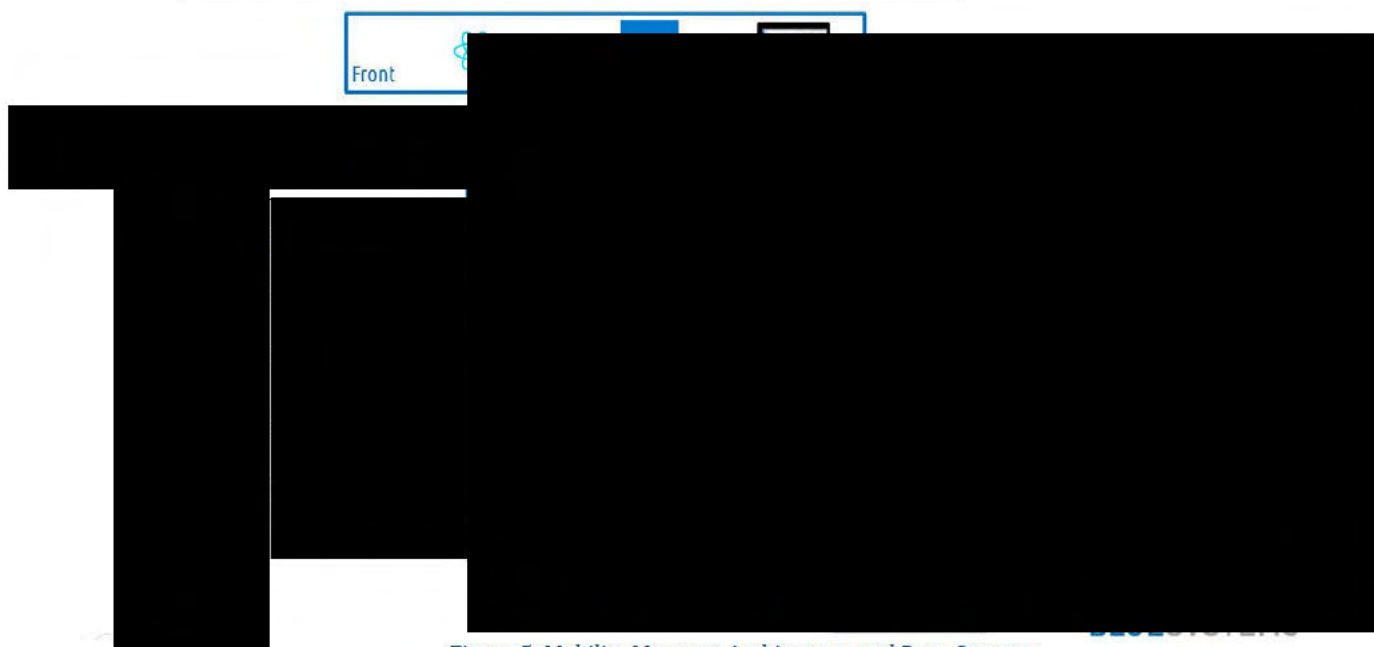


Figure 5: Mobility Manager Architecture and Data Streams

This capability is demonstrated under [REDACTED]  
[REDACTED] and

[REDACTED]  
[REDACTED].

Furthermore, [REDACTED] to [REDACTED]  
[REDACTED]. [REDACTED]  
[REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED] [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]

The bottom line is, Mobility Manager is [REDACTED]  
[REDACTED] when it comes to compatibility with different data standards.

#### 1.39 d. Different data analytics activity

Over the last eight years, we have built a comprehensive expertise [REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

We are committed to deliver [REDACTED]  
[REDACTED]  
[REDACTED] We provide dedicated user training and support  
and [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

We benefit from a broad business intelligence and data visualization expertise of our strong in-house team of data scientists. Blue Systems data experts have built over time a proven track-record:

- Mastering business intelligence [REDACTED],  
[REDACTED]

## Transport for London

- Developing custom-made [REDACTED]  
[REDACTED]
- [REDACTED] [REDACTED]  
[REDACTED]

In other words, by employing us as its micro-mobility platform vendor, TfL will get an experienced partner who has successfully delivered similar platforms to other cities in Europe and the United States.

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

Conce

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]

- [REDACTED]

[REDACTED] [REDACTED]

- [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] [REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]

- [REDACTED]

- [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



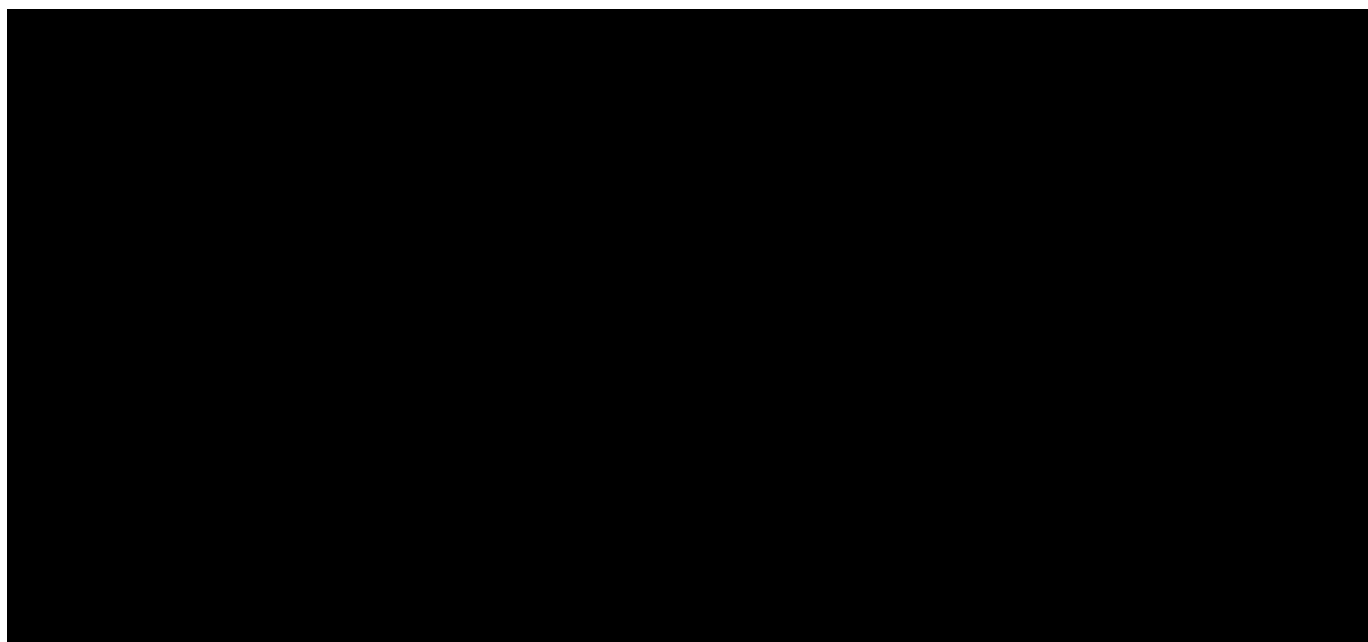


Figure 7: List of existing connected operators to Blue Systems platforms

#### 1.42.1.4

\_\_\_\_\_

- [illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 1.44 c. Our approach to agreements between cities and operators, and our role

To begin, [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] use mobility data is to provide services to TfL as sought by this Tender.

[REDACTED]  
[REDACTED]

### 1. Los Angeles approach:

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] The document could be found on LADOT website here:  
[https://ladot.io/wp-content/uploads/2019/03/2019-04-12\\_Data-ProtectionPrinciples.pdf.pdf](https://ladot.io/wp-content/uploads/2019/03/2019-04-12_Data-ProtectionPrinciples.pdf.pdf)

Once those principles were in place and self-adopted by the LADOT, the City mandated micro-mobility [REDACTED]  
[REDACTED]  
[REDACTED]

As a last step, before any mobility data was shared through our Platform, [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] – i.e., all mobility providers’ data processed by our Mobility Manager.  
[REDACTED]  
[REDACTED]  
[REDACTED]

## *2. Another approach:*

[REDACTED]  
[REDACTED] we [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

In any case, we will appreciate an opportunity to provide full support to TfL in terms of sharing our experience in Los Angeles and Lyon, to enable TfL to choose the right operator engagement approach best suiting its needs and expectations.

## 1.45 5. Demonstration

### 1.46 a. Effective user experience for TfL and borough users

The Platform is intuitive and very easy to use. [REDACTED]

[REDACTED]

By connecting to the Platform, you can immediately see the [REDACTED]

[REDACTED]

[REDACTED]

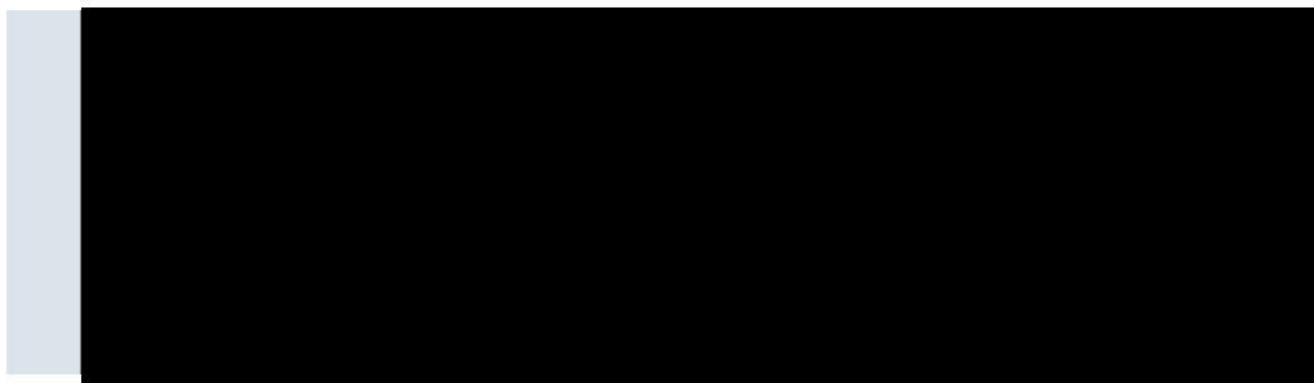
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

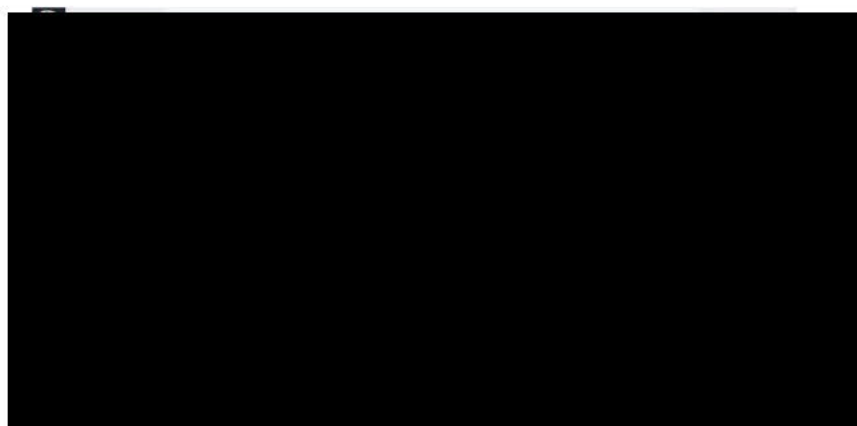
#### 1.46.1.1.1.1 1. Home dashboard and operator snapshot information

Once logged in, Mobility Manager displays a Home dashboard summarizing the state of micro-mobility in the city.



This dashboard consists of two parts:

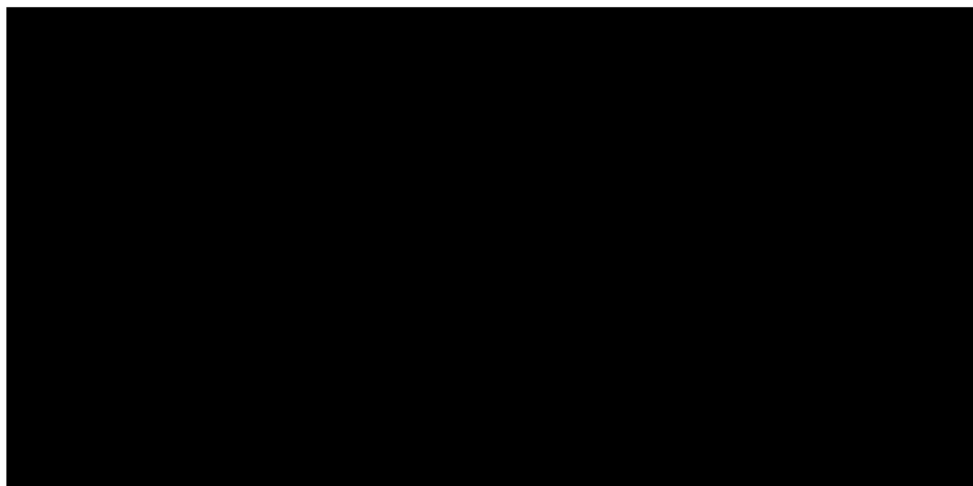
- [Redacted]
- [Redacted]



## 2. [Redacted]

### 1.46.1.2 Live status of operators





The map section displays a [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]



## 1.46.1.3 Vehicle list



## 1.46.1.4 Vehicle pop-up








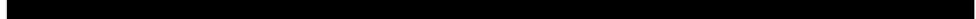
To have a quick overview of the information on a vehicle,   
  
  


## 1.46.1.5 Vehicle detail page

By clicking on a   
  
  
  


## 3. Operators

## 1.46.1.6 Adding a new operator

Adding and connecting an operator   
  
  
  
  
  
  


[REDACTED]

1.46.1.7

[REDACTED]

Mobility Manager is able to collect and send data

[REDACTED]

[REDACTED]

1.46.1.8

Setting up a permit

[REDACTED]

[REDACTED]

Once permits are

[REDACTED]

[REDACTED]

1.46.1.9

Monitoring

[REDACTED]

[REDACTED]

[REDACTED]

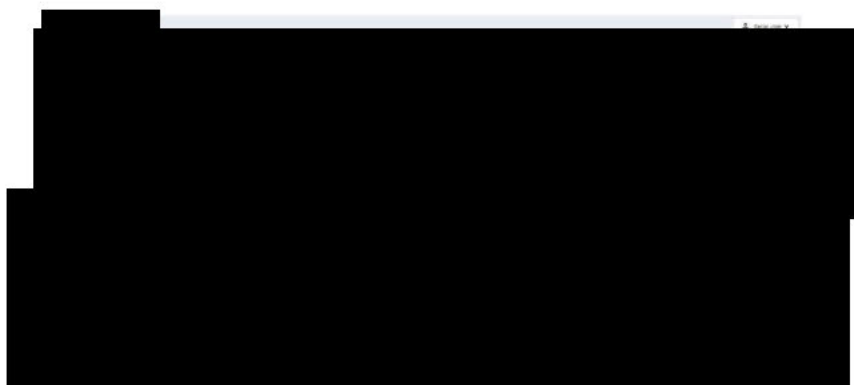




This tool enables the user to visually monitor all [REDACTED]

[REDACTED]  
[REDACTED]

The [REDACTED]  
[REDACTED]



[REDACTED]

By reviewing these graphs and lists, TfL will be able to [REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

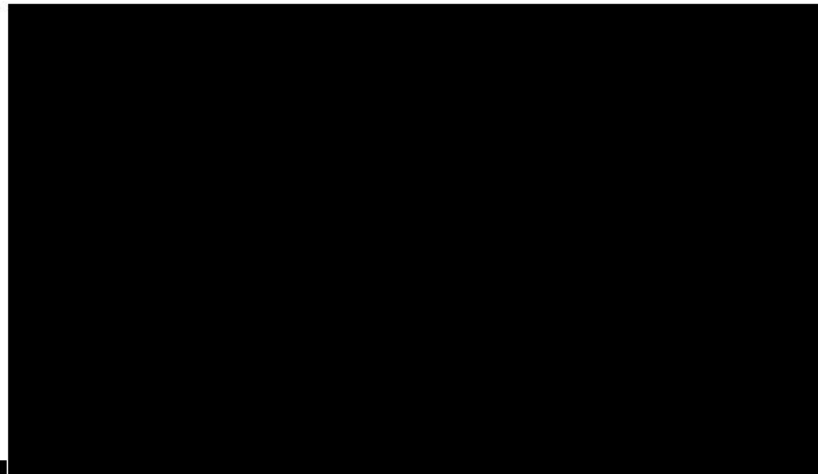
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]

## 4. Trips

### 1.46.1.10 List of trips

In addition to [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

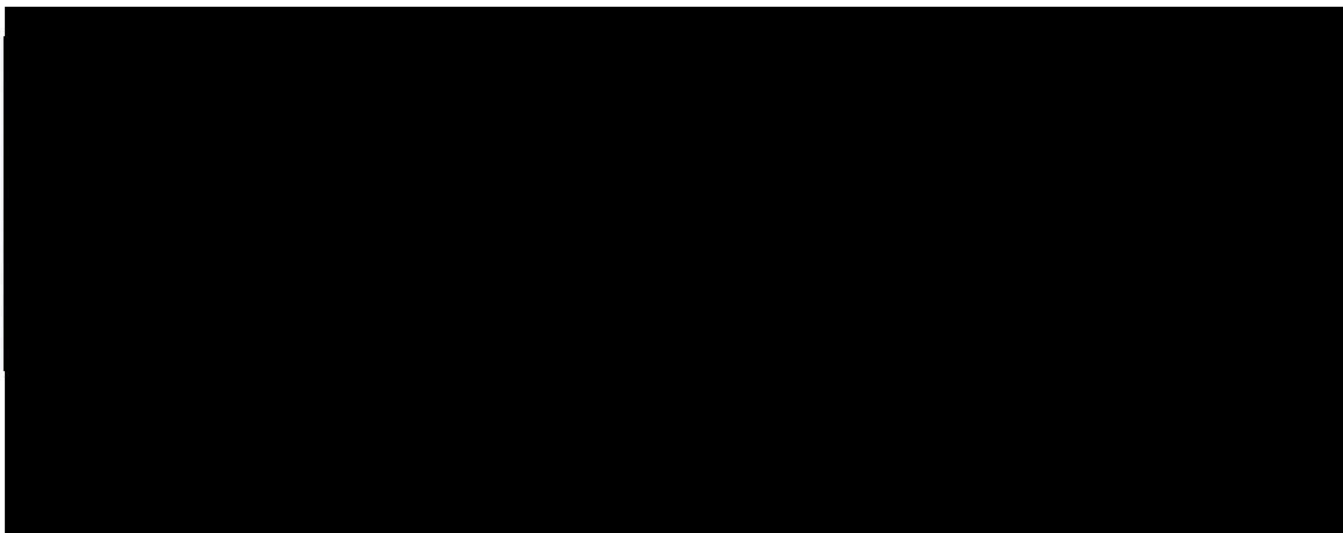


### 1.46.1.11

[REDACTED]

Data can be filtered [REDACTED]  
[REDACTED]  
[REDACTED]

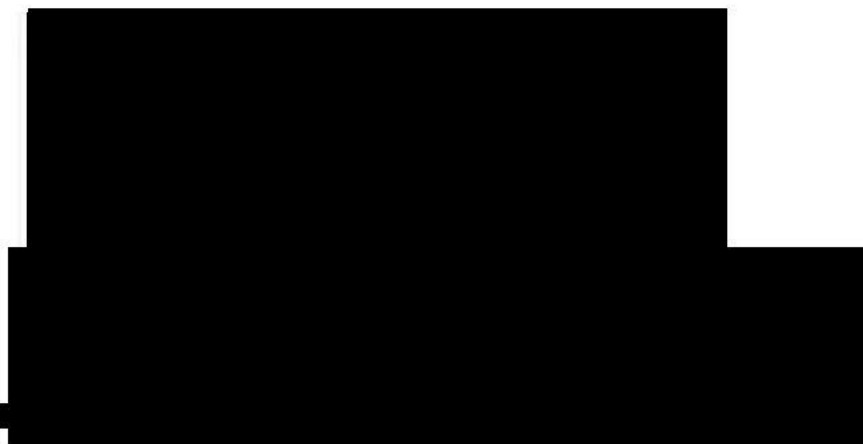
[REDACTED] [REDACTED] heatmap



that enables, due to the effective colouring system

## 1.46.1.13 Alluvial diagram

Mobility Manager also provides



### 1.46.1.13.1 5. Analysis section (Key Performance Indicators)

For historical analysis, some Key Performance Indicators, referred to as KPIs, were developed. The KPIs provide detailed insights based on metrics

## Transport for London

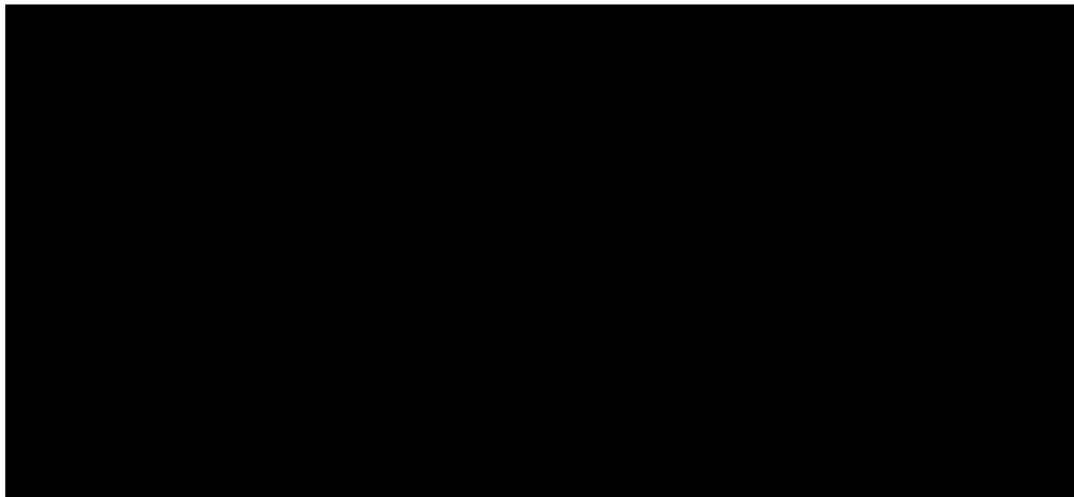
Staff members

You will find below a list of use-cases for those KPIs. An exhaustive list of the proposed metrics and KPIs is available in **Appendix 6 - Screenshots from figure 40 to figure 56.**

KPI use case

To complete this view, the section also offers a map showing

## Transport for London



1.46.1.15

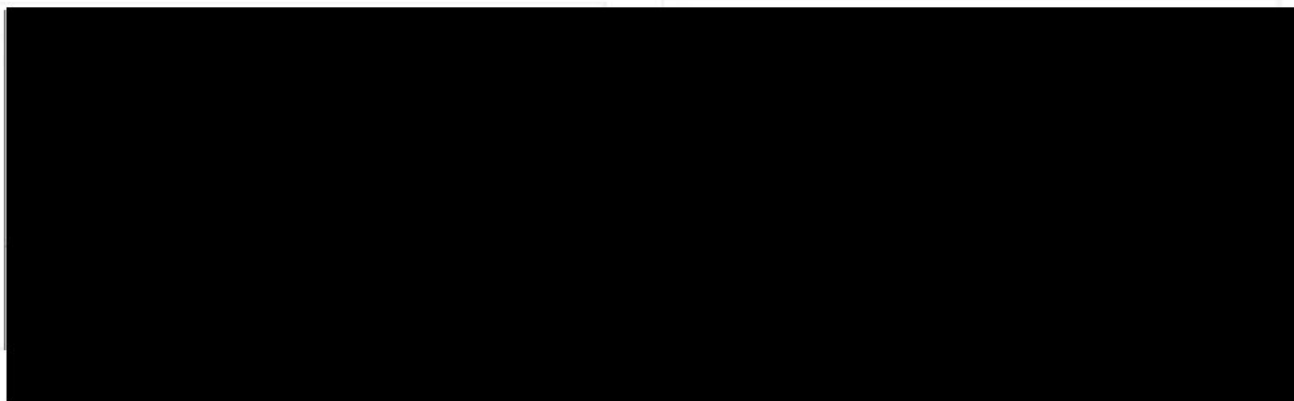
KPI

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted]

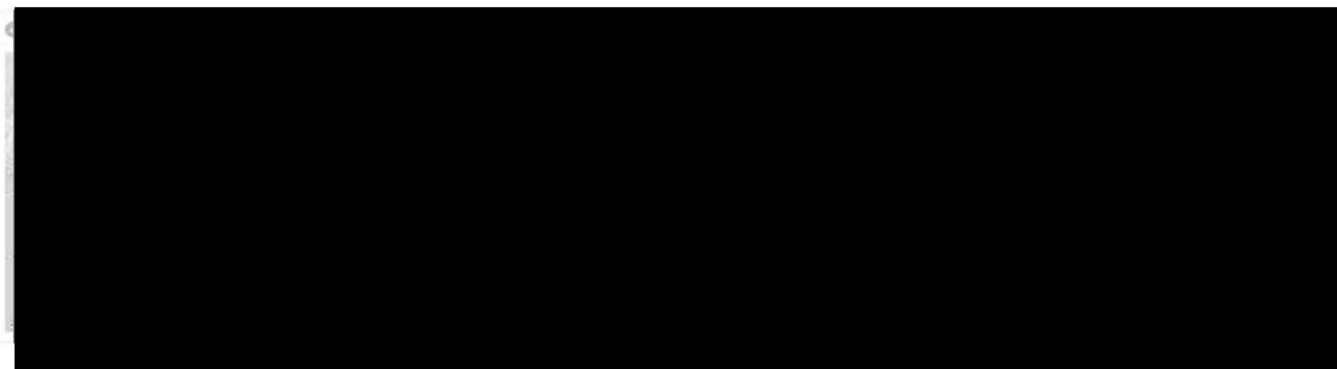
[Redacted]

[Redacted]

[Redacted]

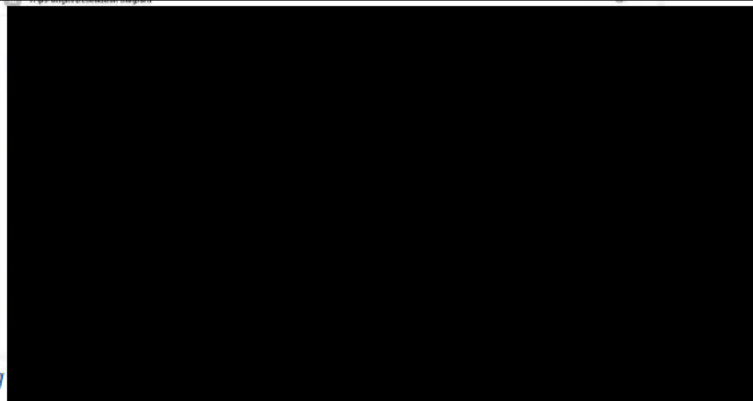
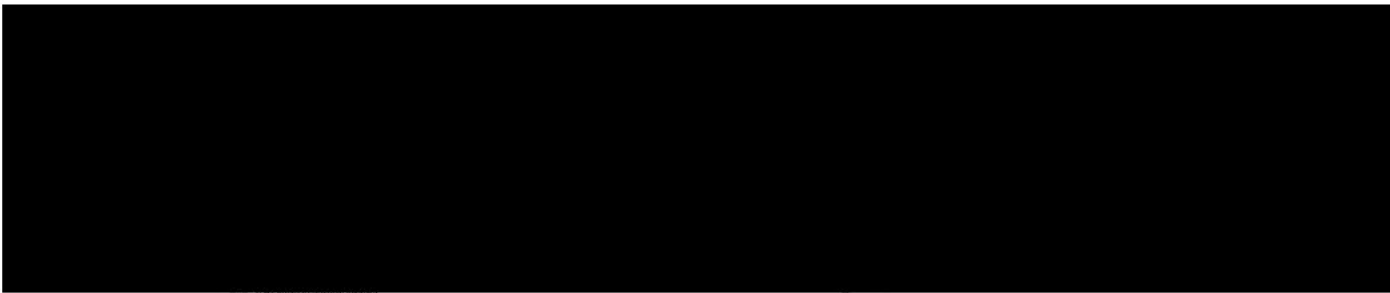
[Redacted]

[Redacted]



[Redacted]

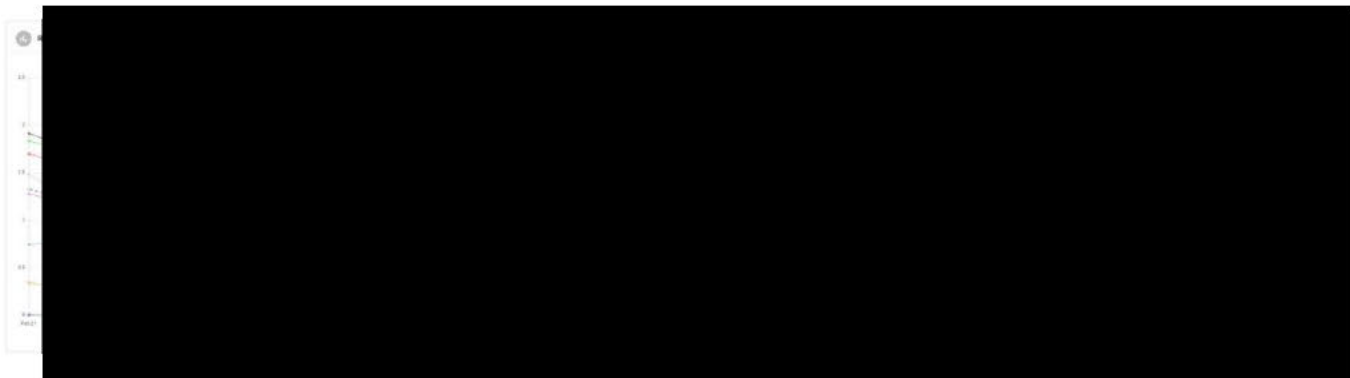
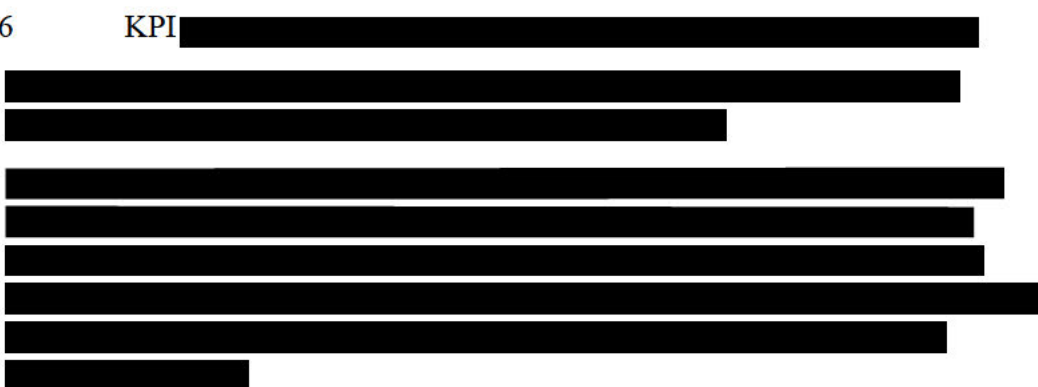
For the trip destination map **see Appendix 6 - Screenshots (figure 35).**



*Fig*

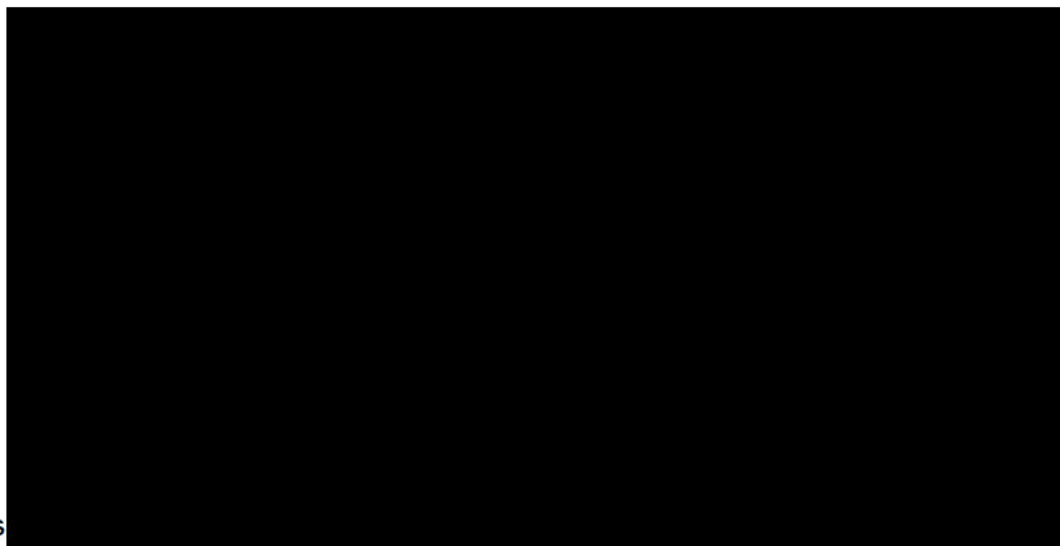
1.46.1.16

KPI



37 and 38:





## 1.46.1.16.1 6. Areas

[Redacted text block]

Areas can be defined in two ways: [Redacted text]

[Redacted text]

[Redacted text]

[Redacted text] **See Appendix 6 - Screenshots (figure 58)**. Once defined, the area is given [Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

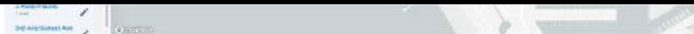
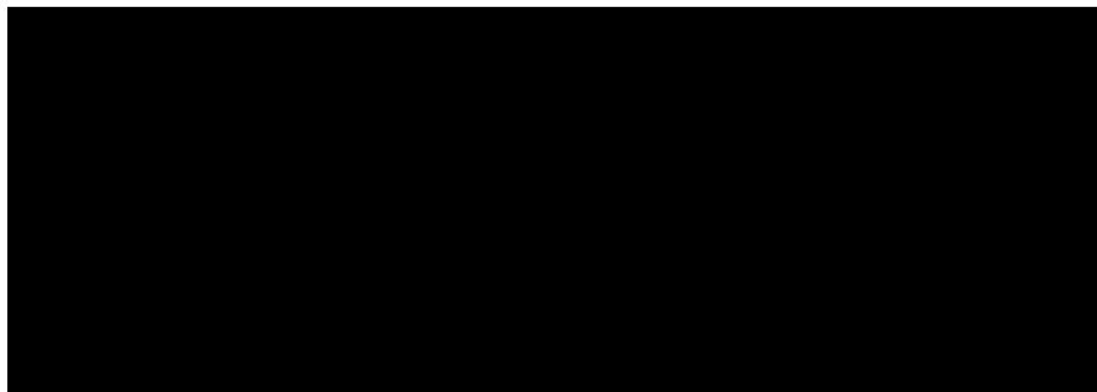


Figure 57: Area creation

Users can [Redacted text]

[Redacted text]

[Redacted text]

## 1.46.1.16.2 7. Custom reports

## Transport for London

The KPIs were developed in order to help cities monitor the use of micro mobility within their boundaries. However, in order to regulate operators by enacting smart data driven policies, further analyses are often needed.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

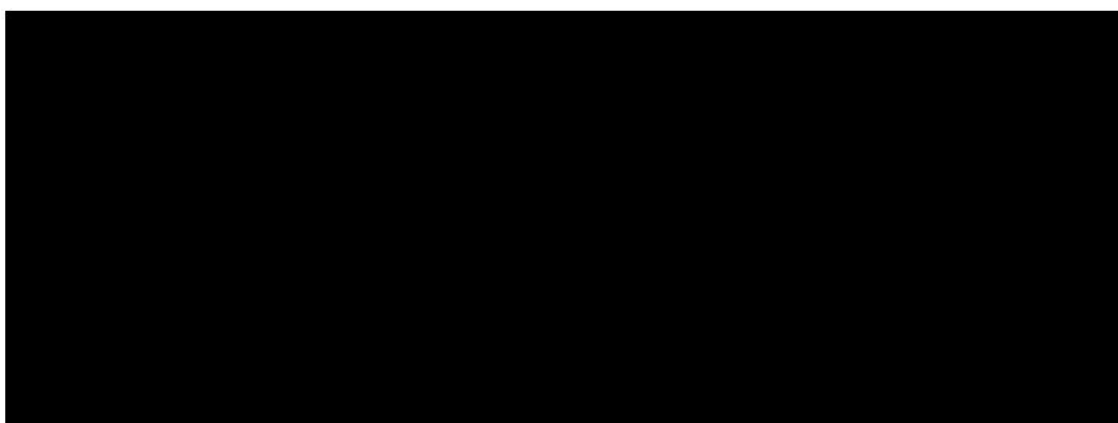
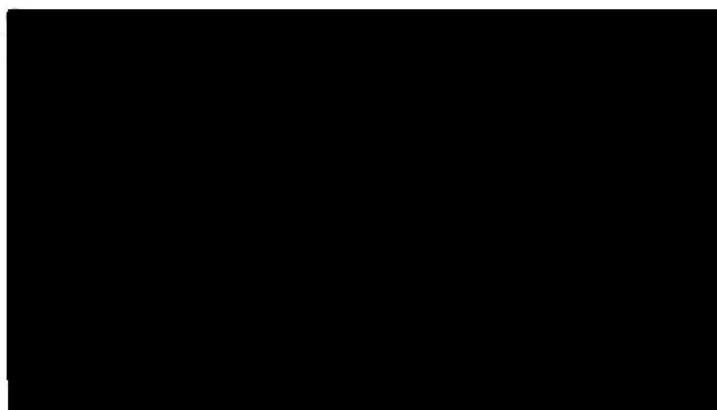
[REDACTED]

[REDACTED]

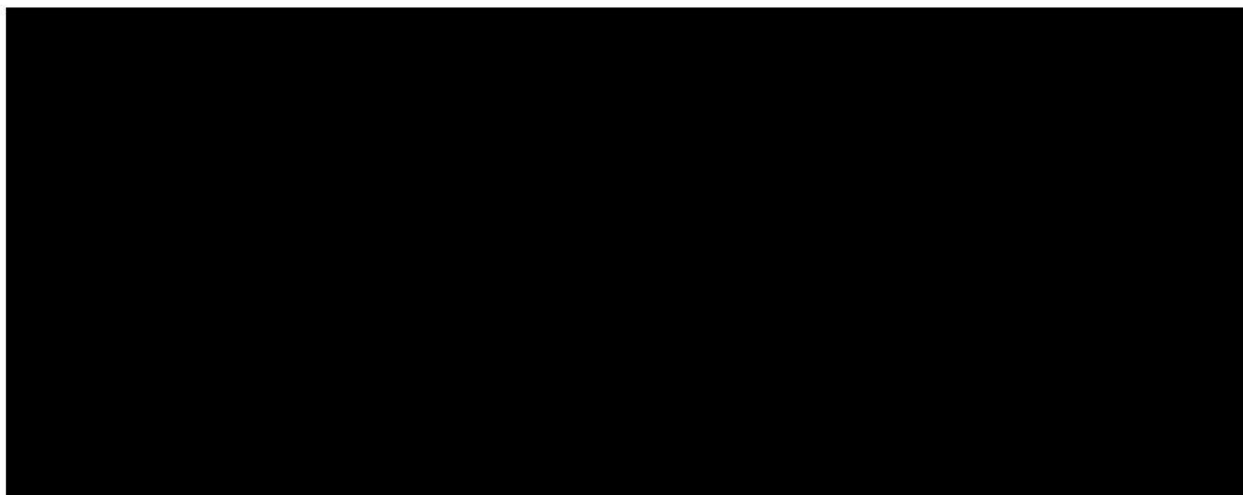
[REDACTED]

[REDACTED]

[REDACTED]



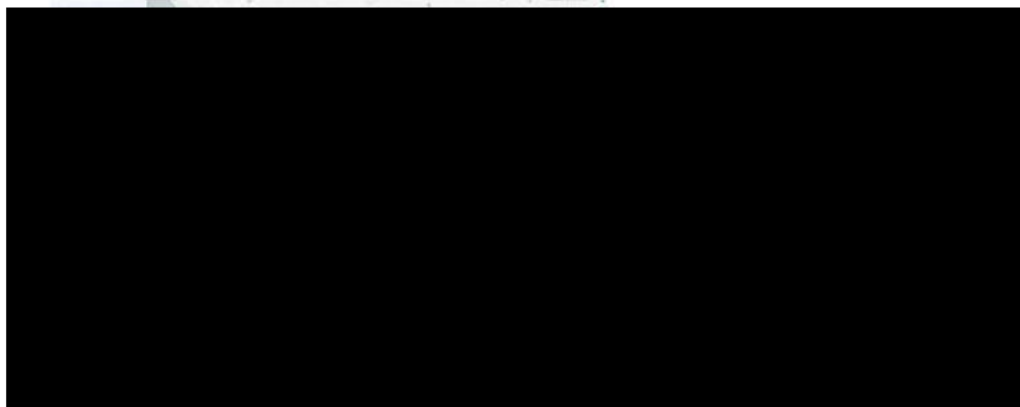




In other words, Custom Area reports feature thus allows TfL to carry out deep data analyses and adapt its regulations and policies to specificities of each area within London.

1.46.1.18

■ [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]



*map*

1.46.1.18.1 8. Policies and Compliance

Based on your analysis of what happened in the past, you will be able to

[Redacted]  
[Redacted]

1.46.1.19 Policy creation mechanism

[Redacted]

[REDACTED]

[REDACTED]

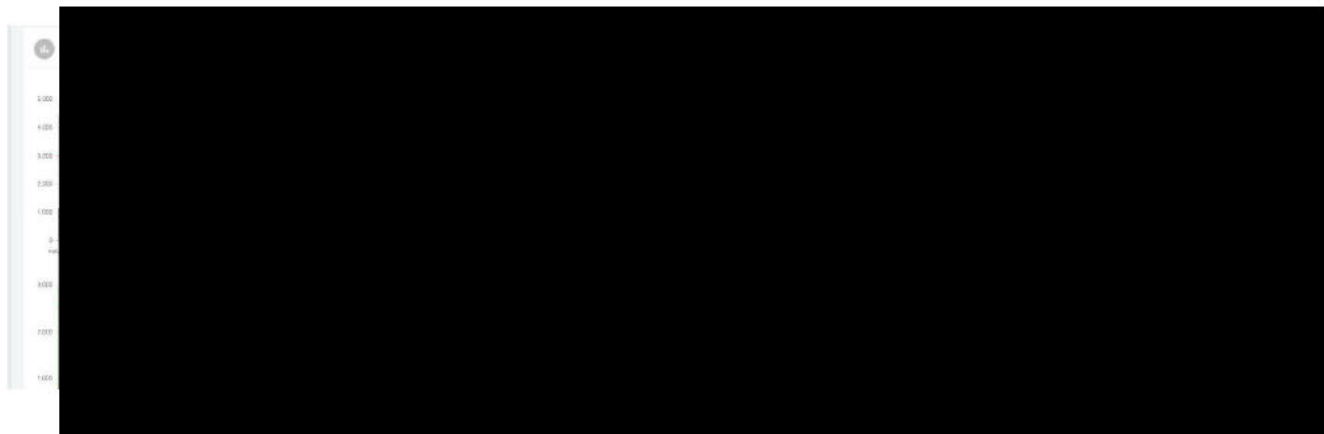
[REDACTED]

[REDACTED]

[REDACTED]

Figure 67

Figure 67



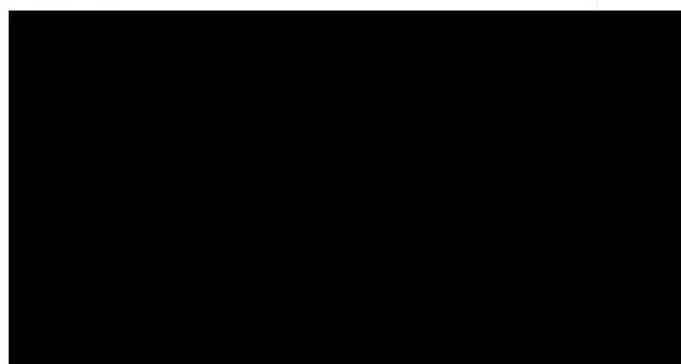
permits



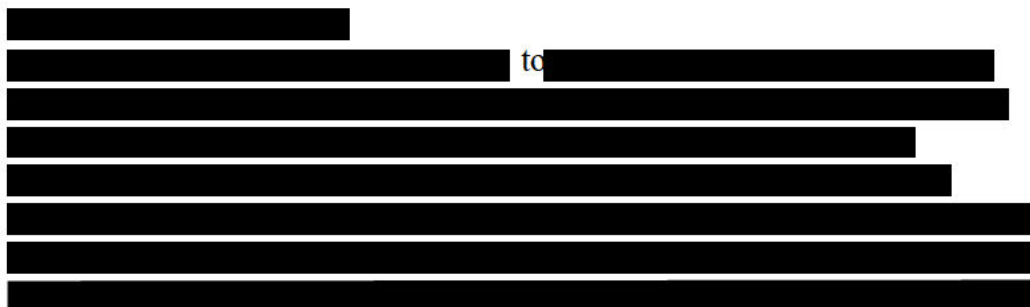


## 1.46.1.21 List of policies

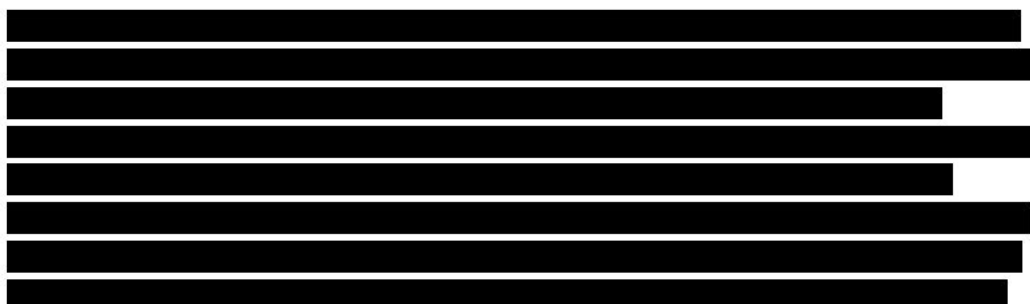
Mobility Manager features multiple policies, which are further described below.

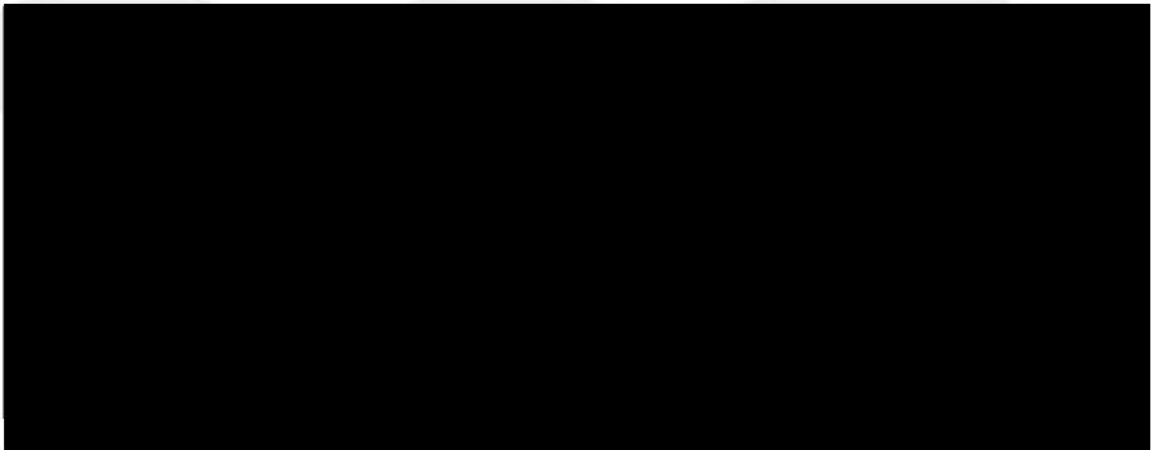


 *Permit policy creation form*



- Screenshots (figure 72).





Areas 

  
  
  
  
 [see Appendix 6](#)

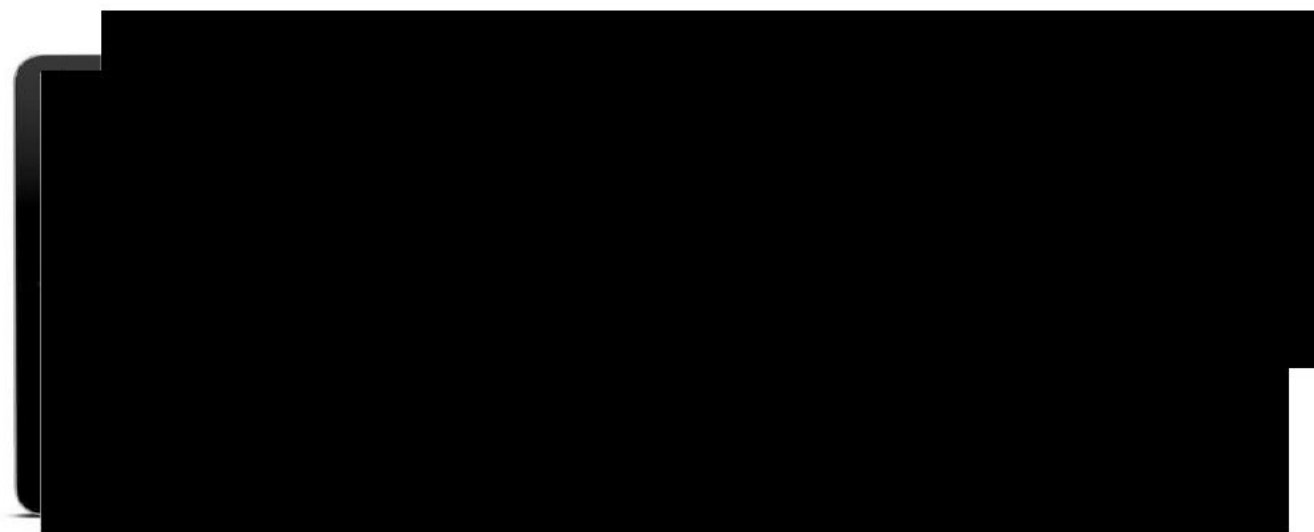
- Screenshots (figure 74).


  Responsive web design

Our Mobility Manager was developed following a responsive web design approach that enables to adapt the display to the size of the screen and the orientation of the device, thus ensuring the friendliest user experience. Mobility Manager Platform can be accessed through desktops, laptops (Windows and Mac), tablets and smartphones running on both Android or IOS.



*Figures 76, 77 and 78: Responsive web design on tablet and smartphone*

1.46.1.21.2



1.47.1.1 **[REDACTED]**. Alignment with data requirements  
Meeting the data requirements

Our Mobility Manager is fully compatible with several data formats including:

- **[REDACTED]** Mobility Data Specification (MDS) developed by the OMF
- **[REDACTED]** General Bikeshare Feed Specification (GBFS) format.



More information on these APIs is available below:

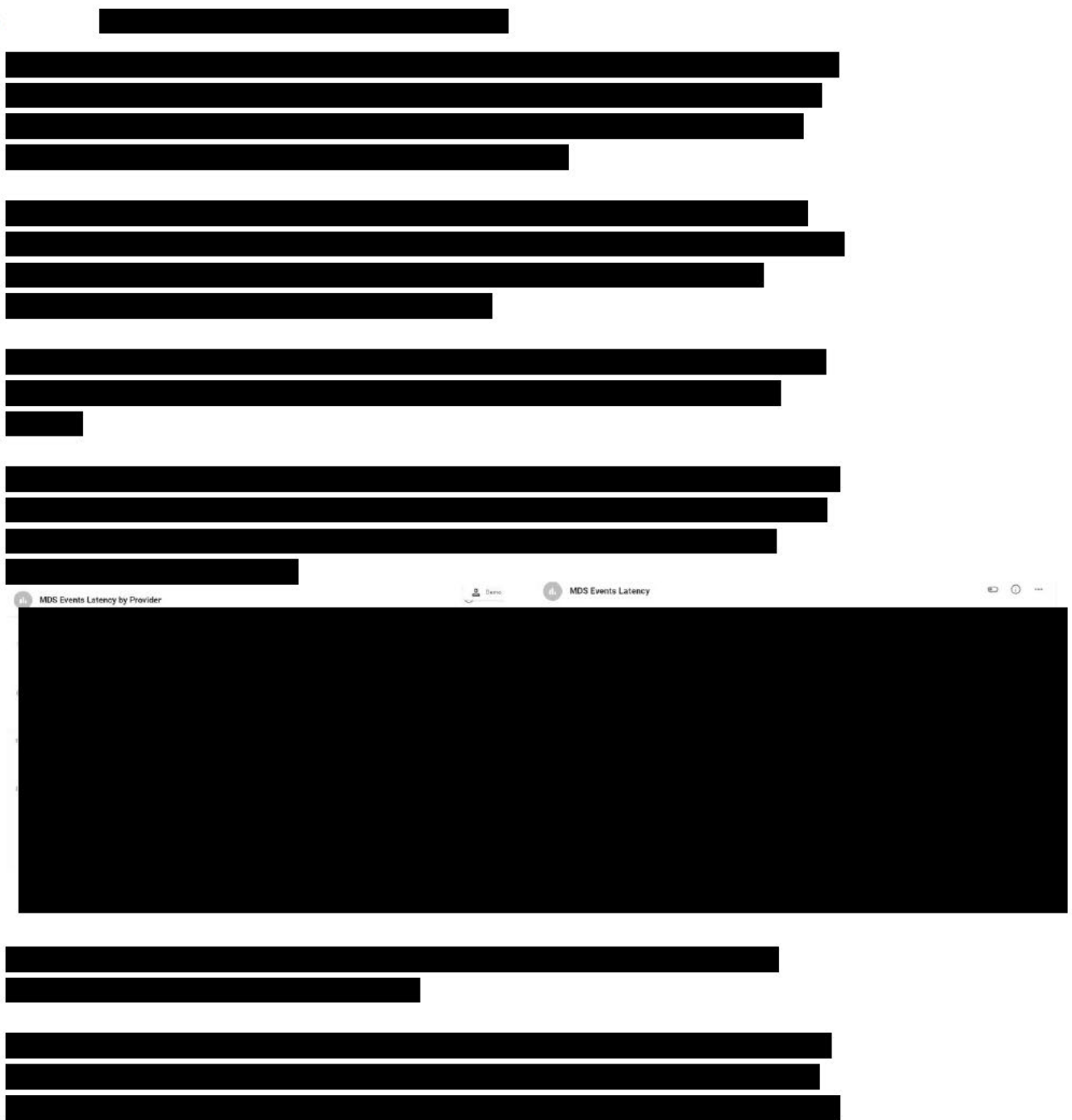
- Provider API: <https://github.com/openmobilityfoundation/mobility-dataspecification/tree/dev/provider>

# Transport for London

- Agency API: <https://github.com/openmobilityfoundation/mobility-dataspecification/tree/dev/agency>
- Policy API: <https://github.com/openmobilityfoundation/mobility-dataspecification/tree/dev/policy>

These data formats fully satisfy all TfL requirements, including locations of all dockless micro-mobility vehicles, unique vehicle identifiers, vehicle type, propulsion type for each vehicle, vehicle status (available for hire/out of service), journey start data and journey end data. MDS goes further and provides for additional data which is used extensively in the Platform.

1.47.1.2



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] 81 and 82: MDS anomalies by provider and MDS anomalies by type

[REDACTED]

## 1.47.1.3 Two-way communication with operators

The Agency, Policy and Compliance APIs that are natively implemented in our tool allow for two-way data sharing between micro-mobility operators and TfL/London borough users. TfL and London boroughs will be available to communicate with operators and supply operational information. [REDACTED]

[REDACTED]

## 1.47.1.4 Data access

TfL and London boroughs will have access to all the real time data collected from mobility operators. Users can view data in the front-end of the Platform any time through individual user accounts with user-defined passwords. [REDACTED]

## 1.47.1.5 Data ownership

Our approach is that we do not claim ownership rights in the data aggregated and processed by the Platform. It would be considered TfL data and as between TfL and Blue Systems, the data will always belong solely to TfL.



# Transport for London

## 1.47.1.6 Data retrieval

TfL staff can access the data it at any time, from anywhere on any device. Data retrieval can be done through several means:

- [REDACTED]
- [REDACTED]
- [REDACTED]

## 1.47.1.7 Data Standard Evolution

Furthermore, the Platform has been designed to be fully adaptable to any new standard or specification that could be released at a later time. This includes evolutions of the existing MDS and GBFS APIs, integration of new MDS APIs (for instance, the Compliance API that is currently being discussed by the MDS community is already integrated), public transit management standards, charge points management standards (OCPI), and even integration of new standards that have not been released at this time [REDACTED] s [REDACTED]

### 1.48 c. Multi-jurisdictional access

#### 1.48.1.1 Multiple user management

Our Mobility Manager is [REDACTED] cloud-based SaaS service. [REDACTED]  
[REDACTED]

#### 1.48.1.2 Customized access rights management

Thanks to our experience in other cities (i.e. Lyon) where we have been requested to provide different levels of access (aggregated data for standard officers, individual trips data for chief of data analytics, scooter KPIs for micro-mobility monitoring teams, carsharing data for relevant city teams etc.) our tool has been designed to properly manage user access rights.

This customization can be done at two different levels: data access level and permission level.

- #### 1.48.1.3 [REDACTED]
- [REDACTED]
  - [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

## 1.48.1.4 Read-write permission levels

The Platform supports two levels of access rights: read-write and read-only. Read-only gives access to all pages but does not allow users to create or edit content. Read-write gives access to all pages with editing and creation capabilities.

Lastly, Mobility Manager allows an organisation to give exceptional read-only or read-andwrite access to staff members from another organisation on a user-per-user basis to facilitate inter-organisation work when needed.

## 1.48.1.5 Custom access-level

Upon request from TfL [REDACTED]

## 1.49 d. Development of customized features

### 1.49.1.1 Custom features implementation

We are strongly committed to developing the most TfL-centric solution by regularly adding new customised features to respond to TfL and other stakeholders' needs. Our flexible solution is intended to evolve fully addressing all use cases of every city where we operate.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 1.49.1.2 Custom reports

As described in **subsection 5.a. “Custom reports”** above, we will actively be working with TfL to understand and respond to your needs. In order to regulate operators by enacting smart data-driven policies, detailed analyses are often needed. The Platform has been designed to add custom reports very easily. Our follow-up calls will help identify the needs and define the reports which we will develop specifically for TfL.

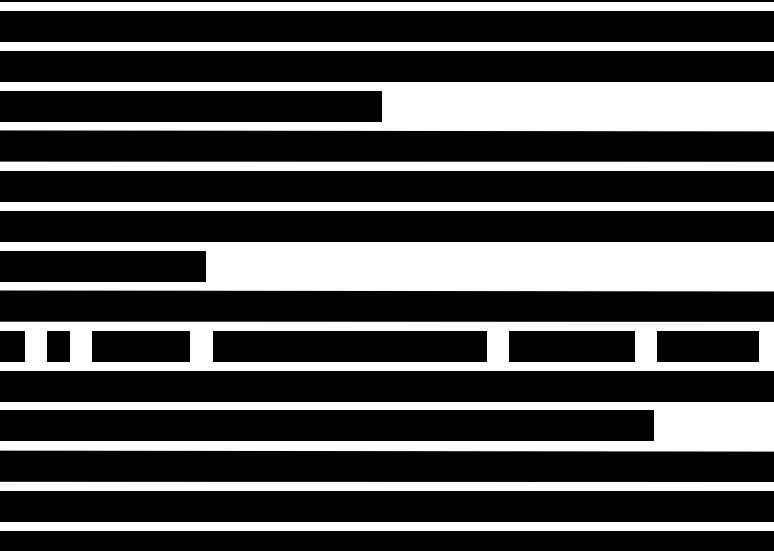
## 1.49.1.3 Custom access level

As described in subsection **5.c. “Custom access level”** above, we will work closely with TfL, boroughs and all stakeholders involved in understanding the user permissions needed and will go even further if need be by implementing feature by feature access depending on the users’ organisations and responsibilities.

## 1.49.1.4 Custom policies implementation

We will be able to develop custom policies and support TfL in the implementation of these additional policies. Some examples are listed below:

- [REDACTED]
- [REDACTED]
- [REDACTED]



that fail to  
 report their data or report inaccurate or incomplete data.

1.50 e. Scalability of the solution

### 1.50.1.1 Immediate scaling possibilities

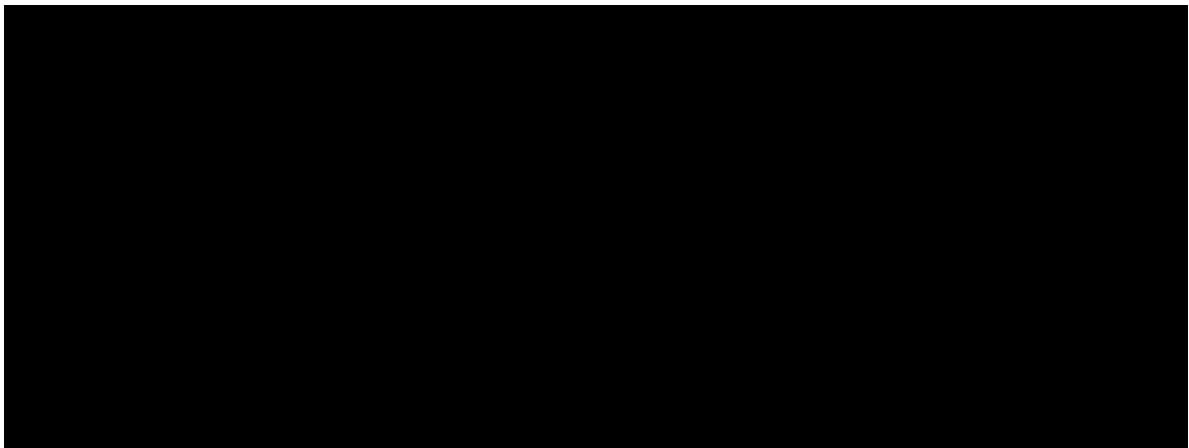
Our solution is not limited to just docked and free-floating bikes. Actually, we already process several other forms of mobility data. These offer immediate scaling opportunities to TfL should TfL wish to extend the scope of the Platform.

- **Dockless E-Scooters:** our micro-mobility analytics platforms are already connected to 13 different dockless e-scooter operators - see Section 4.a. (figure 7) above – and we have even helped some of them to conform to the MDS data format. If London were to add scooters to the pilot, they could be added immediately to the Platform.
- **Carsharing:** we have already integrated two carsharing operators (BlueLA and BlueLY) to our micro-mobility Platform and we were the ones who introduced the “car” format to the MDS which gives us experience in managing data from carsharing systems.
- **Mopeds:** our platform is already fully compliant with the newly introduced “moped” vehicle type in the MDS
- **EV-charge points:** we already manage data from EV-charge points in several cities including London (Source London) and could work with TfL to integrate EV-charge data (OCPI format or other)
- **Parking data:** our parking tool has helped define the national standard for parking data in France. We manage 50 million parking rights and 10 million parking fines each year and would be glad to



# Transport for London

*procedure that would be created, including an estimated time frame for implementation.*



a) [redacted]  
[redacted]  
[redacted]  
[redacted]

[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

b) *explain how the Tenderer shall specify and ensure compliance at all times with security measures and procedures which are sufficient to ensure the Services comply with Volume 2 – Specification;*

[redacted]  
[redacted]  
[redacted]  
[redacted]

[redacted]  
[redacted]  
[redacted]  
[redacted]

i [redacted]  
[redacted]  
[redacted]

# Transport for London

- [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED]

\_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

c) reference and explain what the Tenderer will do to ensure compliance with the security requirements set out in Volume 2 –

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

■) *state any other cyber security industry standards over and above those set out in Volume 2 – Specification which the Tenderer will ensure are implemented and maintained in the delivery of these Services;*

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

e) state all applicable law which relates to the security of the Services.

\_\_\_\_\_

# Transport for London

*Appendix 3, 1.2. In addition to the requirements included in section 1.1 above, Tenderers shall also refer to the guidance included in Table 1 on the following page.*

Please see **Appendix 3 – Cyber Security Table** specifically responding to each point raised.

*Appendix 3, 1.3. Only Tenderers providing a cloud based solution shall consider items reference 1 to 21 in Table 1 (below) as part of their response. Tenderers who are not providing a cloud based solution shall consider items reference 12 to 21 in Table 1 (below) only.*

Please see **Appendix 3 – Cyber Security Table** specifically responding to items 1 to 21.

## 1.52      7. Privacy and Data Protection

*Appendix 4: Tenderers shall submit an outline Privacy and Data Protection plan as their response to quality criterion 7. Where a Tenderer does not currently have a particular policy, process or procedure in place, the response shall describe the policy, process or procedure that would be created, including an estimated time frame for implementation.*

[REDACTED]

*The outline Privacy and Data Protection as a minimum will:*



a) *describe how the Tenderer will ensure compliance with privacy and data protection legislation when delivering the services*

Please see our **Data Security Policy - Appendix 4**, [REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

- I [REDACTED]  
[REDACTED]  
[REDACTED]

- I [REDACTED]  
[REDACTED]  
[REDACTED]

- I [REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]

- I [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

Please **see Appendix 4 – Blue Systems Data Security Policy** for more information.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Data Breach Response Plan attached as

Appendix 5.

1.52.1.1 IT infrastructure physical security

1.52.1.2 [REDACTED]

Response	Percentage
U.S. should take action	95%
U.S. should not take action	5%

## Transport for London

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- *describe how the Tenderer will proactively identify privacy and data protection risks when delivering the services. This should include details of the systems/processes in place to identify, monitor and resolve security incidents involving TfL/borough personal data*

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED] **Data Breach Response Plan**  
**for more information (attached as Appendix 5).**

- d) *describe how you will ensure that all of the Tenderer's employees and temporary workers with access to TfL and borough personal data are:*

- i. *appropriately screened/vetted*

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- ii. *contractually obliged to comply with relevant privacy and data protection obligations*

[REDACTED]

*iii. appropriately trained*

[REDACTED]

- *if the Tenderer is intending to process personal data outside of the EEA:*
  - i. describe the proposed processing*
  - ii. specify the country or countries in which the processing will take place*
  - iii. provide evidence that you can meet the relevant requirements of current privacy and data protection legislation (including willingness to adopt EU Model Clauses)*

Not applicable – we will process all data exclusively within EEA.

*f) describe how the Tenderer will support TfL in meeting its statutory obligations to provide individuals with access to copies of their own personal data in response to a Subject Access Request*

The way our Mobility Manager is set up is to ensure that no personal data of end users of micro-mobility is collected, processed or stored. It is simply not needed and not relevant in order to carry out services sought by TfL here.

Nevertheless, we are very familiar with and had a robust process in place for responding to individual subject access requests by virtue of running a large consumer-facing mobility operation in Europe. Therefore, while we will likely have no data to provide to individuals in response to their requests, we will timely, diligently and thoroughly cooperate with TfL to properly respond to all such requests.

- g) describe how you will ensure that TfL personal data is securely disposed of in accordance with defined retention periods.*

[REDACTED]

[REDACTED]

- h) describe the audit/assurance arrangements that will be in place to monitor compliance with relevant obligations (whether statutory or contractual) covering the processing of TfL personal data.*

[REDACTED]

## Transport for London

## SCHEDULE 4 – CHARGES

Please refer to

Please refer to

## Transport for London

ID	Test	Test Name	Location	Start	Finish	On 4, 2020	On 1, 2021	On 2, 2021

Transport for London

D	Task	Task Name	Duration	Start	Finish	On 4, 2020	On 1, 2021	On 2, 2021



Transport for London

<div>Project MMS-Tilapia data</div> <div>Date Tue 08/12/20</div>	
Task	<div><div></div> Inactive Task</div>
Split	<div><div></div> Inactive Milestone</div>
Milestone	<div><div></div> Inactive Summary</div>
Summary	<div><div></div> Virtual Task</div>
Project Summary	<div><div></div> Duration-only</div>
	<div><div></div> Manual Summary Rollup</div>
	<div><div></div> External Milestone</div>
	<div><div></div> Manual Summary</div>
	<div><div></div> Start-only</div>
	<div><div></div> Finish-only</div>
	<div><div></div> External Tasks</div>
	<div><div></div> Deadline</div>
	<div><div></div> Progress</div>
	<div><div></div> Manual Progress</div>

## SCHEDULE 6 - FORM FOR VARIATION

### PART A

Contract Parties: *[to be inserted]*

Contract Number: *[to be inserted]*

Variation Number: *[to be inserted]*

Authority Contact Telephone: *[to be inserted]*

Fax: *[to be inserted]*

Date: *[to be inserted]*

### 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 (£)
ALLOWANCE TO THE AUTHORITY	
EXTRA COST TO THE AUTHORITY	
TOTAL	

.....  
For the Authority (signed)

.....  
(print name)

<b>ACCEPTANCE BY THE SERVICE PROVIDER</b>	
<b>Date</b>	<b>Signed</b>

## PART B – SUPPLY CHAIN FINANCE OPTION RELATED VARIATIONS

1. The Authority is developing a scheme and system whereby the Service Provider may be permitted, at the Authority's sole discretion, to seek payment of invoices in respect of Charges under this Contract within a time period less than the 30 days of receipt set out Clause 5.4.1 in consideration for a reduction in the Charges due thereunder (the "**Supply Chain Finance Option**").
2. The Service Provider hereby agrees that where such requests are made by the Service Provider and approved by the Authority, by way of such process and/or systems put in place by the Authority acting either on its own behalf or by or via its employees, agents, contractors or otherwise such request, approval and resulting accelerated and reduced payment shall constitute the Service Provider's exercise of the Supply Chain Finance Option and the valid and legally binding:
  - 2.1 variation by the Parties of the related Charges due and payable to the Service Provider under this Contract; and
  - 2.2 waiver by the Service Provider of any right held previously by it to invoice for and be paid the amount by which the Charges are reduced pursuant to its exercise of the Supply Chain Finance Option.

## **SCHEDULE 8 – RE-TENDER COOPERATION**

