



GLA or TfL Standard Contract for Services

Additional Optional Clauses

These are clauses to be inserted into Schedule 2 of the Standard Contract where applicable. Please see Standard Contract for Services - Optional Clauses Checklist for guidance on use.

Ensure all text in square brackets is confirmed or amended and the brackets and italics removed before use.

Contents

A1	Privacy and Data Protection	1
A2	IT Systems.....	10
A3	Personnel Management and Training.....	12
A4	Security and Guarantees	15
A5	Liquidated Damages.....	16
A6	Extension of Time	17
A7	Further Insurance Requirements	18
A8	Further Intellectual Property Requirements	20
A9	Infringement of Intellectual Property Rights	21
A10	Further Confidentiality Requirements	22
A11	Euro - Continuity of Contract	23
A12	Option to Extend Duration	24
A13	Option to Extend Services	25
A14	Crime and Disorder Act 1998	26
A16	Step-in	27
A17	Adjustment to Charges (Indexation)	28
A19	Authority Obligation of Confidentiality	29
A20	Transfer of Employees to Service Provider	30
	Appendix 1 to Clause A20.....	33
A21	Transfer of Employees on Expiry or Termination.....	34
	Appendix 1 to Clause A21	39
A22	Cost Summary.....	41
A23	Sub-contractor Warranty.....	42
A25	Specific LU Standards	43
A26	Offers of Employment (Non-solicitation)	45
A27	Retention of Title Clause	46
A28	Consultancy - Disclaimer Clause.....	48
A29	Timber Standards	49
A30	London Living Wage.....	53
A31	Waste Electrical and Electronic Equipment Regulations 2013	54
A32	Ethical Sourcing.....	55
A33	Supplier Diversity	56
	TfL Supplier Diversity Definitions	63
1.	<i>Document Outline</i>	64

2.	<i>Diverse Suppliers</i>	64
3.	<i>Small and Medium Enterprises (SMEs)</i>	65
4.	<i>Black, Asian and Minority Ethnic (BAME) owned businesses</i>	66
5.	<i>Suppliers from other under-represented groups or protected groups ...</i>	67
6.	<i>Suppliers demonstrating a diverse workforce composition</i>	67
7.	<i>Other Definitions & Information</i>	67
8.	<i>Document Owner & Contact Details</i>	70
A34	Payment Card Industry Data Security Standard	71
	Timber Standards Appendix.....	73
	Ethical Sourcing Appendix: The ETI Base Code	74
	Appendix A - Form of Parent Company Guarantee.....	76
	Appendix B - Form of Legal Opinion for use with Guarantee	80
	Appendix C - Form of Performance Bond	83
	Annex 1	86
	Form of Demand from the Authority to [the bank]	86
	Annex 2	87
	Form of letter from the Authority to the Service Provider	87
	Annex 3	88
	Alternative form of demand from the Authority to [the bank]	88
	Appendix D - Subcontractor Warranty Agreement for Services	89

A1 Privacy and Data Protection

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

“Authority Personal Data”	Personal Data and/or Sensitive Personal Data Processed by the Service Provider or any sub-contractor on behalf of the Authority, pursuant to or in connection with this Contract;
“Data Controller”	has the meaning given to it in Data Protection Legislation;
“Data Processor”	has the meaning given to it in Data Protection Legislation;
“Data Protection Impact Assessment”	a process used to identify and mitigate the privacy and data protection risks associated with an activity involving the Processing of Personal Data;
“Data Protection Legislation”	<p>means:</p> <p>(a) any legislation in force from time to time in the United Kingdom which implements the European Community’s Directive 95/46/EC and Directive 2002/58/EC, including but not limited to the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003;</p> <p>(b) from 25 May 2018 only, 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 (the "General Data Protection Regulation");</p> <p>(c) any other legislation in force from time to time in the United Kingdom relating to privacy and/or the Processing of Personal Data; and</p> <p>(d) any statutory codes of practice issued by the Information Commissioner in relation to such legislation;</p>
“Data Subject”	has the meaning given to it in Data Protection Legislation;
“Personal Data”	has the meaning given to it in Data Protection Legislation;

“Processing”	has the meaning given to it in Data Protection Legislation and “Process” and “Processed” will be construed accordingly;
“Restricted Countries”	any country outside the European Economic Area;
“Sensitive Personal Data”	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
“Subject Access Request”	a request made by a Data Subject to access his or her own Personal Data in accordance with rights granted in Data Protection Legislation.

- 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:
- [List the relevant categories of Data Subject, e.g. staff, customers, members of the public. For advice/guidance contact privacy@tfl.gov.uk]***
- A1.2.2 The Authority Personal Data to be Processed includes the following types of Personal Data and/or Sensitive Personal Data:
- [List the relevant types of Personal Data, e.g. names, email or postal addresses, telephone numbers, images, other unique identifiers. For advice/guidance contact privacy@tfl.gov.uk]***
- A1.2.3 The Authority Personal Data is to be Processed for the following purpose(s):
- [List and summarise the relevant purpose(s). For advice/guidance contact privacy@tfl.gov.uk]***
- A1.2.4 The Authority Personal Data is to be Processed in the following Restricted Countries:
- [Delete A1.2.4 where the Authority Personal Data will not be Processed in any Restricted Countries.]***

Where A1.2.4 does apply, list the relevant countries outside the European Economic Area (which includes all EU member states plus Norway, Iceland and Liechtenstein). For advice/guidance contact privacy@tfl.gov.uk

- A1.3 Without prejudice to the generality of Clause 22, the Service Provider shall:
- A1.3.1 process the Authority Personal Data only in accordance with instructions from the Authority to perform its obligations under the Contract;
 - A1.3.2 use its reasonable endeavours to assist the Authority in complying with any obligations under Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Authority to breach any of its obligations under Data Protection Legislation to the extent the Service Provider is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations;
 - A1.3.3 notify the Authority without undue delay if it determines or is notified that an instruction to Process Personal Data issued to it by the Authority is incompatible with any obligations under Data Protection Legislation to the extent the Service Provider is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations;
 - A1.3.4 maintain, and make available to the Authority on its request, documentation which describes the Processing operations for which it is responsible under this Contract including:
 - A1.3.4.1 the purposes for which Authority Personal Data is Processed;
 - A1.3.4.2 the types of Personal Data and categories of Data Subject involved;
 - A1.3.4.3 the source(s) of the Personal Data;
 - A1.3.4.4 any recipients of the Personal Data;
 - A1.3.4.5 the location(s) of any overseas Processing of Authority Personal Data;
 - A1.3.4.6 retention periods for different types of Authority Personal Data; and
 - A1.3.4.7 where possible a general description of the security measures in place to protect Authority Personal Data.
 - A1.3.5 where requested to do so by the Authority, or where Processing Authority Personal Data presents a specific risk to privacy, carry out a Data Protection Impact Assessment in accordance with guidance issued from time to time by the Information Commissioner (and any relevant requirements detailed in Data

Protection Legislation) and make the results of such an assessment available to the Authority;

- A1.3.6 without prejudice to any cyber security and/or payment card industry data security standard obligations in this Contract, take appropriate technical and organisational security measures that are satisfactory to the Authority from time to time, against unauthorised or unlawful Processing of Authority Personal Data and against accidental loss, destruction of, or damage to such Authority Personal Data;
- A1.3.7 without prejudice to any cyber security and/or payment card industry data security standard obligations in this Contract, provide the Authority with such information as the Authority may from time to time require to satisfy itself of compliance by the Service Provider (and/or any authorised sub-contractor) with Clauses A1.3.6 and A1.3.8, including, protocols, procedures, guidance, training and manuals. For the avoidance of doubt, this shall include a full report recording the results of any privacy or security audit carried out at the request of the Service Provider itself or the Authority;
- A1.3.8 notify the Authority without undue delay and in any event within 24 hours by written notice with all relevant details reasonably available of any actual or suspected breach of this Clause A1, including the unauthorised or unlawful Processing of Authority Personal Data, or its accidental loss, destruction or damage;
- A1.3.9 having notified the Authority of a breach in accordance with Clause A1.3.8, keep the Authority properly and regularly informed in writing until the breach has been resolved to the satisfaction of the Authority;
- A1.3.10 fully cooperate as the Authority requires with any investigation or audit in relation to Authority Personal Data and/or its Processing including allowing access to premises, computers and other information systems, records, documents and agreements as may be reasonably necessary (whether in relation to Processing pursuant to the Contract, in relation to compliance with Data Protection Legislation or in relation to any actual or suspected breach), whether by the Authority (or any agent acting on its behalf), any relevant regulatory body, including the Information Commissioner, the police and any other statutory law enforcement agency, and shall do so both during the Contract and after its termination or expiry (for so long as the Party concerned retains and/or Processes Authority Personal Data);
- A1.3.11 notify the Authority within two (2) Business Days if it, or any sub-contractor, receives:
 - A1.3.11.1 from a Data Subject (or third party on their behalf):
 - A1.3.11.1.1 a Subject Access Request (or purported Subject Access Request);

- A1.3.11.1.2 a request to rectify, block or erase any Authority Personal Data; or
 - A1.3.11.1.3 any other request, complaint or communication relating to the Authority's obligations under Data Protection Legislation.
 - A1.3.11.2 any communication from the Information Commissioner or any other regulatory authority in connection with Authority Personal Data; or
 - A1.3.11.3 a request from any third party for disclosure of Authority Personal Data where compliance with such request is required or purported to be required by law;
- A1.3.12 provide the Authority with full cooperation and assistance (within the timescales reasonably required by the Authority) in relation to any complaint, communication or request made as referred to in Clause A1.3.11, including by promptly providing:
 - A1.3.12.1 the Authority with full details and copies of the complaint, communication or request;
 - A1.3.12.2 where applicable, such assistance as is reasonably requested by the Authority to enable it to comply with the Subject Access Request within the relevant timescales set out in Data Protection Legislation; and
 - A1.3.12.3 where applicable, such assistance as is reasonably required by the Authority to enable it to comply with a request from a Data Subject to rectify, block or erase any Authority Personal Data.
- A1.3.13 when notified in writing by the Authority, supply a copy of, or information about, any Authority Personal Data. The Service Provider shall supply such information or data to the Authority within such time and in such form as specified in the request (such time to be reasonable) or if no period of time is specified in the request, then within two (2) Business Days from the date of the request;
- A1.3.14 when notified in writing by the Authority, comply with any agreement between the Authority and any Data Subject in relation to any Processing which causes or is likely to cause substantial and unwarranted damage or distress to such Data Subject, or any court order requiring the rectification, blocking, erasure or destruction of any Authority Personal Data; and
- A1.3.15 if required to do so by Data Protection Legislation, appoint a designated Data Protection Officer.

- A1.4 The Service Provider shall not share Authority Personal Data with any sub-contractor without prior written consent from the Authority and only where there is a written contract in place between the Service Provider and the sub-contractor which requires the sub-contractor to:
- A1.4.1 only Process Authority Personal Data in accordance with the Authority's instructions to the Service Provider; and
 - A1.4.2 comply with the same obligations which the Service Provider is required to comply with under this Clause A1 (and in particular Clauses 12.1, 16.1, 16.2, 18.1, 20.2, 22 and 23).
- A1.5 The Service Provider shall, and shall procure that any sub-contractor shall:
- A1.5.1 only Process Authority Personal Data in accordance with the Authority's instructions to the Service Provider and as reasonably necessary to perform the Contract in accordance with its terms;
 - A1.5.2 not Process Authority Personal Data for any other purposes (in whole or part) and specifically, but without limitation, reproduce or refer to it in training materials, training courses, commercial discussions and negotiations with third parties or in relation to proposals or tenders with the Authority;
 - A1.5.3 not Process Authority Personal Data in such a way as to:
 - A1.5.3.1 place the Authority in breach of Data Protection Legislation;
 - A1.5.3.2 expose the Authority to the risk of actual or potential liability to the Information Commissioner or Data Subjects;
 - A1.5.3.3 expose the Authority to reputational damage including adverse publicity;
 - A1.5.4 not allow Service Provider's Personnel to access Authority Personal Data unless such access is necessary in connection with the provision of the Services;
 - A1.5.5 take all reasonable steps to ensure the reliability and integrity of all Service Provider's Personnel who can access Authority Personal Data;
 - A1.5.6 ensure that all Service Provider's Personnel who can access Authority Personal Data:
 - A1.5.6.1 are informed of its confidential nature;
 - A1.5.6.2 are made subject to an explicit duty of confidence;
 - A1.5.6.3 understand and comply with any relevant obligations created by either this Contract or Data Protection Legislation; and

- A1.5.6.4 receive adequate training in relation to the use, care, protection and handling of Personal Data on an annual basis.
 - A1.5.7 not disclose or transfer Authority Personal Data to any third party without the Service Provider having obtained the prior written consent of the Authority (save where such disclosure or transfer is specifically authorised under this Contract);
 - A1.5.8 without prejudice to Clause A1.3.6, wherever the Service Provider uses any mobile or portable device for the transmission or storage of Authority Personal Data, ensure that each such device encrypts Authority Personal Data; and
 - A1.5.9 comply during the course of the Contract with any written retention and/or deletion policy or schedule provided by the Authority to the Service Provider from time to time.
- A1.6 The Service Provider shall not, and shall procure that any sub-contractor shall not, Process or otherwise transfer any Authority Personal Data in or to any Restricted Countries without prior written consent from the Authority (which consent may be subject to additional conditions imposed by the Authority).
- A1.7 If, after the Service Commencement Date, the Service Provider or any sub-contractor wishes to Process and/or transfer any Authority Personal Data in or to any Restricted Countries, the following provisions shall apply:
 - A1.7.1 the Service Provider shall submit a written request to the Authority setting out details of the following:
 - A1.7.1.1 the Authority Personal Data which will be transferred to and/or Processed in any Restricted Countries;
 - A1.7.1.2 the Restricted Countries which the Authority Personal Data will be transferred to and/or Processed in;
 - A1.7.1.3 any sub-contractors or other third parties who will be Processing and/or receiving Authority Personal Data in Restricted Countries;
 - A1.7.1.4 how the Service Provider shall ensure an adequate level of protection and adequate safeguards in respect of the Authority Personal Data that will be Processed in and/or transferred to Restricted Countries so as to ensure the Authority's compliance with Data Protection Legislation;
 - A1.7.2 in preparing and evaluating such a request, the Parties shall refer to and comply with applicable policies, procedures, guidance and codes of practice produced by the Parties and/or the Information Commissioner in connection with the Processing

of Personal Data in (and/or transfer of Personal Data to) any Restricted Countries;

A1.7.3 the Service Provider shall comply with any instructions and shall carry out such actions as the Authority may notify in writing when providing its consent to such Processing or transfers, including:

A1.7.3.1 incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) into this Contract or a separate data processing agreement between the Parties; and

A1.7.3.2 procuring that any sub-contractor or other third party who will be Processing and/or receiving or accessing the Authority Personal Data in any Restricted Countries enters into a data processing agreement with the Service Provider on terms which are equivalent to those agreed between the Authority and the Service Provider in connection with the Processing of Authority Personal Data in (and/or transfer of Authority Personal Data to) any Restricted Countries, and which may include the incorporation of the clauses referred to in A1.7.3.1.

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

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

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

A1.8.3 any breach of any obligation in relation to Authority Personal Data and/or negligence in relation to performance or non performance of such obligation shall be deemed a material breach of Contract;

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

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

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

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

- A1.9 Compliance by the Service Provider with this Clause A1 shall be without additional charge to the Authority.
- A1.10 Following termination or expiry of this Contract, howsoever arising, the Service Provider:
- A1.12.1 may Process the Authority Personal Data only for so long and to the extent as is necessary to properly comply with its non-contractual obligations arising under law (and will then comply with Clause A1.10.2);
 - A1.12.2 subject to Clause A1.10.1, shall;
 - A1.10.2.1 on written instructions from the Authority either securely destroy or securely and promptly return to the Authority or a recipient nominated by the Authority (in such usable format as and to the extent the Authority may reasonably require) the Authority Personal Data; or
 - A.10.2.2 in the absence of instructions from the Authority after 12 months from the expiry or termination of the Contract securely destroy the Authority Personal Data.
- A1.11 Authority Personal Data may not be Processed following termination or expiry of the Contract save as permitted by Clause A1.10.
- A1.12 For the avoidance of doubt, and without prejudice to Clause A1.10, the obligations in this Clause A1 shall apply following termination or expiry of the Contract to the extent the Party concerned retains or Processes Authority Personal Data.
- A1.13 The indemnity in Clause 18 shall apply to any breach of Clause A1 and shall survive termination or expiry of the Contract.
- A1.14 The Parties' liability in respect of any breach of Clause 22.1 and this Clause A1 insofar as they relate to fines, court awards, settlements and legal costs shall be unlimited.