

30.3 With respect of the Parties' rights and obligations under the Contract, the Parties acknowledge that the Authority is a Data Controller and that the Service Provider is a Data Processor.

30.4 Details of the Authority Personal Data to be Processed by the Service Provider and the purposes of such Processing are as follows:

30.4.1 Categories of Data Subject

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

Data directly associated to the Authority's customer and any interactions with the Authority relating to these Services

30.4.2 Categories of Authority Personal Data

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

Customer contact details, Oyster card numbers, order history (excluding payment information), interaction with the Authority Personnel via the service channel i.e. calls, correspondence etc

30.4.3 Purpose(s) of the Processing

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

- Ticketing Contact handling services as detailed in Schedule 4 (Service Scope Specification)

30.5 Without prejudice to the generality of Clause 30.1, the Service Provider shall:

30.5.1 process the Authority Personal Data only in accordance with instructions from the Authority to perform its obligations under the Contract;

30.5.2 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;

30.5.3 maintain, and make available to the Authority on its request, documentation, a central register or an inventory which describes the processing operations for which it is responsible and specifies: the purposes for which Authority Personal Data are processed including the legitimate interests pursued by the Authority or any Authority Group member where processing is based on this lawful basis; the categories of Personal Data and Data Subjects involved; the source of the Personal Data; the recipients of the Personal Data; and the location(s) of any overseas processing of those Personal Data;

30.5.4 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;

- 30.5.5 without prejudice to Clause 30.5.4, wherever the Service Provider uses any mobile or portable device for the transmission or storage of Authority Personal Data, ensure that each such device encrypts Authority Personal Data;
- 30.5.6 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 Clause 30.5.4 and 30.5.5, 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;
- 30.5.7 where requested to do so by the Authority, or where Processing Authority Personal Data presents a specific risk to privacy, carry out a Privacy Impact Assessment in accordance with guidance issued from time to time by the Information Commissioner (and any relevant statutory requirements) and make the results of such an assessment available to the Authority;
- 30.5.8 notify the Authority within two (2) Business Days if it, or any sub-contractor, receives:
- 30.5.8.1 from a Data Subject (or third party on their behalf):
 - 30.5.8.1.1 a Subject Access Request (or purported Subject Access Request);
 - 30.5.8.1.2 a request to rectify, block or erase any Authority Personal Data; or
 - 30.5.8.1.3 any other request, complaint for communication relating to the Authority's obligations under Data Protection Legislation;
 - 30.5.8.2 any communication from the Information Commissioner or any other regulatory authority in connection with Authority Personal Data; or
 - 30.5.8.3 a request from any third party for disclosure of Authority Personal Data where compliance with such request is required or purported to be required by law;
- 30.5.9 provide the Authority with full cooperation and assistance (within the timescales reasonably required by the Authority) in relation to any complaint, communication or request made as referred to in Clause 30.5.8, including by promptly providing:
- 30.5.9.1 the Authority with full details and copies of the complaint, communication or request; and
 - 30.5.9.2 where applicable, such assistance as is reasonably requested by the Authority to enable it to comply with the Subject Access Request within the relevant timescales set out in Data Protection Legislation.
- 30.5.10 when notified in writing by the Authority, supply a copy of, or information about, any relevant Authority Personal Data. The Service Provider shall supply such information or data to the Authority within such time and in such form as specified in the request (such time to be reasonable) or if no period of time is specified in the request, then within five (5) Business Days from the date of the request.
- 30.5.11 when notified in writing by the Authority, comply with any agreement between the Authority and any Data Subject in relation to any Processing which causes or is likely to cause substantial and unwarranted damage or

distress to such Data Subject, or any court order requiring the rectification, blocking, erasure or destruction of any Authority Personal Data;

- 30.6 The Authority remains solely responsible for determining the purposes and manner in which Authority Personal Data is to be Processed. The Service Provider shall not share any Authority Personal Data with any sub-contractor or third party without prior written consent from the Authority (in the Contract or otherwise) and unless there is a written contract in place with the sub-contractor which requires the sub-contractor or third party to:
- 30.6.1 only Process Authority Personal Data in accordance with the Authority's instructions to the Service Provider; and
- 30.6.2 comply with the same obligations with which the Service Provider is required to comply with under this Clause 30 (and in particular Clauses 20.1, 24.1, 24.2, 26.1, 28.1, 28.3, 30.1 and 31).
- 30.7 The Service Provider agrees that, and shall procure that any sub-contractor shall agree that, Authority Personal Data:
- 30.7.1 must only be Processed in accordance with the Authority's obligations to comply with Data Protection Legislation and by such of their personnel as need to view or otherwise access Authority Personal Data;
- 30.7.2 must only be used as instructed by the Authority and as reasonably necessary to perform the Contract in accordance with its terms;
- 30.7.3 must not be used for any other purposes (in whole or part) by any of them (and specifically but without limitation must not be copied or referred to in whole or part through training materials, training courses, discussions or negotiations or contractual arrangements with third parties or in relation to proposals or tenders with the Authority (or otherwise), whether on renewal of this Contract or otherwise, without the prior written consent of the Authority); and
- 30.7.4 must not be used so as to place the Authority in breach of Data Protection Legislation and/or to expose it to risk of actual or potential liability to the Information Commissioner, Data Subjects and/or reputational damage and/or to any order being made against the Authority preventing, suspending or limiting the Processing of Authority Personal Data.
- 30.8 The Service Provider shall, and shall procure that any sub-contractor shall:
- 30.8.1 not disclose or transfer Authority Personal Data to any third party or their own personnel unless necessary for the provision of the Services and, for any disclosure or transfer of Authority Personal Data to any third party, obtain the prior written consent of the Authority (save where such disclosure or transfer is specifically authorised under this Contract);
- 30.8.2 notify the Authority within 24 hours by written notice with all relevant details reasonably available of any actual or suspected breach of security and/or of the Contract and/or Clause 30 in relation to Authority Personal Data including unauthorised or unlawful access or Processing of, or accidental loss, destruction or damage of any Authority Personal Data;
- 30.8.3 keep the Authority properly and regularly informed consequently;

- 30.8.4 fully cooperate with the reasonable instructions of the Authority in relation to the Processing and security of Authority Personal Data in accordance with the Contract and in compliance with Data Protection Legislation (including procuring access to sub-contractor premises);
- 30.8.5 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 Data Protection Legislation or in relation to any actual or suspected breach), whether by the Authority (or on its behalf) any relevant regulatory body, including the Information Commissioner, the police, any other statutory law enforcement agency or otherwise 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);
- 30.8.6 take all reasonable steps to ensure the reliability and integrity of all Service Provider's Personnel who can/or do access Authority Personal Data;
- 30.8.7 ensure all Service Provider's Personnel who can/ do access Authority Personal Data are informed of its confidential nature and do not publish, disclose or divulge any of the Personal Data to any third party without the prior consent of the Authority;
- 30.8.8 ensure all Service Provider's Personnel who can/ do access Authority Personal Data have undergone adequate training in relation to the use, care, protection and handling of Personal Data in accordance with Data Protection Legislation and this Contract, understand such obligations and comply with them and ensure that such training is updated at reasonable intervals; and
- 30.8.9 comply during the course of the Contract with any written retention and/or deletion policy or schedule provided to it by the Authority from time to time.
- 30.9 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).
- 30.10 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:
 - 30.10.1 the Service Provider shall submit a written request to the Authority setting out details of the following:
 - 30.10.1.1 the Authority Personal Data which will be transferred to and/or Processed in any Restricted Countries;
 - 30.10.1.2 the Restricted Countries which the Authority Personal Data will be transferred to and/or Processed in;
 - 30.10.1.3 any sub-contractors or other third parties who will be Processing and/or receiving Authority Personal Data in Restricted Countries;
 - 30.10.1.4 how the Service Provider shall ensure an adequate level of protection and adequate safeguards in respect of the Authority Personal Data that will