TCN SCHEDULE 11

PROCESSING PERSONAL DATA

1 Processing Personal Data

This Schedule shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Authority at its absolute discretion.

1.1 The contact details of the Authority's Data Protection Officer are: **Redacted (Department for Transport)**, c/o Redacted (DVSA Representative of the DPO), Data Protection Manager, The Axis Building, 112 Upper Parliament Street, Nottingham NG1 6LP.

1.2 The contact details of the Supplier's Data Protection Officer are: **Redacted (Senior Solicitor, Reed Specialist Recruitment Limited)**, Academy Court, 94 Chancery Lane, London WC2A 1DT.

1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Schedule.

1.5 References in this Schedule 11 to the "Authority" shall be deemed to include, where relevant, DVA in accordance with clause 23.2 of the Agreement.

Description	Details

Identity of Controller for each Category of Personal Data	**The Authority is Controller and the Supplier is Processor**
	
	The Parties acknowledge that in accordance with Clause 23.3 to 23.16 and for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor of the following Personal Data:
	
	• driving theory test candidate information of the following types:
	  ○ full name and title
	  ○ address, telephone number and email address
	  ○ date of birth
	  ○ written signature
	  ○ gender
	  ○ disability, health conditions and learning difficulties, if a candidate notes that they have any and need reasonable adjustments for their theory test
	  ○ information provided by a candidate's non-standard accommodations assistant and translator which is used to establish their identity
	  ○ driving licence number
	  ○ type of test the candidate is taking
	  ○ the language that the candidate has asked to use when they take their test
	  ○ incidents relating to a candidate, including but not limited to health, safety and fraud
	  ○ audio recordings of tests
	  ○ test result
	
	The Supplier is Controller and the Authority is Processor
	
	• *NOT APPLICABLE*
	
	The Parties are Joint Controllers
	
	• *NOT APPLICABLE*
	
	The Parties are Independent Controllers of Personal Data
	
	The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:
	• Business contact details of Supplier Personnel

	• Business contact details of any directors, officers, employees, agents, consultants and contractors of the Authority (excluding the Supplier Personnel) engaged in the performance of the Authority's duties under this Agreement).
	• Personal Data provided by one Party who is Data Controller to the other Party who will separately determine the nature and purposes of its processing the Personal Data on receipt, being:
	  ○ where the Supplier has professional or regulatory obligations in respect of Personal Data received
	  ○ where a standardised service is such that the Authority cannot dictate the way in which Personal Data is processed by the Supplier (for example, Personal Data processed by the Supplier to comply with its on-site health and safety obligations)
	  ○ where the Supplier processes Personal Data to the Authority (for use by the Authority) for which the Supplier is already Controller (for example, redacted CCTV images / footage of certain candidates disclosed by the Supplier to the Authority in order that the Authority can prevent and detect possible fraud in relation to the driving theory test).

Duration of the processing	<u>The Supplier</u> The Supplier will be required to carry out the processing activities required under this Agreement for the duration of its term together with any post-termination supply period set out in the Agreement (if any) or otherwise agreed by the Parties in writing. <u>The Authority</u> The Authority will process: • the candidate Personal Data for the periods noted in its then current 'Book And Manage Your Theory Test: Privacy Notice' (as at the date of this Agreement, these periods are set out at section 5 of the DVSA Privacy Notice: https://www.gov.uk/government/publications/dvsa-privacy-notices/book-and-manage-your-theory-test-privacy-notice) and DVA Privacy Notice: https://www.infrastructure-ni.gov.uk/dfi-privacy • any candidate or third party Personal Data provided to it by the Supplier in relation to the Authority's counter-fraud obligations in accordance with the periods noted in the Authority's then current 'DVSA Counter-Fraud: Privacy Notice' (as at the date of this Agreement, these periods are set out at section 5 of the Privacy Notice): https://www.gov.uk/government/publications/dvsa-privacy-notices/dvsa-counter-fraud-privacy-notice) • other relevant incident data relating to the Services.
Nature and purposes of the processing	<u>The Supplier</u> In performing the Services, the nature of the processing by the Supplier will include any operation in relation to the Personal Data relating to the Services, being: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means). The purpose of this processing is for the Supplier to effectively perform the Services set out in this Agreement. <u>The Authority</u>

	In receiving the Services, the nature of the processing by the Supplier will include any operation in relation to the Personal Data relating to the Services, being: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means).
Type of Personal Data	The following types of personal data will be processed: • full name and title of candidate • address, telephone number and email address of candidate • date of birth of candidate • written signature • gender of candidate • disability, health conditions and learning difficulties, if candidate requests any reasonable adjustments for their theory test • information provided by a candidate's non-standard accommodations assistant and translator which is used to establish their identity • candidate's driving licence number • type of test being taking by candidate - if relating to an instructor theory test, this will also include the candidate's personal reference number • the language that candidate has asked to use when taking test • incidents relating to a candidate, including but not limited to health, safety and fraud • audio recordings of tests • test result
Categories of Data Subject	Categories of Data Subject include: • driving test theory candidates • staff (including volunteers, agents, and temporary workers) • translators • suppliers • contractors • Authority personnel • other delivery partners or authorised suppliers of the Authority in relation to the Services.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The data will be retained as per the FTTS retention schedule and/or the Supplier must ensure that all data is returned to the Authority including on termination of the contract and securely removed in compliance with the Schedule 2.4 Security Requirements from any systems they have been using to deliver services under the contract.

Annex: Joint Controller Agreement – *NOT APPLICABLE BUT DRAFTING BELOW INTENTIONALLY INCLUDED SHOULD THE PARTIES NEED TO AGREE PROVISIONS RELATING TO JOINT DATA CONTROLLER OBLIGATIONS AS A CHANGE UNDER CLAUSE 13 OF THE AGREEMENT IN THE FUTURE.*

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 1 (Joint Controller Agreement) in replacement of Clauses 23.3-23.16 (Where one Party is Controller and the other Party is Processor) and 23.18-23.28 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Authority]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Joint Controller Agreement (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of paragraph 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Data Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Authority each undertake that they shall:

(a) report to the other Party every three (3) months on:

(i) the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

that it has received in relation to the subject matter of the Agreement during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under this Agreement or is required by Law). For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its personnel who have access to the Personal Data and ensure that its personnel:

(i) are aware of and comply with their duties under this Annex 1 (Joint Controller Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(i) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its' obligations

under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3**. Data Protection Breach**

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event, by telephone, within one (1) hour of becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach and in writing within twenty-four (24) hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(i) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(ii) all reasonable assistance, including:

(a) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
(b) co-operation with the other Party including taking such reasonable steps as are directed by the Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(c) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;
(d) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Paragraph 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as if it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and by telephone, within one (1) hour of becoming aware of any Personal Data Breach and in writing within twenty-four (24) hours, in particular:

(i) the nature of the Personal Data Breach;
(ii) the nature of Personal Data affected;
(iii) the categories and number of Data Subjects concerned;
(iv) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
(v) measures taken or proposed to be taken to address the Personal Data Breach; and
(vi) describe the likely consequences of the Personal Data Breach.

4**. Audit**

4.1 The Supplier shall permit:

(a) the Authority, or a third-party auditor acting under the Authority's direction, to conduct, at the Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 1 and the Data Protection Legislation.
(b) the Authority, or a third-party auditor acting under the Authority's direction, access to premises at which the Personal Data is physically accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the

Agreement, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.
4.2 The Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures);
(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with this Agreement, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Authority may on not less than thirty (30) Working Days' notice to the Supplier amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

a) If in the view of the Information Commissioner, the Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Authority, then the Authority shall be responsible for the payment of such Financial Penalties. In this case, the Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such data incident. The Supplier shall provide to the Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such data incident;
b) If in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a breach that the Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Authority and its auditors, on request and at the Contractor's sole cost, full cooperation and access to conduct a thorough audit of such data incident.
c) If no view as to responsibility is expressed by the Information Commissioner, then the Authority and the Supplier shall work together to investigate the relevant data incident and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Schedule 8.3 (*Dispute Resolution Procedure)*.

7.2 If either the Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the **"Claim Losses"**):

a) if the Authority is responsible for the relevant breach, then the Authority shall be responsible for the Claim Losses;
b) if the Supplier is responsible for the relevant breach, then the Supplier shall be responsible for the Claim Losses: and
c) if responsibility is unclear, then the Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in Paragraphs 7.2-7.3 shall preclude the Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the breach and the legal and financial obligations of the Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 1 (*Joint Control Agreement*), the Authority shall be entitled to terminate this Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 33 *(Termination Rights*).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(i) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Agreement, and provide evidence of such due diligence to the other Party where reasonably requested; and

(ii) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by a Party for statutory compliance purposes or as otherwise required by this Agreement), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and any related policies.