VARIATION TO SERVICES AGREEMENT FORM

SERVICES AGREEMENT TITLE: Services Agreement relating to the Driver Certificate of Professional Competence, Taxi Schemes and Drink Drive Rehabilitation. Dated 29th November 2012.

SERVICE AGREEMENT NUMBER: DSA04512.

SERVICES AGREEMENT VARIATION NUMBER: Variation No. 6.

SERVICES AGREEMENT VARIATION TITLE: Services Agreement extension

SERVICE AGREEMENT REFERENCE: Extension of Services Agreement to 31 March 2021 and updates to Data Protection terms

BETWEEN: The Secretary of State for Transport and the Department for Infrastructure acting respectively through The Driver and Vehicle Standards Agency and the Driver and Vehicle Agency (Northern Ireland) (hereinafter called "**the Agencies**") and the Joint Approvals Unit for Periodic Training (hereinafter together called "**the Approval Body**").

The Services Agreement is varied as follows:

1. Extension of Services Agreement to 31 March 2021 and changes to the Data Protection terms (see SA Changes 1 April 2020 attached).
2. This variation shall be implemented from 1 April 2020.
3. Words and expressions in this variation shall have the meanings given to them in the Services Agreement.
4. The Services Agreement shall remain effective and unaltered except as amended by this variation.

Authorised to sign for and on behalf of the Joint Approvals Unit for Periodic Training

Signature:
XXXX Redacted under FOIA section 40

Date: 24/03/2020

Name in Capitals: **XXXX Redacted under FOIA section 40**

Address: **XXXX Redacted under FOIA section 40**

Authorised to sign for and on behalf of the Driver and Vehicle Standards Agency

Signature:
XXXX Redacted under FOIA section 40

Date: 25/03/2020

Name in Capitals: **XXXX Redacted under FOIA section 40**

Address: DVSA, BERKELEY HOUSE, CROYDON STREET, BRISTOL, BS5 0DA

Authorised to sign for and on behalf of the Driver and Vehicle Agency

Signature: **XXXX Redacted under FOIA section 40**

Date: 24 March 2020

Name in Capitals: **XXXX Redacted under FOIA section 40**

Address: DVA, Balmoral Road, Belfast BT12 6QL

SA Changes 1 April 2020

The following are changes to the Service Agreement effective from 1 April 2020 and take precedence over the Service Agreement.

1. DEFINITIONS

"Data Protection Legislation" means (i) the GDPR (General Data Protection Regulation) 2018, the LED (Law Enforcement Directive (Directive (EU) 2016/680)) and any applicable national implementing Laws as amended from time to time (ii) The DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy

"DPA" means the Data Protection Act 2018, and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner in relation to such legislation

"GDPR" General Data Protection Regulation *(Regulation (EU) 2016/679)*

"LED" Law Enforcement Directive *(Directive (EU) 2016/680)*

"Personal Data" means personal data as defined in the Data Protection Act 2018 which is supplied to one party by the other or obtained by one party from the other in the course of performing their obligations under this Agreement;

24. DATA PROTECTION AND DATA SECURITY

24.1 In relation to all Personal Data, the Approval Body and any Sub-Contractor shall at all times comply with Data Protection Legislation (DP Legislation) if necessary, including maintaining a valid and up to date registration or notification under DP Legislation covering the data processing to be performed in connection with the Services.

24.2 The Approval Body and any Subcontractor shall only undertake processing of Personal Data reasonably required in connection with the Services and shall not transfer any Personal Data to any country or territory outside the European Economic Area without prior written approval.

24.5 The Agencies may, at reasonable intervals, request a written description of the technical and organisational methods employed by the Approval Body or the Subcontractors referred to in clause 24.4. Within twenty (20) Working Days of such a request, the Approval Body shall supply written particulars of all such measures detailed to a reasonable level such that the Agencies can determine whether or not, in connection with the Personal Data, it is compliant with DP Legislation.

24.8 Subject to clause 24.9, each Party shall notify the other Party without delay if it, in connection with Personal Data processed under this MoU:

(a) receives a Subject Request (or purported Subject Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority;

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

(f) and in any event within 24 hours of becoming aware of a Personal Data Breach.

24.9 The Processor's obligation to notify under clause 23.9 shall include the provision of further information to the Controller in phases, as details become available.

Schedule 7 – Data Protection, Data Security, Freedom of Information, and Confidentiality

The Approval Body and any sub-contractors acting on its behalf shall as data processor acting on behalf of the Agencies, comply with Crown Commercial Services (CCS) mandatory data security requirements. These requirements include, but are not limited to, compliance with the Data Protection Act 2018 and the provision of assistance and co-operation to the Agencies in meeting their information disclosure obligations under the Freedom of Information Act 2000 and Environmental Information Regulations 2004.

7 Data Protection

7.1 The Parties acknowledge that for the purposes of the DP Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Schedule 7a. The only processing that the Processor is authorised to do is listed in Schedule 7a by the Controller and may not be determined by the Processor.

7.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the DP Legislation.

7.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

7.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule 7a, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 7a);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

A. are aware of and comply with the Processor's duties under this clause;

B. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

C. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

D. have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the DP Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

7.5 Subject to clause 7.6, the Processor shall notify the Controller immediately if it:

(a) receives a Data Subject Request (or purported Data Subject Request);
(b) receives a request to rectify, block or erase any Personal Data;
(c) receives any other request, complaint or communication relating to either Party's obligations under the DP Legislation;
(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
(f) becomes aware of a Data Loss Event.

7.6 The Processor's obligation to notify under clause 7.5 shall include the provision of further information to the Controller in phases, as details become available.

7.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under DP Legislation and any complaint, communication or request made under clause 7.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;
(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the DP Legislation;
(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
(d) assistance as requested by the Controller following any Data Loss Event;
(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

7.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
(a) the Controller determines that the processing is not occasional;
(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

7.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

7.10 Each Party shall designate its own data protection officer if required by the DP Legislation.

7.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;
(b) obtain the written consent of the Controller;
(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 7.11 such that they apply to the Sub-processor; and
(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

7.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

7.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

7.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 7a - Schedule of Processing, Personal Data and Data Subjects

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 Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are: InformationManagementSecurity@dvsa.gov.uk
2. The contact details of the Processor's Data Protection Officer are: **XXXX Redacted under FOIA section 40**
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Agency is the Controller and the Approval Body is the Processor.
Subject matter of the processing	The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide an approval and audit service to members of the public.
Duration of the processing	For the duration of the Service Agreement i.e. until March 2021 unless amended.

Nature and purposes of the processing	The nature of the processing means any operation such as 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) etc. The purpose is for the fulfillment of the contract to deliver statutory accreditation and audit services on behalf of the controller.
Type of Personal Data being Processed	DCPC, DDR and TDPT training centres, course approvals and compliance data - application forms, audit reports, emails between centre/responsible person, reports or findings from visit and records of corrective action taken. Contact names of trainer, phone number, email and name of training provider. Audit details - reports inc. centre, course and trainer name and contact details, and centre performance rating. The PCV trainer register - Trainer name, trainer address, trainer email address, trainer telephone number and evidence of training/qualifications/licences.
Categories of Data Subject	Members of the public delivering DCPC, DDR, TDPT or those on the PCV trainer register.
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	All data associated with the delivery of services will be returned to the controller if the SA expires or is terminated.