**Schedule 20 (Processing Data)**

1. Status of the Controller
   1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:
      1. “Controller” in respect of the other Party who is “Processor”;
      2. “Processor” in respect of the other Party who is “Controller”;
      3. “Joint Controller” with the other Party;
      4. “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

1. Where one Party is Controller and the other Party its Processor
   1. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.
   2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
   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:
      1. a systematic description of the envisaged Processing and the purpose of the Processing;
      2. an assessment of the necessity and proportionality of the Processing in relation to the Services;
      3. an assessment of the risks to the rights and freedoms of Data Subjects; and
      4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
   4. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
      1. Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
      2. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 18.4 of the Core Terms*,* 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:
         1. nature of the data to be protected;
         2. harm that might result from a Personal Data Breach;
         3. state of technological development; and
         4. cost of implementing any measures;
      3. ensure that:
         1. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
         2. it uses all reasonable endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
            1. are aware of and comply with the Processor’s duties under this Schedule 20, Clauses 18 (Data protection), 19 (What you must keep confidential) and 20 (When you can share information);
            2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
            3. 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 the Contract; and
            4. have undergone adequate training in the use, care, protection and handling of Personal Data;
      4. not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
         1. the transfer is in accordance with Article 45 of the UK GDPR (or section 73 of DPA 2018); or
         2. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the “**IDTA**”), or International Data Transfer Agreement Addendum to the European Commission’s SCCs (the “**Addendum**”), as published by the Information Commissioner’s Office from time to time, as well as any additional measures determined by the Controller;
         3. the Data Subject has enforceable rights and effective legal remedies;
         4. the Processor complies with its obligations under the Data Protection 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
         5. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;
      5. where the Personal Data is subject to EU GDPR, 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:
         1. the transfer is in accordance with Article 45 of the EU GDPR; or
         2. the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission’s decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the non-transferring Party;
         3. the Data Subject has enforceable rights and effective legal remedies;
         4. the transferring Party complies with its obligations under the Data Protection 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 non-transferring Party in meeting its obligations); and
         5. the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and
      6. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
   5. Subject to Paragraph 2.6 of this Schedule 20, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
      1. receives a Data Subject Access Request (or purported Data Subject Access Request);
      2. receives a request to rectify, block or erase any Personal Data;
      3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
      4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
      5. 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
      6. becomes aware of a Personal Data Breach.
   6. The Processor’s obligation to notify under Paragraph 2.5 of this Schedule 20 shall include the provision of further information to the Controller, as details become available.
   7. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 2.5 of this Schedule 20 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
      1. the Controller with full details and copies of the complaint, communication or request;
      2. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
      3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
      4. assistance as requested by the Controller following any Personal Data Breach; and/or
      5. assistance as requested by the Controller with respect to any request from the Information Commissioner’s Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.
   8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Schedule 20. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
      1. the Controller determines that the Processing is not occasional;
      2. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
      3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
   9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
   10. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
   11. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
       1. notify the Controller in writing of the intended Subprocessor and Processing;
       2. obtain the written consent of the Controller;
       3. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Schedule 20 such that they apply to the Subprocessor; and
       4. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
   12. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
   13. The Buyer may, at any time on not less than 30 Working Days’ notice, revise this Schedule 20 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 the Contract).
   14. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Buyer may on not less than 30 Working Days’ notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.
2. Where the Parties are Joint Controllers of Personal Data
   1. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Schedule 20 (*Processing Data*).

**Independent Controllers of Personal Data**

* 1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
  2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
  3. Where a Party has provided Personal Data to the other Party in accordance with Paragraph 3.2 of this Schedule 20 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
  4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
  5. The Parties shall only provide Personal Data to each other:
     1. to the extent necessary to perform their respective obligations under the Contract;
     2. in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
     3. where it has recorded it in Annex 1 *(Processing Personal Data).*
  6. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
  7. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
  8. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **(“Request Recipient”)**:
     1. the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
     2. where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
        1. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
        2. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
  9. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
     1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
     2. implement any measures necessary to restore the security of any compromised Personal Data;
     3. work with the other Party to make any required notifications to the Information Commissioner’s Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
     4. not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
  10. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*
  11. Personal Data shall not be retained or processed for longer than is necessary to perform each Party’s respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.
  12. Notwithstanding the general application of Paragraphs 2.1 to 2.14 of this Schedule 20 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 3.2 to 3.12 of this Schedule 20.

**Annex 1 - Processing Personal Data**

1. This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.
   1. The contact details of the Buyer’s Data Protection Officer are:

XXXXXX redacted under FOIA section No 40

XXXXXX redacted under FOIA section No 40

Email: XXXXXX redacted under FOIA section No 40

The contact details of the DVSA Data Protection Manager are:

XXXXXX redacted under FOIA section No 40

Driver and Vehicle Standards Agency,

The Axis Building, 112 Upper Parliament Street, Nottingham,NG16LP   
Phone: XXXXXX redacted under FOIA section No 40

Email: XXXXXX redacted under FOIA section No 40

* 1. The contact details of the Supplier’s Data Protection Officer are:

XXXXXX redacted under FOIA section No 40

Data Protection and Records Manager, XXXXXX redacted under FOIA section No 40

* 1. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
  2. Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with Paragraph 2 and for the purposes of the Data Protection Legislation, the Buyer is the Controller, and the Supplier is the Processor all data in relation to training providers, their personnel, training material, drivers/candidates engaged in the delivery of the Carriage of Dangerous Goods (ADR) qualification:   * Dangerous Goods Driver Training (DGDT) * Dangerous Goods Safety Advisor (DGSA) |
| Duration of the Processing | Three (3) years with an option for two 12-month extensions (3+1+1) |
| Nature and purposes of the Processing | DVSA will also need to collect and record the Supplier’s organisation details including but not limited to name, address, telephone number, staff email addresses and financial data.  This data will be collected, recorded, stored and destroyed by the Supplier.  for the purposes of delivering the Statutory ADR Scheme.  DVSA will collect, record, structure, store, alter, use, disclosure by transmission, restriction and erasure or destruction of data (whether or not by automated means) for the purposes of management of audit services. |
| Type of Personal Data | **Supplier:** Organisation name, address, telephone number Staff name, telephone number and email address  **Training Providers:**  Organisation name, address, telephone number Responsible person name, telephone number, email address Primary contact name, telephone number, email address Instructor’s full name Instructor qualifications/credentials  **Candidates:** Candidate’s full name, postal address, telephone number, email address, nationality, date of birth, photograph of the candidate (for the purposes of issuing a ADR Driver Training Certificate) |
| Categories of Data Subject | Supplier’s staff  Customers: Training providers and candidates |
| Plan for return and destruction of the data once the Processing is complete  UNLESS requirement under law to preserve that type of data | In accordance with DfT’s Terms and Conditions and the Exit Plan detailed in Paragraph 4.1 of Schedule 30. |
| Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract | United Kingdom is preferred.  Scottish Qualifications Authority  The Optima Building, 58 Robertson Street, GLASGOW G2 8DQ |
| Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under this Contract Agreement against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach | The supplier will be required to comply with all applicable requirements of the Data Protection Legislation (including the UK General Data Protection Regulation 2016/679 following the UK exit) (“UK GDPR”), the Law Enforcement Directive (Directive (EU) 2016/680), and all applicable Law about the processing of personal data and privacy).  The Supplier shall ensure that the infrastructure, software and end user devices (if applicable) are fully encrypted, have anti-virus software (malware protection) installed, which is maintained and allows the safe and secure transfer of data.  The Supplier shall ensure that all infrastructure, software and end user devices (if applicable) have up to date Microsoft Operating Systems.   DVSA reserves the right to monitor the Supplier’s performance and equipment (including subcontractors working for the Supplier in delivery of the contracted service) by measuring adherence to service levels as set out in the Specification, the Contract or notified to the Supplier at any time in writing (which shall include Email). This includes periodic audits conducted by DVSA or an approved third party.  The Supplier shall ensure that all IT equipment used for the services provided must be used for professional purposes only.  The Supplier shall conduct baseline security checks on staff (including subcontractors working for the Supplier in delivery of the contracted service) including but not limited to identity, employment history (past 3 years), national and immigration (right to work) status and unspent criminal record.  The Supplier shall provide details of security awareness training given to and completed by all staff (including subcontractors working for the Supplier in delivery of the contracted service. The Supplier shall keep DVSA indemnified against all losses incurred by it in respect of any breach of Data Protection by the Supplier. Awareness of and response to incidents involving data and potential breaches of personal data must have defined incident notification and management processes compliant with GDPR (72 hours to notify).  The Supplier shall retain and produce when required such accounts, documents (including working documents), files and records as DVSA may request in connection with the Contract, at any time during the Contract and for a period of 90 days from the date of expiry or termination or such longer period as may be agreed between DVSA and the Supplier in writing at or before the commencement of the Contract.  The Supplier shall ensure that DVSA data and relevant files associated with the Contract are returned as part of the Exit Plan on expiry or termination of this Contract. Any data generated that is not returned must be securely erased and evidence provided to DVSA.  SQA operates Sophos Anti-Virus protection against malware and has in place resilient firewalls.  SQA devices are fully encrypted and have up to date Microsoft Operating Systems, currently Windows 10.  A managed security operations centre is in place.  Systems running supported software are patched within 14 days.  Access controls and password protection apply to all SQA systems. Access is managed in accordance with the ‘need to know’ principle and following established joiners, movers and leavers processes.  SQA’s Microsoft Office 365 tenancy is protected by multi-factor authentication: requiring username, password and token code for access.  The team providing the services is ISO27001:2013 certified.  SQA has in place a suite of information governance, information security and data protection policies, which are reviewed on a regular basis and updated where necessary.  As part of the employee recruitment process, right to work checks are undertaken and confirmation provided of unspent criminal convictions. Employees and appointee contracts include confidentiality requirements.  Employees must complete data protection and information security training within 4 weeks of starting.  SQA has a retention and disposal policy supported by established processes and records retention schedule. As well as established security incident management procedures.  For further information, please see the data protection policy embedded:  XXXXXX redacted under FOIA section No 43 |

**Annex 2 - Joint Controller Agreement**

**Not Used**