Joint Schedule 11 (Processing Data)

1. Definitions

"Controller"	has the meaning given in the GDPR;
"Data Protection Legislation"	means i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; ii) the DPA 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;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679)
"Joint Control"	means where two or more Controllers jointly determine the purposes and means of processing
"Personal Data"	has the meaning given in the GDPR to which the Processor has access to from time to time in the course of the Services

Part B - JOINT CONTROL OF PERSONAL DATA

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data which has been identified in Joint Schedule 11 as 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 Part B in replacement of Clause 14 (Data Protection) of the Core Terms. Accordingly, the Parties each undertake to comply with the applicable Data Protection Law in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the 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 Memorandum of Understanding (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 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 Law 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 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 Law;

(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 to (v); and

(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 Law.

(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 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 's duties under this Annex 1 (Data Sharing 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 Law;

(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 Law, 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 Law and shall not perform its obligations under this Part in such a way as to cause the other Joint Controller to breach any of it's obligations under

applicable Data Protection Law 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 within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Authority 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 Laws;

(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 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 within 48 hours of the Personal Data Breach relating to the Personal Data Breach, 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 Provider'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 Provider's data security and privacy procedures relating to Personal Data, its compliance with this Part B and the Data Protection Law.
(b) the Authority, or a third-party auditor acting under the Authority's direction, access to premises at which the Personal Data is 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 Provider to assist in the provision of the Services.

4.2 The Authority may, in its sole discretion, require the Provider to provide evidence of the Provider'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 the 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 Provider 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 Provider for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

a) If in the view of the Information Commissoner, 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, Suppliers (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 Provider'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 Supplier'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 Provider 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 Clause 34 (Resolving Disputes) of the Core Terms.

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 Provider shall be responsible for the Claim Losses: and
c) if responsibility is unclear, then the Authority and the Provider shall be responsible for the Claim Losses equally.

7.4 Nothing in paragraphs 9.2-9.3 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 A, the Authority shall be entitled to terminate this Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 10 (Ending the Contract) of the Core Terms.

9. Sub-Processing

9.1 In respect of any Processing of Personal 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 Law.

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 Law and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the 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 Law and its privacy policy.

Annex 1 – Record of Personal Data

1. The contract details of the Authority Data Protection Officer is:

   XXXXXX – redacted under FOIA section 40 – Personal Information

2. The contract details of the Supplier Data Protection Officer is:

   XXXXXX – redacted under FOIA section 40 – Personal Information

3. Any such further instructions shall be incorporated into this table.

Call-Off Contract:	**RM6096, Lot 3** **K280021055: Vehicle Lease, Fleet Management & Flexible Rental Solutions**
Date:	**18 February 2021**
Description Of Authorised Processing	**Details**
Identity of the Joint Controller	The Parties acknowledge that they are joint Controllers for the purposes of the Data Protection Legislation in respect of the personal data of end users and Part B (Joint Control Of Personal Data) to this Schedule shall apply in replacement of Clause 14 of the Core Terms.
Provision of Personal Data	The following Personal Data is provided by the Supplier to the Buyer: Employee details and vehicle allocation details through Knowles Associates Limitedfleet management system/portalEmployee details and P11d liabilities through Knowles Associates Limitedfleet management system/portal The following Personal Data is provided by the Buyer to the Supplier: Staff Name Telephone Number Email address Home address Employee Number Vehicle registration number
Uses of Personal Data under this Agreement	The Supplier uses personal data to provide appropriate fleet management services to DVSA drivers under the terms of contract K280021055 The Supplier establishes if and when to disclose personal data to third parties in order to perform services under the contract e.g. vehicle delivery, repair or accident management

	of claims etc. (i.e. the Supplier decides to pass on the name and contact details of a driver to a garage when a driver calls the Supplier service desk to book their vehicle in for repair or in the case of an Accident when the driver needs to be recovered by the AA and a hire car arranged for them).
Duration of the processing and retention.	DVSA requires that all personal data should be retained by the Supplier no longer than six full fiscal years plus after one year after the expiry date of the contract; this is to enable full reporting of P11d liabilities, and appropriate management of vehicles, fines and accident claims. Full reasoning as to why data should be kept for longer than the contract expiry dates as follows: • The overall contract may end; however the Supplier continues to maintenance manage vehicles under the individual vehicle contracts, therefore will require driver details for the individual vehicles concerned in order to arrange recalls, MOT, Tax, General Maintenance Service and Repairs, if we delivered a vehicle to a driver just prior to termination of the contract then that vehicle could remain on contract with the Supplier for up to 5 years (if extended) so we need to retain the driver data to manage this. • HMRC can audit P11d for up to 6 years plus the current year following submission, therefore the data is generally held for a minimum of 6 years plus one, likewise should DVSA have any queries regarding the P11d submission we would need to keep the data to assist. Removal of all P11d and P46 data prematurely would impact DVSA ability to resolve any future disputes in this area. • Future fines for vehicles out on contract will continue to be managed by the Supplier and fines such as speeding offences, redirected fines etc. would need to be sent to the driver in the same way they are managed currently. • An ongoing Accident claim can take a number of years to resolve to settlement, there is also the possibility of a claim coming through from the third party involved up to 6 years after the accident occurred and therefore the details of incidents reports are retained for 6 years. Arrangements will be agreed between DVSA and the Supplier prior to contract expiry for the full transfer of DVSA data held by the Supplier at the point of contract expiry.

Nature and purposes of the processing	• Contact with a driver in order to arrange delivery or collection of a lease or hire vehicle. • Collection of accident details, including name, phone number, address and accident details. • Contact with a driver in order to arrange mobile tyre fitting or glass replacement services. • P11d reporting –The Supplier updates the Knowles Associates Limited fleet management system/portal P11d System (includes driver email address and staff number); this is provided to the Supplier via emailas requested. • Nominations of Notices of Intended Prosecutions (NIP) - sent to the driver's home address.
Type of Personal Data	• Staff Name • Telephone Number • Home Address • Email Address • Payroll Number • Vehicle Registration Number
Categories of Data Subject	DVSA drivers would expect to exercise their rights against the visible outsourced service provider, Knowles Associates Limited, as opposed to their employer, DVSA. The Supplier would be fielding and responding to Data Subject Access Request's.