THIRD PARTY PRODUCT TERMS - VRM LOOKUP

1. INTRODUCTION

1.1 These Third-Party Product Terms ("Terms") detail the provision by Klipboard to Customer of Vehicle Registration Mark Lookup functionality ("VRM Lookup") within its Products.

1.2 The Products incorporate and rely on certain services, software and/or technology provided by independent third-party service providers (each a "Third Party Provider").

1.3 Capitalised terms used in these Terms, but not defined in these Terms, are defined in the Klipboard Section A Terms and Conditions.

1.4 The Customer acknowledges and agrees that the obligations set out in this Terms are owed directly to the respective Third-Party Provider and form part of and are incorporated into the Agreement between Klipboard and the Customer. A Customer's continued use of the Products constitutes its acceptance of these Terms.

2. STRUCTURE OF THESE TERMS

These Terms consists of the following:

Part A: General provisions applicable to all Third-Party providers; and
Part B: Flow down terms of each specific Third-Party Provider.

PART A:
GENERAL PROVISIONS APPLICABLE TO THIRD PARTY PROVIDERS

1. BINDING NATURE:

1.1 You agree to comply with the flow-down terms of each Third-Party Provider listed below. Any breach by you of those terms will be deemed a breach of your Agreement with Klipboard.

2. NO WARRANTY OR LIABILITY BY THIRD PARTIES:

Customer acknowledges that the services of Third-Party Providers are provided as is and without warranty of any kind, whether express, implied, statutory or otherwise and Klipboard disclaims all implied warranties including any implied merchantability, fitness for a particular purpose or non-infringement to the fullest extent permitted by law.

3. CHARGES AND PAYMENT:

3.1 Klipboard shall invoice Customer periodically or monthly (whichever is applicable) for access to and use of the Products as set out in the relevant Quotation.

3.2 The Charges may be varied at any time on notice from Klipboard to Customer. Without limitation, Klipboard reserves the right to vary Charges to reflect any increase in costs from a relevant Third-Party Provider.

3.3 Customer is responsible for checking all invoices and Charges in relation to its use of the Product. Any Dispute solely relating to Charges for the Product must be raised within 7 days of receipt of an invoice from Klipboard, and with sufficient information to enable Klipboard to raise any related dispute with the relevant Third-Party Provider. Nothing in this clause shall entitle Customer to withhold payment of any invoices. Customer must act reasonably and in good faith in relation to any Third-Party Service disputes or Charge queries.

4. SUSPENSION AND TERMINATION:

4.1 Klipboard may suspend or terminate Customer's access to or use of the Product immediately without notice:

4.1.1 on instruction or at the request of a Third-Party Provider;

4.1.2 in the event of a suspected breach of or where required by any acceptable use policy, applicable laws or regulations of a Third-Party Provider;

4.1.3 in the event of a material breach of these Terms by a Customer.

5. GENERAL:

5.1 Klipboard may make changes to these Third-Party Product Terms:

5.1.1 at any time following an update in the terms and/or requirements of a relevant Third-Party Provider;

5.1.2 at any time following a change in law or regulation in relating to the use or provision of the Third-Party Products; or

5.1.3 on not less than 30 days' prior notice

and the latest version of these Terms shall apply.

5.2 The latest version of these Third-Party Product Terms is available at https://www.kerridgecs.com/page/site/documentation#access

PART B:

FLOW DOWN TERMS OF EACH SPECIFIC THIRD-PARTY PROVIDER.

PART B.1 – HAYNESPRO FLOW DOWN TERMS

1. Description of Services:

Customer is granted a licence for access to and/or use the following services and functionality from HaynesPro:

(a) VRM (vehicle registration lookup);

(b) Workshop Technical Data;

(c) MOT Expiry Data;

(d) Reporting.

(the "HaynesPro Services")

2. Customer Obligations:

Customer acknowledges and agree that:-

2.1 access to and use of the HaynesPro Services is at its sole risk and that the services are provided on a "as is" and "as available" basis.

2.2 the content and accuracy of the data is outside the control of HaynesPro;

2.3 HaynesPro has the right (pursuant to Contracts (Rights of Third Parties) Act 1999) to bring proceedings directly against the Customer for any breach of the restriction of use of data imposed by HaynesPro.

2.4 It shall not:

(a) Use and/ or otherwise access or store the data obtained from the HaynesPro Services other than strictly necessary for the permitted purpose of the services.

(b) Systematically download data or store data from the HaynesPro Services in a way that allows for later "offline" retrieval without access to the HaynesPro Services as stored on HaynesPro's systems'

(c) Create any copy of the data access via the HaynesPro Services and/or stored on the systems of HaynesPro in whole or in part; or

(d) Use the data accessed from the HaynesPro Services to provide credit reference services or moveable asset enquire services to any other person.

PART B.2 – DVLA DATA FLOW DOWN TERMS

1. Description of Services:

The services and/or functionality provided by the Driver and Vehicle Licensing Agency (“DVLA”) within the Products are the transmission of DVLA derived data to the Customer. (“DVLA Services”).

2. Definitions:

2.1 For purposes of the DVLA Services, unless the context otherwise indicates the following words shall have the meanings given to them below:

"Agreement" means this written agreement between the Supplier and the Customer consisting of these clauses and any attached Schedules and Annexes.

"Annexes" means an annex attached to, and forming part of, this Agreement.

"Anomaly" means a problem relating to information contained in the Data that relates to a specific vehicle. Anomalies may include, but not be limited to:

a) a mismatch between new Data provided by Supplier to the Customer and Data previously provided by Supplier to the Customer;

b) a mismatch between Data provided by Supplier to the Customer and Data already held by the Customer which has been sourced from another organization; and

c) a dispute between the registered vehicle keeper, dealer or manufacturer in relation to the vehicle that relates to the Data.

"Caching" means the process of storing Data in a temporary storage area (a "Cache") for further use within a defined period of time. A Cache is a hardware or software component that stores Data so that future requests for that Data can be served faster.

"Commercial Manager" shall have the meaning given in clause 4.1(b)(i).

"Confidential Information" means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person, Trade Secrets, Intellectual Property Rights, or know-how of either Party and all materials within the meaning of Data Protection Legislation. Confidential Information shall not include information which:

i) was public knowledge at the time of disclosure (otherwise than by breach of clause 7);

ii) was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party;

iii) is received from a third party (who lawfully acquired it) without restriction as to its disclosure;

iv) is independently developed without access to the Confidential Information;

v) any information which is agreed by the Parties in writing not to be Confidential.

"Conviction" means, other than for minor road traffic offences, any previous or pending prosecutions, convictions, cautions and binding-over orders (including any spent convictions as

contemplated by section 1(I) of the Rehabilitation of Offenders Act 1974 (as amended) by virtue of the exemptions specified in Part II of Schedule 1 of the Rehabilitation of Offenders Act 1974 (Exemptions) Order 1975 (SI 1975/1023) (as amended) or any replacement or amendment to that Order, or being placed on a list kept pursuant to the safeguarding of Vulnerable Groups Act 2006 (as amended).

"Crown" means the government of the United Kingdom (including the Northern Ireland Executive Committee and Northern Ireland Departments, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers, government departments, government agencies, particularly executive agencies and non-departmental government bodies.

"DVLA-derived Data" means Data from the vehicles register that is to be provided to the Customer more particularly described in clause 3 of this Section. Unless otherwise specified, references to "Data" in this Section shall mean "DVLA-derived Data".

"Data Controller" has the meaning given to that term (or the term "Controller") in Data Protection Legislation, means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State Law, the controller or the specific criteria for its nomination may be provided for by Union or Member State Law.

"Data Manager" shall have the meaning given in clause 4.1(b)(ii).

"Data Processor" has the meaning given to that term (or the term "Processor") in Data Protection Legislation and means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

"Data Protection Legislation" means:

(i) the General Data Protection Regulation (Regulation (EU) 2016/679), the Law Enforcement Directive (LED) and any applicable national implementing Laws as amended from time to time;

(ii) the Data Protection Act 2018 (as amended) 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.

"Data Subject" has the meaning given to that term in Data Protection Legislation, means an identified or identifiable natural person, directly or indirectly through Personal Data.

"Data Subject Access Request" means a request made by, or on behalf of, a Data Subject in accordance with the rights granted, pursuant to Data Protection Legislation to access their Personal Data.

"Days" shall mean calendar days, save where the context otherwise requires.

"Default" means any breach of the obligations of the relevant Party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or negligent statement of the relevant Party or the Staff in connection with or in relation to the subject matter of this Agreement and in respect of which such Party is liable to the other.

"Dispute" means any dispute, difference or question of interpretation arising out of or in connection with this Agreement, including any dispute, difference or question of interpretation relating to the Service or protection of the Data or any matter where this Agreement directs the Parties to resolve any issue by reference to the Dispute Resolution Procedure.

"DVLA" means the Secretary of State for Transport, his Department, Executive Agencies of the Department and persons authorised to act on his behalf.

"Equipment" means the Customer's equipment, plant, materials and such other items used by the Customer in the performance of its obligations under this Agreement, or otherwise used to access or store Data.

"FOIA" means the Freedom of Information Act 2000 (as amended) 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 or relevant government departments in relation to such regulations.

"Fraud" means any offence under Laws creating offences in respect of fraudulent acts or at common law in respect of fraudulent acts in relation to this Agreement or defrauding or attempting to defraud or conspiring to defraud the Crown.

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679).

"Industry Best Practice" means at any time the exercise of that degree of skill, care, diligence, prudence, efficiency, foresight, standards, practices, methods, procedures and timeliness which would be expected at such time from a leading and expert company within the industry, such company seeking to comply with its contractual obligations in full and complying with all applicable Laws.

"Intellectual Property Rights" means patents, inventions, trademarks, service-marks, logos, design rights (whether registrable or otherwise), know how, confidential information, trademarks discoveries, inventions, applications for any of the foregoing, copyright, database rights, domain names, trade or business names, moral rights and other similar rights or obligations whether registrable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off. In each case it includes these rights and interests in every part of the world for their full terms, including any renewals and extensions, and the right to receive any income from them and any compensation in respect of their infringement.

"Intermediary" means an organization who receives the Data from the Customer and uses it to provide products and services to other organisations (to be referred to as "Third Party Customers") that demonstrate Reasonable Cause in accordance with 3.1, 5.5(ii) and Schedule 4 of this Agreement.

"Key Staff" means those persons listed in ANNEX A (CUSTOMERS KEY STAFF) completed by the Customer in accordance with clause 4.1

"Law" means any law, statute, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978 (as amended) bye-law, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972 (as

amended), regulatory policy, guidance or industry code, judgment of a relevant court of law, directives or requirements or any Regulatory Body which the Customer is bound to comply.

"LED" means the Law Enforcement Directive (Directive (EU) 2016/680).

"Loss" of any Data means any instance where the Data has been lost, misplaced or destroyed, where unauthorised persons have gained or been allowed access to the Data, or where, due to the breakdown of, or failure to comply with protective security policies or measures including technical and procedural measures, there is a potential that unintended or unauthorised access to the Data may be possible.

"Malicious Software" means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, Data or other information, executable code or application software, macros, whether or not its operation is immediate or delayed, and whether the Malicious Software is introduced wilfully, negligently or without knowledge of its existence.

"Material Breach" means a breach (including an anticipatory breach) which is not minimal or trivial in its consequences to the other Party. In deciding whether any breach is material regard shall be had to whether it occurs by some accident, mishap, mistake or misunderstanding.

"Month" means calendar month.

"Party" and "Parties" means a party to this Agreement.

"Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data Breach" means any event that results in, or may result in a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Premises" means the location where the Data is to be supplied to the Customer, or accessed, stored or destroyed by the Customer.

"Processing" has the meaning given to that term in Data Protection Legislation (and related terms such as 'Process' have corresponding meaning) Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, 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.

"Reasonable Cause" means the purpose for which the Data is provided by the DVLA to the Supplier and by the Supplier to the Customer via the Service as stated in clause 3.1 of this Agreement.

"Requestor" means a person who is making an enquiry for Data about a particular vehicle, using products or services provided by the Customer or an Intermediary or a Third Party Customer in accordance with 3.1 and Schedule 4 of this Agreement.

"Regulatory Bodies" means those government departments and regulatory, statutory and other entities, committees, ombudsmen and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Agreement or any affairs of the DVLA and **"Regulatory Body"** shall be construed accordingly.

"Related Persons" means the Customer, its directors, the Commercial Manager, the Data Manager and the other Key Staff.

"Relevant Conviction" means a Conviction which the Customer, acting reasonably and in accordance with Industry Best Practice, deems to preclude a person from being involved in any way with use of the Data.

"Removable Media" means all physical items and devices that can carry and transfer electronic information. Examples include but are not limited to DVDs, CD-ROMs, floppy disks, portable hard disk drives, USB memory sticks, flash drives, portable music and video players including mobile phones, hand held devices such as Smartphones and Personal Digital Assistants.

"Schedule" means a schedule attached to, and forming part of, this Agreement.

"SMMT" means Society of Motor Manufacturers and Traders.

"Services" means the transmission of the DVLA-derived Data to the Customer, the Customer first having shown Reasonable Cause.

"Staff" means all persons employed by a Party to perform its obligations under this Agreement together with the Party's servants, agents, suppliers and sub-contractors used in the performance of its obligations under this Agreement.

"Sub-Contracting" means the Customer appointing a third party to provide services on behalf of the Customer providing an appropriate Sub-Contracting agreement is in place. The Customer will retain Data Controller responsibilities while the Sub-Contractor is a Data Processor. The Customer shall be responsible for the acts and omissions of its Sub-Contractors as though they are its own.

"Sub-Contractor(s)" means a Third Party appointed by the Customer to provide services on behalf of the Customer. The Customer will retain Data Controller responsibilities while the Sub Contractor is a Data Processor.

"Supplier" means the DVLA

"Third Party Customer" means any organisation that:

a) is not an Intermediary; and

b) receives Data from the Customer or an Intermediary providing Reasonable Cause can be demonstrated, in accordance with clause 3.1, 5.5(b)(ii) and Schedule 4 of this Agreement.

"VIN" means Vehicle Identification Number.

"VRN" means Vehicle Registration Number.

"Working Day" means a day (other than a Saturday or Sunday) on which banks are open for general business in the City of London

2.2 The interpretation and construction of this Agreement shall be subject to the following provisions:

(a) words importing the singular meaning include where the context so admits the plural meaning and vice versa;

(b) words importing the masculine include the feminine and the neuter;

(c) reference to a clause is a reference to the whole of that clause unless stated otherwise;

(d) reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent enactment, modification, order, regulation or instrument as subsequently amended, modified or re-enacted;

(e) reference to any person shall include natural persons and partnerships, firms and other incorporated bodies and all other legal persons of whatever kind and howsoever constituted and their successors and permitted assigns or transferees;

(f) the words "include", "includes" and "including" are to be construed as if they were immediately followed by the words "without limitation", and any obligation on a Party to do any act or thing includes an obligation to procure that it be done and any obligation on a Party not to do any act or thing includes an obligation not to allow that act or thing to be done and to use its best endeavours to prevent such act or thing being done by a third party; and

(g) headings are included in this Agreement for ease of reference only and shall not affect the interpretation or construction of this Agreement

3. Provision of data:

3.1 Purpose for which DVLA-derived Data is Provided:

(a) The Customer will provide the Supplier with a statement detailing the type of business it conducts and a description of products or services it offers to its customers that involve the use of Data.

(b) Organisations that cannot prove a Reasonable Cause for accessing the Data will not be considered further.

(c) Categories of business that may meet this pre-requisite include, but may not be limited to, vehicle checking companies. In order to demonstrate Reasonable Cause, products or services delivered by any Service customer using the Data must have benefit to one or more of the following:

(i) improving vehicle and road safety;

(ii) reducing vehicle crime;

(iii)Consumer Protection;

(iv)Environmental impact (greener transport);

(v)facilitating best practice and due diligence compliance.

(d) The Customer will notify Supplier of any changes to their business need for access to the Data.

(e) The requirements of clause D4 (Transfer of the Data outside the UK) apply to the Customer's backup or disaster recovery sites.

(f) The Customer will not sell or permit the Data to be sold to any third party without the Supplier's prior written consent. The Customer acknowledges and accepts that such consent may be subject to **DVLA pass-down consent**.

3.2 **Customer Obligations:**

(a) During the term of this Agreement, the Customer shall use the Data detailed in this Agreement only for the Purpose (and with Reasonable Cause) and in accordance with any instructions of the Supplier.

(b) Without prejudice to this Agreement, the Customer shall research, identify and notify Supplier without delay of the existence of any situation or envisaged development that will influence the ability of the Customer to purchase or use the Data over the term of the agreement.

(c) The Customer is only permitted to disclose Data (relating to a specific vehicle) to a Third Party Customer or intermediary in the following cases:

(i) if the VRN relates to a vehicle where the Requestor is either owner or registered keeper of that vehicle; or

(ii) if the VRN relates to a vehicle that is being or intended to be marketed or offered for sale; or

(iii) if the Requestor has a genuine and legitimate interest in determining the provenance, statue or technical specification of that vehicle; or

(iv) where confirmation of the vehicle identity is a pre-requisite for the Data being accessed by the Requestor.

(v) If the VRN relates to a vehicle that the Requestor, Intermediary or Third Party Customer has involvement in providing services to. This may include where the Requestor, Intermediary or Third Party Customer:

- Has sold, repaired, modified, or services that vehicle;
- Is providing an insurance quotation or vehicle finance for that vehicle;
- Is involved in reducing crime for that vehicle.

(d) To restrict excessive Data being disclosed to a Third party Customer, Intermediary or Requestor, the Customer is only permitted to disclose the following Data free of charge:

Make	Year of Manufacture
Model	Export Marker
Colour	Vehicle Type Approval
Date of First Registration	Wheelplan
Body Type	Vehicle/Revenue Weight
Fuel Type	Tax Data
Engine Capacity	MOT Data
CO2	Gearbox (Obtained from SMMT)
BHP (obtained from SMMT)	

(e) Where there is a change to, or additional use of the Data from that stated in clause 3.1, the Customer shall obtain the Supplier's prior written approval before using the Data for any other

purpose. The Customer acknowledges and accepts that such approval may be subject to DVLA pass-down consent.

(f) The Customer shall provide any information reasonably requested by the Supplier with respect to the use made of the Data.

(g) Further details on the use of the Data and Vehicle Identification Number (VIN) are shown in Schedule 5 (restrictions on Disclosure of Vehicle Identification Number).

3.3 **Customer Criteria:**

(a) The Customer shall ensure that each member of the Customer's Staff comply with any notification requirements under the Data Protection Legislation and will duly observe all their obligations under Data Protection Legislation which arise in connection with the Agreement.

(b) The Customer must provide full details and outline their Reasonable Cause, which should include:

(i) The Customer, Address and full contact details (address provided must not include a PO Box Number); and

(ii) a statement as to the type of business and description of service to customers (business type must fall in line with one of the stated categories e.g. vehicle checking companies).

3.4 **Third Parties:**

(a) If the Customer allows a Third Party (including Third Party Customers and Intermediaries) access to the Data, the Customer shall enter into a written contract which requires that Third Party to abide by and the requirements in **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)** and **SCHEDULE 4 (REQUIREMENTS IN RELATION TO INTERMEDIARIES, THIRD PARTY CUSTOMERS AND REQUESTORS)**.

(b) If the Third Party allows a Requestor access to the Data, that Third Party shall at all times comply with the requirements set out in **SCHEDULE 2** and **SCHEDULE 4** of this Section 3 to ensure compliance by each Requestor with the terms of its particular contract with the Customer.

(c) Where the Customer provides Data to a Third Party, the Customer must provide Supplier with a complete and accurate list of those Third Parties upon request by Supplier.

(d) Where the Customer provides Data to a Third Party, the Customer will audit those Third Parties and notify Supplier of any changes or issues. Evidence of the audit must be made available to Supplier upon request. Customer acknowledges and accepts that Supplier may be required to make available such audit detail to DVLA

3.5 **Distribution and Accuracy of Data:**

It will be the responsibility of the Customer to ensure that the method of record provision by Supplier is suitable and satisfactory to meet the Customer's Reasonable Cause.

4. Management of this Agreement:

4.1 The Customer's Key Staff:

(a) The Customer shall complete the list at **ANNEX A (CUSTOMER'S KEY STAFF)** of the individuals who have direct responsibilities for the use of the Data and for the Customer's other obligations under this Agreement, giving their names and business addresses and other contact details and specifying the capacities in which they are concerned with the Data.

(b) As a minimum, the list shall include details of the Customer's registered office, as recorded by Companies' House and:

(i) the manager who shall be responsible for the Customer's general contractual matters and shall receive Notices under the Agreement sent to the Customer's registered office, and who shall be referred to in this Agreement as the **Commercial Manager**; and

(ii) the manager who is responsible for the management of the Data once in the hands of the Customer, to be referred to in this Agreement as the **Data Manager**.

(c) The Customer shall inform Supplier immediately of any changes in personnel listed in **ANNEX A (CUSTOMERS KEY STAFF)** or their business contact details., and who shall be referred to in this Agreement as the **Commercial Manager**; and

(d) the manager who is responsible for the management of the Data once in the hands of the Customer, to be referred to in this Agreement as the **Data Manager**.

(e) The Customer shall inform Supplier immediately of any changes in personnel listed in **ANNEX A (CUSTOMERS KEY STAFF)** or their business contact details

4.2 Reviews and Meetings:

(a) The Customer shall upon receipt of reasonable notice and during normal office hours attend all meetings arranged by Supplier for the discussion of matters connected with the performance of this Agreement.

(b) Without prejudice to any other requirement in this Agreement, the Customer shall provide such reports in the performance of the Agreement or any other information relating to the Customer's request for and use of the Data as Supplier may reasonably require.

(c) The Supplier reserves the right to review the Agreement with the Customer at any time and the Customer Agrees to cooperate with Supplier's own review obligations to the DVLA in relation to any such review.

5. Data Protection

5.1 The Data Protection Legislation

(a) The Parties shall comply with the requirements of Data Protection Legislation and subordinate legislation made under it, or any legislation which may supersede it, together with any relevant guidance and/or codes of practice issued by the Information Commissioner. All these requirements are referred to in this Agreement as "Data Protection Legislation".

(b) For the purpose of this Clause 5, the terms "Data Controller", "Data Processor", "Data Subject", "Information Commissioner", "Information Commissioner's Office", "Personal Data", and "Processing" shall have the meanings prescribed under Data Protection Legislation.

(c) The Parties agree that the Data constitutes Personal Data as they relate to a living individual who can be directly or indirectly identified from the Data.

(d) It is the duty of the Data Controller to comply with Data Protection Legislation. The Customer, separately from the Supplier, shall be the Data Controller of each item of Data received from the Supplier from the point of receipt of that Data by the Customer and shall be responsible for complying with data protection principles in relation to its further Processing of that Data.

(e) The Customer shall (and shall ensure that each member of the Customer's Staff) comply with Data Protection Legislation and will duly observe all their obligations under Data Protection Legislation which arise in connection with this Agreement.

(f) The Customer shall ensure that the individual rights of the Data Subject are taken into account in responding to any Data Subject Access Request.

(g) The Customer shall notify Supplier immediately if it received a request from any third party for disclosure of the Data where compliance with such request is required or purported to be required by Law.

5.2 Data Security

(a) Both Parties shall ensure the safe transportation/transmission of the Data in accordance with the appropriate technical and organisational measures.

(b) The Customer shall ensure the Data is processed in accordance with Data Protection Legislation guidance and codes of practice.

(c) The Customer shall comply with all minimum security requirements set out in **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)** and any other data security requirements that the Supplier shall make from time to time.

(d) The Customer shall notify the Supplier immediately, within a maximum of **24 hours** of becoming aware, of any failure to comply with the requirements set out in **SCHEDULE 2 (MINIMUM SECURITY REQUIREMENTS)**.

(e) The Customer shall not transfer or in any way make Data available to Third Parties unconnected with the Reasonable Causes.

5.3 Malicious Software

(a) The Customer shall, as an enduring obligation throughout the term of this Agreement, use the latest versions of anti-virus software available from an industry accepted anti-virus software vendor to check for and remove Malicious Software from the ICT Environment.

(b) Notwithstanding clause 5.3, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Data, assist each other to mitigate any losses and to restore the Bulk Service to their desired operating efficiency.

5.4 Transfer of the Data outside the UK

(a) The Customer shall not transfer Personal Data outside of the EU unless the **prior written approval of the Supplier** has been obtained and the following conditions are fulfilled: a) the Customer has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer; b) the Data Subject has enforceable rights and effective legal remedies; c) the Customer 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 Process of Personal Data); and d) the Customer complies with any reasonable instructions notified to it in advance by the Supplier with respect to the Processing of Personal Data.

(b) Where the Supplier gives the prior and express written approval referred to in clause 5.4, the Customer shall disclose the Data only to the extent agreed and in accordance with any conditions attached to the giving of that approval.

5.5 Restrictions on Disclosure of the Data

The Customer shall respect the confidentiality of the Data and shall not disclose it to any person, except in the following circumstances:

(i) to a Sub Contractor who acts as the Customer's Data Processor, with prior written approval of the Supplier (and the Customer acknowledges and accepts that such approval may be subject to **DVLA pass-down consent**), and with whom the Customer shall have entered into a written contract, that requires the Data Processor to abide by the requirements in **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)** and the terms for Sub-contractors set out in **SCHEDULE 3 (REQUIRED TERMS FOR CONTRACTS WITH SUB-CONTRACTORS)**; or

(ii) to a Third Party Customer, with whom the Customer shall have entered into a written contract, that requires that Third Party Customer to abide by the requirements in **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)**, **SCHEDULE 4 (REQUIREMENTS IN RELATION TO THIRD PARTY CUSTOMERS AND REQUESTORS)** and **SCHEDULE 5**

(RESTRICTIONS ON DISCLOSURE OF VEHICLE IDENTIFICATION NUMBER), and the Data is only released on a case-by-case basis, where Reasonable Cause can be demonstrated; or

(iii) with the prior written approval of Supplier (which may be given, refused and withdrawn at the absolute discretion of the Supplier and / or (where applicable) the DVLA), providing the Data is released in accordance with **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)**, **SCHEDULE 4 (REQUIREMENTS IN RELATION TO INTERMEDIARIES, THIRD PARTY CUSTOMERS AND REQUESTORS)** and **SCHEDULE 5 (RESTRICTIONS ON DISCLOSURE OF VEHICLE IDENTIFICATION NUMBER)**, and the Data is only released on a case-by-case basis, where Reasonable Cause can be demonstrated; or

(iv) if required to do so by Law.

5.6 **Retention of Data and Evidence**

(a) In accordance with the Data Protection Legislation, the Customer shall retain each item of Data only for as long as is necessary with reference to the Reasonable Cause for which it was shared.

(b) The Customer shall arrange for the secure destruction or deletion of each item of Data, in accordance with the requirements of the Data Protection Legislation, so soon as it is no longer necessary to retain it.

(c) The Customer shall retain for **two years** after Provision of the Data, to allow inspection by Supplier and / or (where applicable) the DVLA, the evidence that the Customer relies on to show its compliance with the requirements of this Agreement. There is no need, for such inspection purposes, for the Data to be retained as part of this requirement. The Data must be disposed of in accordance with the provision of clause 5.6 above.

5.7 **The Customer's Vetting and Disciplinary Policies**

(a) The Customer shall maintain policies for vetting, hiring, training and disciplining the Customer's Staff and shall set out with these in respect of each person who has access to the Service. The minimum requirements for such vetting procedures are set out in **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)**.

5.8 **The Customer's Internal Compliance Checks**

(a) The Customer shall ensure that its business processes, records of customer interactions and transactions, audit procedures on business activities and financial reporting are appropriate and effective to ensure proper use of the Data in compliance with the requirements of the Data Protection Legislation and the minimum requirements for such internal compliance are set out in **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)**.

(b) The Customer shall carry out its own internal compliance checks at least **annually** and shall, upon the request of Supplier provide details of the outcome of such checks.

5.9 Audits and Reviews

(a) The Customer shall share with the Supplier the outcome of any other checks, audits or reviews that have been carried out on its activities as a Data Controller that are relevant to the Processing of the Data.

(b) The Customer shall notify the Supplier immediately, within a maximum of **24 hours** of becoming aware, of any audits that are being carried out by the Information Commissioner's Office under Data Protection Legislation that are relevant to the Processing of the Data.

5.10 Incidents

(a) The Customer shall notify the Supplier immediately, within a maximum of **24 hours** of becoming aware, of any losses, compromise or misuse of the Data or any **Personal Data Breach** and keep Supplier informed of any communications about the incident with: the individuals whose Personal Data is affected; the Information Commissioner's Office; or the media.

(b) The Customer understands that as the Data Controller it shall be responsible for taking any action necessary to resolve any such incident.

5.11 Inspection

(a) The Supplier or an agent acting on its (or, where applicable, the DVLA's) behalf reserves the right to carry out an Inspection at any time of the Customer's compliance with the terms of this Agreement. Where possible, the Supplier shall give the Customer **7 Days' written notice** of any such inspection.

(b) The Customer agrees to co-operate fully with any such Inspection and to allow the Supplier or an agent acting on its (or, where applicable, the DVLA's) behalf access to its Premises, Equipment, evidence and the Customer's Staff for the purposes of the Inspection.

(c) The Customer will respond as required to the findings and recommendations of any such Inspection and will provide updates as required on the implementation of any required actions.

(d) The Supplier (in its own discretion or at the direction of the DVLA) may, by written notice to the Customer, forbid access to the Data, or withdraw permission for continued access to the Data, to: i) any member of the Customer's Staff; or ii) any person employed or engaged by any member of the Customer's Staff; or whose access to or use of the Data would, in the reasonable opinion of the Supplier (and, where applicable, the DVLA), be undesirable.

(e) The decision of the Supplier (and, where applicable, the DVLA) as to whether any person is to be forbidden from accessing the Data and as to whether the Customer has failed to comply with this clause shall be final and conclusive.

(f) The Customer will be written to be reimbursed by the Customer for all Supplier's reasonable costs incurred in the course of the Inspection, such costs will include any costs required by the Supplier to be paid to the DVLA pursuant to the same obligation in the Supplier's Contract with the DVLA.

5.12 Action on Complaint

(a) Where a complaint is received about the Customer or the manner in which its services have been supplied or work has been performed or procedures used or about any other matter connected with the performance of the Customer's obligations under this Agreement or the use of Data, the Supplier may notify the Customer, and where considered appropriate by the Supplier, investigate the complaint. The Supplier may, in its sole discretion and / or otherwise at the direction of the DVLA, acting reasonably, uphold the complaint and take further action in accordance with Clause 9 of this Agreement

6. Statutory Obligations:

6.1 Prevention of Corruption

(a) The Customer shall not offer or give, or agree to give, to the Supplier or the any other public body or person employed by or on behalf of the Supplier or any other public body any gift or consideration of any kind as an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of this Agreement or any other contract with the Supplier, the DVLA or any other public body, or for showing or refraining from showing favour or disfavour to any person in relation to this Agreement or any such contract.

(b) If the Customer, its Staff or anyone acting on the Customer's behalf, engages in conduct prohibited by clause 6.1 or the Bribery Act 2010 (as amended) the Supplier may: i) terminate and recover from the Customer the amount of any loss suffered by the Supplier resulting from the termination; or ii) recover in full from the Customer any other loss sustained by the Supplier in consequence of any breach of that clause.

6.2 Prevention of Fraud

(a) The Customer shall take all reasonable steps, in accordance with Industry Best Practice, to prevent Fraud by the Customer's Staff and the Customer (including its shareholder, members, and directors) in connection with the receipt of the Data pursuant this Agreement.

(b) The Customer shall notify the DVLA immediately, within a maximum of **24 hours** of becoming aware, if it has reason to suspect that any fraud has occurred or is occurring or is likely to occur.

(c) If the Customer or its Staff commits Fraud in relation to this or any contract it has with the Crown (including the DVLA) the Supplier may: i) terminate this Agreement and recover from the Customer the amount of any loss suffered by the Supplier resulting from the termination; or ii)

recover in full from the Customer any other loss sustained by the Supplier in consequence of any breach of this clause.

6.3 **Discrimination:**

(a) The Customer must not unlawfully discriminate either directly or indirectly or by way of victimisation or harassment against a person on such grounds as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, colour, ethnic or national origin, sex or sexual orientation, and without prejudice to the generality of the foregoing to the Customer must not unlawfully discriminate within the meaning and scope of the Equality Acts 2006 and 2010 (as amended), the Human Rights Act 1998 9as amended) or other relevant or equivalent legislation, or any statutory modification or re-enactment thereof.

(b) The Customer shall take all reasonable steps to secure the observance of clause 6.3(a) by all of its Staff.

6.4 **The Contracts (Rights of Third Parties) Act 1999:**

(a) A person who is not a party to this Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of both Parties. This clause does not affect any right or remedy of any person which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999 (as amended) and does not apply to the Crown.

6.5 **Health and Safety:**

(a) The Customer shall promptly notify the Supplier of any health & safety hazards which may arise in connection with the performance of its obligations under this Agreement, including but not limited to, on Inspection by the Supplier.

(b) The Customer must comply with the requirements of the Health & Safety at Work etc. Act 1974 (as amended) and any other acts, orders, regulations and codes of practice relating to health & safety, which may apply to the Customer's Staff and other persons working on the Premises in the performance of its obligations under this Agreement.

7. Protection of Information:

7.1 **Publicity and Media:**

(a) The Customer shall notify the Supplier immediately if any circumstances arise which could result in publicity or media attention to the Customer which could adversely reflect on the Supplier, the DVLA or any data service provided by the DVLA.

(b) The Customer shall not use any Supplier or DVLA logo or create or approve any publicity implying or stating that the Supplier or the DVLA has a connection with any service provided by the Customer without the prior written approval of the Supplier and/or the DVLA(as applicable). Prior written approval shall be obtained for each individual piece of publicity.

8. Control of this Agreement:

8.1 Transfer and Sub-Contracting:

(a) The Customer shall not assign, sub-contract or in any other way dispose of the Agreement or any part of it without the prior written permission of the Supplier.

(b) Sub-Contracting any part of the Agreement shall not relieve the Customer of any of its obligations or duties under the Agreement. The Customer shall be responsible for the acts and omissions of its Sub-Contractors as though they are its own. Where the Supplier has given approval to the placing of sub-contracts, copies of each sub-contract shall, at the request of the Supplier, be sent by the Customer to the Supplier as soon as reasonably practicable.

8.2 Insolvency:

(a) The Customer shall notify the Supplier immediately in writing where the Customer is a company and in respect of the Customer:

(i) A proposal is made for a voluntary arrangement within Part 1 of the Insolvency Act 1986 (as amended) or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or

(ii) A shareholder's meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for it winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or

(iii) A petition is presented for its winding up (which is not dismissed within 14 Days of service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting s is convened pursuant to section 98 of the Insolvency Act 1986 (as amended); or

(iv) A receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or

(v) An application order is made either for the appointment of an administrator or for an administration order, and an administration is appointed, or notice of intention to appoint an administrator is given or

(vi) It is or become insolvent within the meaning of section 123 of the Insolvency Act 1986 (as amended); or

(vii) Being a “small company” within the meaning of section 247(3) of the Companies Act 1985 (as amended), a moratorium comes into force pursuant to Schedule 1A of the Insolvency Act 1986 (as amended); or

(viii) Any event similar to those listed in this clause occurs under the law of any other jurisdiction.

(b) The Customer shall notify the Supplier immediately in writing where the Customer is an individual and:

(i) An application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 (as amended) or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, the Customer’s creditors; or

(ii) A petition is presented and not dismissed within 14 Days or order made for the Customer’s bankruptcy; or

(iii) A receiver, or similar officer is appointed over the whole or any part of the Customer's assets or a person become entitled to appoint a receiver, or similar officer over the whole or any part of his assets; or

(iv) The Customer is unable to pay his debts or has no reasonable prospect of doing so, in either case within the meaning of section 268 of the Insolvency Act 1986 (as amended); or

(v) A creditor or encumbrancer attaches of takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the Customer’s assets and such attachment or process is not discharged within 14 Days; or

(vi) He suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business.

8.3 **Change of Control:**

(a) The Customer shall seek the prior written agreement of the Supplier to any change of control within the meaning of section 450 of the Corporation Taxes Act 2010 ("Change of Control") (as amended). Where the Supplier has not given its written agreement before the Change of Control, the Supplier may terminate this Agreement by notice in writing with immediate effect within 26 weeks of:

(i) Being notified that that change or control has occurred; or

(ii) Where no notification has been made, the date the Supplier becomes aware of that change of Control.

9. Defaults, Disruption, Suspension and Termination:

In addition to the termination rights set out in this clause 9 and without prejudice to any other rights or liabilities set out in the Agreement, the Supplier reserves the right to suspend the Services or otherwise terminate the Agreement to the extent that the supply of the DVLA-derived

Data supplied by the DVLA to the Supplier under the Contract is suspended or otherwise terminated.

9.1 **Termination for Material Breach**

(a) A Party may terminate this Agreement with immediate effect by written notice to the other Party on or at any time after the occurrence of an event specified in clause 9.1(b).

(b) The events are that:

(i) the Customer fails to pay any amount due under this Agreement on the due date for payment and remains in default not less than 60 days after being notified in writing to make such payment;

(ii) the Customer commits any three or more Defaults, whether simultaneously or singly at any time during the operation of this Agreement, irrespective of whether any or all of such breaches is minimal or trivial in nature;

(iii) the Customer commits a Material Breach of any other term of this agreement which breach is irremediable or (if such breach is remediable) fails to remedy that breach within a period of 26 weeks after being notified to do so.

(c) For the purposes of clause 9.1(b), a Material Breach is remediable if time is not of the essence in performance of the obligation and if in the reasonable opinion of the Supplier the Material Breach is capable of remedy within the 26 week period.

9.2 **Suspension of the Services (including but not limited to the provision of DVLA-derived Data):**

(a) If it comes to the attention of the Supplier that the Customer has committed any Default (including Material Breaches and all other Defaults), the Supplier may suspend all or part of the Services without further notice and with immediate effect and investigate the nature and effect of the breach.

(b) The Supplier may from time-to-time issue guidance on its principles on suspending the Services and terminating contracts to supply DVLA-derived Data. The guidance may include guidance concerning: types of Defaults which the Supplier and / or DVLA (as applicable) may consider to be Material Breaches; guidance as to specific types of breach that the Supplier and / or DVLA (as applicable) will consider to be remediable; how such breaches may be remedied; how long suspension may last; and guidance as to which types of breach the Supplier and / or DVLA (as applicable) will consider to be irremediable.

9.3 **Effect of Suspension:**

(a) If the Supplier suspends the Services at any time, the Customer shall co-operate with any further investigation, audit or review that the Supplier requires to be carried out in relation to the Data provided to the Customer.

(b) The Supplier may refuse to resume the Service until the Customer provides assurances that the matter resulting in the suspension has been resolved to the satisfaction of the Supplier and / or DVLA (as applicable), and takes specified actions within a reasonable period set by the Supplier.

(c) The DVLA may require that an Inspection is carried out after the Services are resumed, to check the Customer's compliance with this Agreement and Data Protection Legislation.

(d) The Supplier may (at Supplier's sole discretion) require the Customer to pay the reconnection fee and the fee for any inspection, before it will resume the Services.

(e) The Customer shall reimburse the Supplier for all Supplier's cost and expenses incurred in relation to the Supplier's right under clause 3.1 to carry out an inspection, investigation, audit or review of the Customer.

9.4 **Insolvency:**

(a) Where the Supplier is notified in writing of any of the circumstances listed in clause 8.2 (Insolvency), the Supplier may suspend the Services without further notice and with immediate effect and investigate further whether any of the Customer's directors or any liquidator, receiver, administrative receiver, administrator, or other officer is capable of ensuring that the provisions of this Agreement and of Data Protection Legislation are complied with. If the Supplier is not satisfied that any such person shall ensure such compliance, the Supplier may terminate the Agreement by written notice with immediate effect.

9.5 **Other Termination Rights:**

(a) The Supplier may terminate the Agreement by written notice with immediate effect if in the reasonable view of the Supplier, during any period of suspension of the Services the Customer: i) fails to co-operate with any investigation, audit or review; ii) fails to provide any assurances or take any actions within the reasonable period set by the Supplier under clause 9.3.; or ii) fails to provide assurances that satisfy the Supplier (acting reasonably) that the Customer has complied and shall continue to comply with the requirements of the Agreement and of Data Protection Legislation.

(b) The Supplier may terminate the Agreement by written notice with immediate effect if the Customer fails to pay the Supplier undisputed sums of money.

(c) The Supplier may terminate the Agreement by written notice with immediate effect if the Customer is found to be in breach of any aspect of the Law that could, in the reasonable opinion of the Supplier and / or the DVLA (as applicable), bring the Supplier and / or the DVLA (as applicable) into disrepute.

(d) The Supplier may terminate the Agreement by written notice with immediate effect if the Customer is an individual and he has died or is adjudged incapable of managing his affairs within the Mental Capacity Act 2005 (as amended).

9.6 **Consequences of Suspension and Termination:**

(a) After the Services have been suspended or the Agreement has been terminated or both, the Customer shall continue to comply with its obligations under this Agreement and under Data Protection Legislation in relation to the Data which it holds, including as to the proper use of the Data, retention of the Data and secure destruction of the Data.

SCHEDULE 2

MINIMUM DATA SECURITY REQUIREMENTS

1. Data Security Requirements:

1.1 The minimum security requirements, which are required by clause D2 are as follows:

(a) Data, including back-up data, must be retained in secure premises and locked away;

(b) the Data supplied may only be copied for back-up and for the purposes of Processing the Data. Copies must be erased immediately thereafter and they must not be otherwise duplicated;

(c) the Customer will retain the Data only for as long as necessary with reference to the Reasonable Cause for which it was shared in accordance with the Data Protection Legislation;

(d) the Customer, in accordance to Data Protection Legislation, should dispose of the Data where there is no business need to retain it;

(e) Data, including back-up Data, must be protected from unauthorised access, release or loss;

(f) A User ID and a robust password must be required to enter all databases on which the Data is stored;

(g) the password for the encrypted CD-ROM must be stored separately from the CD-ROM itself;

(h) A unique User ID and password must be attributable to an individual and must be allocated to each person with access to the Data;

(i) User IDs and passwords must not be shared between the Customer's Staff;

(j) Access to the Data must be minimised so that only where necessary are individuals given the following levels of access:

(i) ability to view material from single identifiable records;

(ii) ability to view material from many identifiable records;

(iii) functional access, including: searching, amendment, deletion, printing, downloading or transferring information;

(k) the Data must not then be copied onto or stored on Removable Media. Laptops may be used but only if the device has full disk encryption installed in line with Industry Best Practice and the devices are securely protected when not in use;

(l) Data must be used only for the Reasonable Cause for which it was obtained;

(m) Paper records must be destroyed by incineration, pulping or shredding finely so that reconstruction is unlikely;

(n) Electronic Data must be securely destroyed or deleted in accordance with current guidance from the Information Commissioner's Office as soon as it is no longer needed; Please refer to clause 6.6(b).;

(o) All premises and buildings in which the Data is stored must be secure;

(p) the Customer must be registered with the Information Commissioner and the permission must cover all activities actually carried out;

(q) Information must not be passed to third parties except with the prior written approval of the Supplier, in accordance with 5.5 (and the Customer acknowledges and accepts that such consent may be subject to DVLA pass-down consent); and

(r) transfer of the Data to third parties (where approval has been granted by the Supplier in accordance with clause 5.5 must be in accordance with the principles of Data Protection Legislation. Any other conditions required by the Supplier (and / or the DVLA, as applicable) in giving permission for disclosure to third parties must be satisfied.

2 Inspection, Internal Compliance and Audit:

2.1 The Data Governance Assessment form shall be completed upon Supplier request and shall confirm whether or not the following requirements have been complied with:

(a) all of the Data Security requirements in paragraph 1 of SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS);

(b) the requirements set out in SCHEDULE 4 and SCHEDULE 5.

2.2 The Customer must ensure that Caching of Data by Intermediaries or Third Party Customers is only possible where that Intermediary or Third Party Customer is compliant with all the requirements of the parent contract, and only in the following circumstances:

(a) for a limited period of 24 hours to allow multiple hits against a single record as part of continuous enquiry (e.g. multiple insurance quotes from a website or call centre);

(b) the Cache is protected from unauthorised access by way of encryption in accordance with Industry Best Practice;

(c) the Customer must ensure that Intermediaries and Third Party Customers are made aware that they must not use the Data to fulfil further enquiries or transactions on that Intermediary or Third Party Customer's systems, or in favour or on behalf of actual or potential customers of the Intermediary or Third Party Customer, nor to fulfil multiple enquiries such as insurance or financial quotes after the 24 hour period permitted above has expired;

(d) the Customer must make Intermediaries and Third Party Customers aware of the above and that storage of the Data for future use/download/transfer after this period is not permitted. The Customer's attention is drawn to the requirements of SCHEDULE 5 (RESTRICTIONS ON DISCLOSURE OF VEHICLE IDENTIFICATION NUMBER (VIN)).

3 Minimum Requirements for the Customer's Staff Vetting and Disciplinary Procedures:

3.1 The minimum requirements for the Customer's Staff vetting procedures, which are required by clause 5.7 of this Agreement, are as follows:

(a) the Customer shall confirm the identity of its entire new Staff;

(b) the Customer shall confirm the references of its entire Staff;

(c) the Customer shall require all persons who are to have access to the Data to complete and sign a written declaration of any unspent criminal Convictions;

(d) the Customer shall not allow any person with unspent criminal convictions to have access to the Data, except with the prior written permission of the Supplier;

(e) the Customer shall ensure that no person who discloses that he or she has a Relevant Conviction, or who is found by the Customer to have any Relevant Conviction is allowed access to the Data;

(f) the Customer shall require all persons who are to have access to the Data to complete and sign an agreement to use the Data only for the Reasonable Causes set out in this Agreement and in accordance with the Customer's procedures;

(g) the Customer shall require that each person who has access to the Data shall sign a document confirming that the person shall use the Data only in accordance with the Customer's procedures and only for the Reasonable Cause;

(h) the Customer shall ensure that each person who has access to the Data shall act with all due skill, care and diligence and shall possess such qualifications, skills and experience as are necessary for the proper use of the Data;

(i) the Customer shall ensure that each person who has access to the Data is appropriately trained in and aware of his or her duties and responsibilities under the Data Protection Legislation and this Agreement;

(j) the Customer shall create and maintain a unique user account ID for each person who has access to the Data;

(k) The Customer shall maintain a procedure for authorizing the creation of user accounts and for the prompt deletion of accounts that are no longer required. The Customer must ensure that the person or persons carrying out this work are appropriately trained and that their duties are separate from that of a normal user account. A normal user must not be able to manage their own account;

(l) The Customer's disciplinary policy shall state that misuse of the Data by any person shall constitute gross misconduct and may result in summary dismissal of that person. The Customer shall notify such misuse to the Supplier (and the Customer acknowledges that the Supplier must in turn notify such misuse to the DVLA) and the person involved shall be refused all future access to DVLA-derived Data;

(m) System administrators must receive appropriate training;

(n) The system administration role must be separated from any other role to ensure a separation of duties.

SCHEDULE 3
REQUIRED TERMS FOR CONTRACTS WITH SUB-CONTRACTORS

1. Data Protection:

1.1 In accordance with clause 5.5, the following terms must be included in the written contract between the Customer and any Sub-Contractor with access to the Data (each a **"Sub-Contract"**):

1.2 For the purposes of each Sub-Contract, the terms **"Conviction Data"**, **"Data Controller"**, **"Data Processor"**, **"Data Subject"**, **"Information Commissioner"**, **"Information Commissioners Office"**, **"Personal Data"**, **"Process"** and **"Processing"** shall have the meanings prescribed under Data Protection Legislation.

1.3 The Sub-Contractor shall (and shall ensure that every member of its Staff complies with any notification requirements under Data Protection Legislation and both Parties will duly observe all their obligations under Data Protection Legislation which arise in connection with the Sub-Contract.

1.4 The Sub-Contractor acknowledges that the Data constitutes Personal Data to which Data Protection Legislation applies and that the Customer is the Data Controller of the Data.

1.5 The Sub-Contractor shall process the Data only in accordance with instructions from the Customer (which may be specific instructions or instructions of a general nature) as set out in the Data Protection Declaration or otherwise notified by the Customer.

1.6 The Sub-Contractor shall comply with all applicable Laws, including Data Protection Legislation.

1.7 The Sub-Contractor shall process the Data only to the extent and in such manner as is necessary to achieve the Reasonable Causes or as is required by Law or any Regulatory Body.

1.8 The Sub-Contractor shall implement appropriate technical and organisational measures to protect the Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Data and having regard to the personal nature of the Data which is to be protected. These measures shall as a minimum satisfy the requirements in **SCHEDULE 2 (MINIMUM DATA SECURITY REQUIREMENTS)** to this Agreement.

1.9 The Sub-Contractor shall take reasonable steps to ensure the reliability of its Staff and agents who may have access to the Data.

1.10 The Sub-Contractor shall not transfer the Data to any sub-contractor except with the prior written approval of the Customer who shall have sought and received the prior written approval of the Supplier (who shall first have received DVLA pass-down consent) to that transfer, which shall include the requirement that the Sub-Contractor has entered into a written contract with the sub-contractor which includes all of the provisions in SCHEDULE 2, 3, 4 and 5.

1.11 The Sub-Contractor shall not transfer or permit any Personal Data to be transferred outside the EU unless the prior written approval of the Customer has been obtained, (who shall first have

notified the Supplier, who in turn shall first have notified the DVLA) and the following conditions are fulfilled: * (i) The Customer or the Sub-Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer. * (ii) The Data Subject has enforceable rights and effective legal remedies. * (iii) The Sub-Contractor 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 Process of Personal Data). * (iv) The Sub-Contractor complies with any reasonable instructions notified to it in advance by the Customer with respect to the Processing of the Data.

1.12 The Sub-Contractor shall ensure that all Staff and agents required to access the Data are informed of the confidential nature of the Data and comply with the obligations set out in this Agreement, and have undergone adequate training in the use, care, protection and handling of the Data.

1.13 The Sub-Contractor shall ensure that none of the Staff and agents publish, disclose or divulge any of the Data to any third parties unless directed in writing to do so by the Customer.

1.14 The Sub-Contractor shall not disclose any of the Data to any third parties in any circumstances other directed in writing to do so by the Customer.

1.15 The Sub-Contractor shall notify the Customer within five Working Days if it receives a request from a Data Subject to have access to that person's Personal Data, or a complaint or request relating to the Customer's obligations under Data Protection Legislation, or any communication from the Information Commissioner or any other regulatory authority in connection with the Personal Data processed under this Agreement.

1.16 The provisions of this Agreement shall apply during the period that the Sub-Contractor processes the Data on behalf of the Customer and indefinitely after the end of that period.

1.17 The Sub-Contractor shall ensure that no person who discloses that he or she has a Relevant Conviction, or who is found by the Sub-Contractor to have any Relevant Conviction is allowed access to the Data without the prior written approval of the Supplier (and the Customer acknowledges and accepts that such approval may be subject to DVLA pass-down consent).

1.18 The Sub-Contractor shall notify the Customer immediately if it: * a) receives a request to rectify, block or erase any Data; * b) becomes aware of the loss of any Data.

1.19 The Sub-Contractor shall notify the Customer of any losses, compromise or misuse of the Data immediately and keep the Customer informed of any relevant communications.

1.20 The Sub-Contractor acknowledges that the Supplier reserves the right to withdraw permission relating to Sub-Contracting at any time. Where the Supplier has withdrawn permission, the Sub-Contractor will be required to cease all Data processing activities relating to the Data.

1.21 Withdrawal of such permission as set out in paragraph 1.20 will also apply to any other sub-contracting arrangement that involves the processing of the Data by the Sub-Contractor.

2 Compliance and Inspection:

2.1 The Sub-Contractor shall carry out its own internal compliance checks at least annually, which include at least the matters listed in **SCHEDULE 2, 3, 4, and 5**. The Sub-Contractor shall notify the Customer in writing within 28 Days of the outcome of such checks, which will be issued by the Customer to the Supplier when required and the Customer acknowledges and accepts that such outcome may also be issued by the Supplier to the DVLA.

2.2 The Customer reserves the right to carry out an Inspection at any time of the Sub-Contractor's compliance with the terms of the Sub-Contract. The Customer shall give the Sub-Contractor **28 Days' written notice** of any such inspection.

2.3 The Sub-Contractor agrees to co-operate fully with any such inspection and to allow the Customer access to its Premises, Equipment and Staff for the purposes of the inspection.

2.4 The Sub-Contractor shall share with the Customer the outcome of any other checks, audits or reviews that have been carried out on its activities as a Sub-Contractor, to the extent that they have relevance to the Processing of the Data.

2.5 The Sub-Contractor shall notify the Customer immediately of any audits that are being carried out by the Information Commissioner's Office under Data Protection Legislation, to the extent that they have relevance to the Processing of the Data.

3 Termination:

3.1 If at any time the Customer becomes aware that the Sub-Contractor has breached the requirements of clause 1 or 2 of **SCHEDULE 3 (REQUIRED TERMS FOR CONTRACTS WITH SUB-CONTRACTORS)**, the Customer may terminate this Agreement immediately.

SCHEDULE 4

REQUIREMENTS IN RELATION TO THIRD PARTY CUSTOMERS AND REQUESTORS

1. Contractual Obligations of all Third Party Customers

1.1 The obligations imposed on the Customer and to be imposed by the Customer on its own Third Party Customers, are as follows:

(a) the obligations of the Customer in clause 3.1 (Purpose For Which Data is Provided);

(b) the obligations of the Customer in clause 4.1 (The Customer's Key Staff), except that the obligation on the Customer in clause 4.1(c) (changes in personnel) to notify the Supplier shall instead be an obligation on the Third Party Customer to notify the Customer;

(c) the obligations of the Customer in Clause 6 (STATUTORY OBLIGATIONS) and 7 (Publicity and Media);

(d) the obligations of the Customer in the following clauses, except that any obligation to seek the permission of or to notify the Supplier shall instead be an obligation to seek the permission of or to notify the Customer:

1.1.d.1 8.1, 5.1(c) and 8.1(b);

1.1.d.2 8.2;

1.1.d.3 8.3;

1.1.d.4. 9.6

2. Contractual Obligations of Intermediaries and Third Party Customers with Access to the Data

2.1 In accordance with clause 3.4, the obligations to be imposed on the Intermediary or Third Party Customer in the written contract between the Customer and each Intermediary and Third Party Customer are as follows:

(a) the obligations of the Customer in clause 3.5 (Accuracy of the Data);

(b) the obligations of the Customer in clause 4.2 (Reviews and meetings), except that the requirements in that clause to attend meetings and otherwise may be placed on the Intermediary or Third Party Customer by the Customer and not by the Supplier (and / or the DVLA, as applicable);

(c) the obligations of the Customer in clause 5 (DATA PROTECTION), except that the obligations on the Customer in the following clauses to notify, inform, share information with or co-operate with the Supplier (and/or the DVLA, as applicable) shall instead be obligations to notify, inform or share information with and co-operate with the Customer:

2.1.c.1 5.8(b) (outcome of internal compliance checks);

2.1.c.2 5.9 (Audits and Reviews);

2.1.c.3 5.10(a) (Incidents);

2.1.c.4 5.11(Inspection).

(d) the requirements in **SCHEDULE 2**, **4**, and **5**.

3. Contractual Rights and Powers

3.1 The rights and powers to be reserved by the Customer in accordance with clause 3.4, in the written contract between the Customer and each Intermediary or Third Party Customer, are as follows:

(a) the rights and powers of the Supplier (and / or the DVLA, as applicable) in clauses 5.11 and 5.12;

(b) the right of the Supplier to terminate the Agreement, in accordance with clause 9.1 or 9.5; and

(c) the right of the Supplier (and / or the DVLA, as applicable) to suspend access to the Data to the Third Party Customer under clauses 9.2 and 9.4, and the effect of suspension under clause 9.3, except that the obligation to pay fees under clause 9.3(d) shall be an obligation to pay those fees to the Customer, or may be varied or waived by the Customer.

4. DVLA-derived Compliance and Intermediaries and Third Party Customers

4.1 In accordance with clause 3.4 and in order to ensure the compliance of its Intermediaries or Third-Party Customers with the obligations in **SCHEDULE 4 (REQUIREMENTS IN RELATION TO INTERMEDIARIES AND THIRD PARTY CUSTOMERS)**, the Customer shall:

(a) at all times maintain a written contract with the Intermediary or Third-Party Customer that includes all the obligations and rights required to be included under this Agreement;

(b) audit each Intermediary or Third Party Customer at least once in the first calendar year during which the Customer discloses Data to such Intermediary or Third Party Customer, and annually thereafter, and make evidence of such audits available to the Supplier at its request (and the Customer acknowledges and accepts that such evidence may also be made available by the Supplier to the DVLA);

(c) notify the Supplier immediately of any Defaults that the Customer considers to have been committed by the Intermediary or Third-Party Customer, whether discovered on or audit by the Customer or at any other time; and

(d) take any additional action the Customer considers reasonable to ensure that the Intermediary or Third-Party Customer shall comply with all of the Bulk user obligations.

5. Conditions on the Use of VRN as Search Criteria

5.1 Disclosure of the Data (or any extract from it) relating a specific vehicle upon entry of a VRN by a Requestor, an Intermediary or a Third-Party Customer are only permitted in the following cases:

(a) The VRN relates to a vehicle where the Requestor is either owner or registered keeper of that vehicle; or

(b) The VRN relates to a vehicle that is being or intended to be marketed or offered for sale; or

(c) The Requestor has a genuine and legitimate interest in determining the provenance, status or technical specification of that vehicle; or

(d) Where confirmation of the vehicle identity is a pre-requisite for the Data being accessed by the Requestor.

(e) The VRN relates to a vehicle that the Requestor, Intermediary or Third-Party Customer has involvement in providing services to. This may include where the Requestor, Intermediary or Third-Party Customer:

- Has sold, repaired, modified, or serviced that vehicle;
- Is providing an insurance quotation or vehicle finance for that vehicle;
- Is involved in reducing crime for that vehicle.

6. Restrictions on Free Disclosure of the Data

6.1 To restrict excessive amounts of Data from being disclosed to Third Party Customers, Intermediaries or Requestors, the Customer is only permitted to disclose the following Data fields free of charge and free of any conditions:

Make	Year of Manufacture
Model	Export Marker
Colour	Vehicle Type Approval
Date of First Registration	Wheelplan
Body Type	Vehicle/Revenue Weight
Fuel Type	Tax Data
Engine Capacity	MOT Data
CO2	Gearbox (obtained from SMMT)
BHP (obtained from SMMT)	

SCHEDULE 5

RESTRICTIONS ON DISCLOSURE OF VEHICLE IDENTIFICATION NUMBER (VIN)

1. Introduction

1.1 It is necessary to have key identifying criteria and references (such as a serial number) for most assets. The main identifiers for a motor vehicle are the VRN (Vehicle Registration Number) and the VIN (Vehicle Identification Number). As the VIN is only applicable once the vehicle is registered and can be transferred to another vehicle, the most reliable identifier has become the VIN.

1.2 Within the automotive sector, correctly identifying a vehicle is vital in order to ensure the correct details are recorded and disclosed during the life of that vehicle. This applies in particular when specific events occur such as registration, secured finance, resale, repair, cherished plate transfer process, future finance applications and insurance application/renewal.

1.3 To address this market need, the Customer (can release the full VIN in certain circumstances, to agreed trade sectors, in accordance with Reasonable Cause as set out in 3.1 and 5.5 of this Agreement, and subject to specified conditions.

1.4 The table in section 2 below sets out the specified conditions for disclosure of the full VIN. The full VIN must only be released where absolutely essential and where this is not necessary VIN confirmation or partial VIN release should be the preferred solution.

1.5 Section 4 below sets out conditions on disclosure of the partial VIN.

2. Market Sectors Where Disclosure of Full VIN is Permitted

Market Sector	Purpose for Release of VIN	Permitted Disclosure
Motor Dealers Franchised	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To confirm a correct VIN to be compared to the VIN displayed on the vehicle.	Displayed on the vehicle search report / certificate. Recorded on the vehicle inventory, stock report, ledgers and customer database / service record. Information disclosed to vehicle purchaser / owner, dealership staff, sub-contractors and auditors.
Motor Dealers Non-Franchised	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To confirm a correct VIN to be compared to the VIN displayed on the vehicle.	Displayed on the vehicle search report / certificate. Recorded on the vehicle inventory, stock report, ledgers and customer database / service record. Information disclosed to vehicle purchaser / owner, dealership staff, sub-contractors and auditors.
Auction Houses	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To confirm a correct VIN to be compared to the VIN displayed on the vehicle.	Displayed on the vehicle search report / sale lot. Recorded on the vehicle asset / inventory files, stock report and ledgers. Information disclosed to vehicle vendor / purchaser, auction staff, sub-contractors and auditors.

Original Equipment Manufacturers	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To use the VIN as an identifier of vehicle is not yet registered.	Displayed on the vehicle search report / certificate. Recorded on the vehicle inventory, stock report, ledgers and customer database / service record. Information disclosed to franchise holders, vehicle owner / purchaser, OEM staff, sub-contractors and auditors.
Finance Companies	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To use the VIN as an identifier if vehicle is not yet registered.	Displayed on the vehicle asset / inventory files. Contract reports, ledgers and customer database / record. Information disclosed to vehicle operator / owner / purchaser, finance company staff, sub-contractors and auditors.
Insurance Companies	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle.	Displayed on the vehicle history / claims files, contract reports, ledgers and customer database / record. Information disclosed to vehicle operator / owner / policyholder, insurance company staff, sub-contractors and auditors.
Fleet and Leasing Companies	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To use the VIN as an identifier if vehicle is not yet registered.	Recorded on the vehicle asset / inventory files. Contract reports, ledgers and customer database / service record. Information disclosed to vehicle operator / owner / purchaser, fleet & leasing company staff, sub-contractors and auditors.
Aftermarket Service Providers	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. Used to help identify and link to replacement parts and accessories.	Displayed on the vehicle order record, ledgers and customer database / service record. Information disclosed to vehicle repairer / operator / owner / purchaser, aftermarket company staff, sub-contractors and auditors.
Automotive Systems and Application Companies (e.g. Vendors of Dealer Management Systems)	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle.	Displayed on the vehicle search report / certificate. Recorded on the application schedule to handle vehicle inventory, stock report, ledgers and customer database / service record. Information disclosed to vehicle owner / system user, system owner, vehicle owner / purchaser, systems integrator company staff, sub-contractors and auditors.
Law Enforcement Agencies	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To confirm a correct VIN to be compared to the VIN displayed on the vehicle. To use the VIN as an identifier if vehicle is not yet registered.	Displayed on the vehicle search report / certificate. Recorded on the police information systems, stock report, ledgers. Information disclosed to authorised individuals and bodies involved in and processing the case / enquiry.
Salvage Companies	To assist in confirming the identity of the vehicle by validating that the VIN searched relates to the correct vehicle. To confirm a correct VIN to be compared to the VIN displayed on the vehicle.	Displayed on the vehicle record / COD (Certificate Of Destruction). Recorded on the vehicle inventory, stock report, ledgers and customer database. Information disclosed to vehicle operator / owner, salvage company staff, sub-contractors and auditors.

3. Market Sectors Where Disclosure of Full VIN is Not Permitted

3.1 Disclosure of the full VIN is not permitted to the following market sectors:

(a) Consumers.

(b) Marketing Companies (other than those working on behalf of approved trade sector clients in respect of their core activities under permitted uses).

(c) Companies, Partnerships and Sole Traders who do not meet the criteria set out in the table in section 2 above.

3.2 Where there is a requirement to disclose the full VIN to new market sectors or for new purposes other than those set out in the table above in section 2 of this **SCHEDULE 5**, the Customer must detail this in writing and obtain **formal written approval from the Supplier** (and the Customer acknowledges and accepts that such approval may be subject to DVLA pass-down consent). The Customer shall not disclose the full VIN to any additional market sectors or for any new purposes without a contract variation in accordance with clause H5, and formal written approval from the Supplier (and the Customer acknowledges and accepts that such approval may be subject to DVLA pass-down consent).

4. Conditions on Disclosure of Partial VIN

4.1 The Society of Motor Manufacturers and Traders (SMMT) has informed DVLA that the release of the end characters of a VIN (so a partial VIN) may lead to the ability to uniquely identify a vehicle in a very limited range of circumstances.

4.2 Where there are fewer than 500 vehicles of a particular type registered in a year, only the last three characters are needed to uniquely identify a vehicle, assuming that the make and model of that vehicle is known.

4.3 Where Reasonable Cause can be demonstrated to allow a Requestor, Intermediary or Third Party Customer to identify a unique vehicle (in accordance with clause 3.1of this Agreement), and where there are fewer than 500 vehicles of a particular vehicle type registered in one year, the Customer must only disclose **the last two characters** of the VIN.

ANNEX A
CUSTOMER'S KEY STAFF WITH DIRECT RESPONSIBILITIES FOR THE DATA AND FOR THE OTHER OBLIGATIONS UNDER THE AGREEMENT

1. The contact details of the Customer's Key Staff with responsibility for the Data and the performance of the Agreement as referred to in clause 4.1 of this Agreement, are set out in Annex A.

1.1 The contact details of the Commercial Manager referred to in clause 4.1(b)(i)

Name: _____

Job Title: _____

Registered Business Address: _____

_____

_____

_____

_____

Business telephone number: _____

Business mobile number: _____

Business email address: _____

1.2 The contact details of the Data manager referred to in clause 4.1(b)(ii):

Name: _____

Job Title: _____

Registered Business Address: _____

_____

_____

_____

_____

Business telephone number: _____

Business mobile number: _____

Business email address: _____

1.3 The contact details of any other Key Staff, who are responsible for the Data or for supervision of the Staff with access to the Data, should be provided below and continuation sheets attached to Annex A (Customer key Staff).

1.4 The contact details for the Data Protection Officer ("DPO") where applicable:

Name: _____

Job Title: _____

Registered Business Address: _____

_____

_____

_____

_____

Business telephone number: _____

Business mobile number: _____

Business email address: _____