DATED 27 NOVEMBER 2023

DRIVER UK MASTER S.A.,
acting for and on behalf of its Compartment 7
(as Issuer)

- and -

VOLKSWAGEN FINANCIAL SERVICES (UK) LIMITED
(as Seller and Servicer)

- and -

INTERTRUST TRUSTEES GMBH
(as Security Trustee)

- and -

DATA CUSTODY AGENT SERVICES B.V.
(as Data Protection Trustee)

DATA PROTECTION TRUST AGREEMENT

Hogan Lovells

Matter ref: 153290/000064
Ref: F2/4125-3586-3369

Hogan Lovells International LLP
Atlantic House, Holborn Viaduct, London EC1A 2FG

CONTENTS

THIS DATA PROTECTION TRUST AGREEMENT ("**this Agreement**") is made on 27 November 2023

BETWEEN:

(1) **Driver UK Master S.A.**, a public company (*société anonyme*) incorporated with limited liability under the laws of Luxembourg and registered with the Luxembourg register of commerce and companies under registration number B 162723 and having its registered office at 22-24 Boulevard Royal, L-2449 Luxembourg, acting for and on behalf of its Compartment 7 (the "**Issuer**");

(2) **Volkswagen Financial Services (UK) Limited**, a limited company incorporated under the laws of England and Wales, with registered number 02835230 and having its registered office at Brunswick Court, Yeomans Drive, Blakelands, Milton Keynes MK14 5LR, United Kingdom, as seller and servicer (the "**Seller**" and the "**Servicer**", or in any capacity, "**VWFS**");

(3) **Intertrust Trustees GmbH**, a private limited liability company (*Gesellschaft mit beschränkter Haftung*) incorporated under the laws of Germany and having its registered office at Eschersheimer Landstraße 14, 60322 Frankfurt am Main, Germany, registered with the commercial register (*Handelsregister*) of the local court (*Amtsgericht*) of Frankfurt am Main, Germany under HRB 98921 (the "**Security Trustee**" which expression shall, where the context so admits, include all other persons for the time being acting as security trustee pursuant to the Trust Agreement and the Deed of Charge and Assignment); and

(4) **Data Custody Agent Services B.V.**, a private company with limited liability (*besloten* vennootschap met *beperkte aansprakelijkheid*) incorporated under the laws of the Netherlands, having its official seat (*statutaire zetel*) in Amsterdam, The Netherlands, and its registered office at Basisweg 10, 1043 AP Amsterdam, The Netherlands, registered in the Trade Register under number 812770286 (the "**Data Protection Trustee**").

WHEREAS

(A) Driver UK Master S.A. was established as a public company (*société anonyme*) incorporated with limited liability under the Luxembourg Securitisation Law on 29 July 2011 for the purposes of asset-backed securitisation. The sole shareholder of the Issuer is Stichting CarLux, a foundation duly incorporated in Amsterdam, the Netherlands.

(B) VWFS has entered into various agreements for the provision of credit in relation to the purchase, by way of hire purchase agreements or personal contract purchase agreements, of motor vehicles by its customers in the ordinary course of its business pursuant to which such customers shall be obliged to make periodic payments in respect of Receivables.

(C) VWFS has agreed to sell and the Issuer has agreed to purchase (for allocation to its Compartment 7) VWFS's right, title and interest in and to certain Receivables together with the related Ancillary Rights, on the terms of the Receivables Purchase Agreement.

(D) The Issuer has funded the acquisition of the Purchased Receivables through (i) advances under the Schuldschein Loans granted by several Lenders under the terms of the Programme Agreement, (ii) the issuance of the Notes purchased by several Note Purchasers under the terms of the Programme Agreement and (iii) advances under the Subordinated Loan in accordance with the Subordinated Loan Agreement granted by the Subordinated Lender.

(E) In order to comply with the Data Protection Rules, the Seller and the Issuer will jointly appoint Data Custody Agent Services B.V. as the Data Protection Trustee in accordance with the terms set forth below.

IT IS AGREED AS FOLLOWS:

1. **DEFINITIONS, INTERPRETATION AND COMMON TERMS**

1.1 **Definitions**

(a) Unless otherwise defined herein or the context requires otherwise, capitalised terms used in this Agreement have the meanings ascribed to them in clause 1 (*Definitions*) of the Master Definitions Schedule (the "**Master Definitions Schedule**") set out in the Incorporated Terms Memorandum (the "**Incorporated Terms Memorandum**") which is dated on or about the date of this Agreement and signed for purposes of identification, by each of the Transaction Parties. The terms of the Master Definitions Schedule are hereby expressly incorporated into this Agreement by reference. In addition:

"**DP Communication**" means any rights of data subjects that may be exercised under the UK General Data Protection Regulation along with any complaints, notices, enquiries, notices, investigations or other forms of communication received by either the Relevant Controller or the Data Protection Trustee from a data subject, an organisation acting on behalf of one or more data subjects or a supervisory authority.

"**Qualified Replacement Data Protection Trustee**" means any entity which is appointed to replace the Data Protection Trustee in accordance with clause 6 or clause 7.

"**Relevant Controller**" means VWFS until the first to occur of (i) the Servicer Termination Date or (ii) the service of a Notification Event Notice on the Obligors and thereafter the Issuer.

(b) If there is any conflict between the Master Definitions Schedule and this Agreement, this Agreement shall prevail.

1.2 **Interpretation**

Terms in this Agreement, except where otherwise stated or where the context otherwise requires, shall be interpreted in the same way as set forth in clause 2 (*Interpretation*) of the Master Definitions Schedule set out in the Incorporated Terms Memorandum.

1.3 **Common Terms**

(a) **Incorporation of Common Terms**

Except as provided below, the Common Terms apply to this Agreement and shall be binding on the Transaction Parties to this Agreement as if set out in full in this Agreement.

(b) **Common Terms**

In the event of any conflict between the provisions of the Common Terms and the provisions of this Agreement, the provisions of this Agreement shall prevail, subject always to compliance with clause 10 (*Non-Petition and Limited Recourse*) of the Common Terms.

(c) **Governing law and jurisdiction**

This Agreement and all matters (including non-contractual duties and claims) arising from or connected with it shall be governed by German law in accordance with clause 14 (*Governing Law*) of the Common Terms. Clause 15 (*Jurisdiction*) of the Common Terms applies to this Agreement as if set out in full in this Agreement.

2. **PORTFOLIO DECRYPTION KEY/TRANSFER OF PERSONAL DATA TO DATA PROTECTION TRUSTEE**

2.1 On a Business Day falling no later than 7 Business Days after the Closing Date, VWFS will deposit, or cause to be deposited, with the Data Protection Trustee a sealed containment key or such other information (the "**Portfolio Decryption Key**") necessary for the identification of the names and addresses of the respective Obligors for each contract number relating to a Financing Contract which relates to a Purchased Receivable.

2.2 On a Business Day falling no later than 7 Business Days after the Closing Date, VWFS will provide the Issuer with an encrypted list with the personal data (comprising the name, address and the contract number) of the Obligors (the "**Initial Encrypted List**") which may be read only with the Portfolio Decryption Key and which is necessary for the identification of the Obligors in relation to all Purchased Receivables.

2.3 In clause 4.6 (*Sales of Additional Receivables*) of the Receivables Purchase Agreement, VWFS further undertakes, on or about each Payment Date, to update the Initial Encrypted List (or the Additional Encrypted List, as applicable) (including to reflect any Purchased Receivables purchased in the Monthly Period) and to make such updated encrypted list available to the Issuer (the "**Additional Encrypted List**"). VWFS will, at the same time ensure that the Portfolio Decryption Key entrusted to the Data Protection Trustee remains valid and, if not, forthwith make a new Portfolio Decryption Key available to the Data Protection Trustee.

3. **SAFEKEEPING OF THE PORTFOLIO DECRYPTION KEY/NOTIFICATION OF THE OBLIGORS OF THE ASSIGNMENT OF PURCHASED RECEIVABLES**

3.1 The Data Protection Trustee shall carefully safeguard the Portfolio Decryption Key and protect it from unauthorised access by third parties. The Data Protection Trustee must keep confidential all data received hereunder. The Data Protection Trustee shall implement the technical and organisational measures necessary to secure and ensure the availability of the Portfolio Decryption Key (as required and in accordance with this Agreement), having regard to potential risks, available technology and the costs of implementation, and to ensure the implementation of the provisions of the General Data Protection Regulation.

3.2 Upon the occurrence of a Notification Event, the Issuer shall deliver a copy of the Initial Encrypted List or Additional Encrypted List to the Data Protection Trustee.

3.3 The Data Protection Trustee will, without undue delay following delivery of a Notification Event Notice, notify the Obligors of the assignment of the Purchased Receivables to the Issuer and instruct the Obligors to make all payments in respect of the Purchased Receivables to the Distribution Account of the Issuer. The notification to the Obligors shall include, to the extent provided by the Relevant Controller to the Data Protection Trustee in writing, all information required to be provided to the Obligors by the Data Protection Rules relating to how their personal data is being processed.

3.4 The right to disclose the assignments of the Purchased Receivables: (i) in connection with the Instruments, (ii) as required by law or (iii) in all other cases in which disclosure is

required under this Agreement, the other Transaction Documents, the Notes Conditions and the Loan Conditions also remain unaffected, as do any further express restrictions in other Transaction Documents. The Issuer undertakes to provide the Data Protection Trustee with any missing information for the completion of the above stipulated obligations to the extent the Issuer has access to such information.

3.5 References to 'personal data', 'process/processes/processing', 'processor', 'controller', 'transfer', 'data subject', 'personal data breach', 'supervisory authority' in clause 3.6 below shall be interpreted in accordance with the General Data Protection Regulation.

3.6 Whenever the Data Protection Trustee processes personal data in its role as a Data Protection Trustee (the "**Relevant Personal Data**") under this Agreement upon the delivery of a copy of the Initial Encrypted List or Additional Encrypted List pursuant to clause 3.2 above it shall act on behalf of the Relevant Controller as his processor and shall:

(a) comply with the Data Protection Rules applicable to it;

(b) only process such Relevant Personal Data for the purpose of performing its role as Data Protection Trustee and as instructed in writing under this Agreement or otherwise by the Relevant Controller. If the Data Protection Trustee is required to process the Relevant Personal Data other than in accordance with the Relevant Controller's written instructions by a European Union or Member State law, the Data Protection Trustee shall inform the Relevant Controller of that legal requirement before processing, unless that law prohibits such notice. In the event that the Data Protection Trustee is of the opinion that a processing instruction received from the Relevant Controller may infringe any applicable laws, then the Data Protection Trustee shall immediately notify the Relevant Controller of the same;

(c) not sub-contract any processing of the Relevant Personal Data to a third party (a "**Sub-processor**") except with the prior written consent of the Relevant Controller, not to be unreasonably withheld, and in any event such Sub-processor shall only be appointed if the Sub-processor:

(i) is subject to binding data protection terms which are equal or comparable to the Data Protection Rules with the Data Protection Trustee which are the same as those imposed on the Data Protection Trustee; and

(ii) provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the General Data Protection Regulation;

The Data Protection Trustee shall remain liable for any processing of the Relevant Personal Data carried out by a sub-contractor;

(d) not transfer the Relevant Personal Data outside of the EEA without obtaining the prior written consent of the Relevant Controller, not to be unreasonably withheld, and in any event shall ensure that the transfer is in compliance with the General Data Protection Regulation and all applicable laws;

(e) securely delete all copies of the Relevant Personal Data after it ceases to be the Data Protection Trustee unless otherwise provided by applicable law;

(f) provide any reasonably required assistance to the Relevant Controller to enable the Relevant Controller to demonstrate compliance with its obligations under Article 32 to 36 of the General Data Protection Regulation, and taking into account the nature

of the processing and insofar as possible, by implementing appropriate technical and organisational measures to ensure a level of security over the Relevant Personal Data as appropriate to the risk;

(g) notify the Relevant Controller within 72 hours of receiving a DP Communication and forward the contents of any such DP Communication in full;

(h) make available all information necessary in order to enable the Relevant Controller to comply and demonstrate compliance with Data Protection Rules and within five (5) Business days of the Relevant Controller's written request (or such shorter time as required by a supervisory authority), and allow for and contribute to audits, including inspections, conducted by the Relevant Controller, an auditor mandated by the Relevant Controller or a supervisory authority; and

(i) implement appropriate technical and organisational security measures (including ensuring that all personnel are subject to binding confidentiality obligations to ensure the confidentiality of the Relevant Personal Data) to ensure a level of security appropriate to the risks that are presented by the processing of the Relevant Personal Data. The measures will take into account the factors specified in Article 32 of the General Data Protection Regulation. In particular, measures shall be taken in order:

(i) to prevent unauthorised persons from gaining access to data processing systems with which Relevant Personal Data are processed or used (access control),

(ii) to prevent data processing systems from being used without authorisation (access control),

(iii) to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that Relevant Personal Data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage (access control),

(iv) to ensure that Relevant Personal Data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport or storage on data carriers, and that it is possible to check and to establish to which bodies the transfer of Relevant Personal Data by means of data transmission facilities is envisaged (transmission control),

(v) to ensure that it is possible afterwards to check and establish whether and by whom Relevant Personal Data have been entered into data processing systems, modified or removed (input control),

(vi) to ensure that, in the case of commissioned processing of Relevant Personal Data, the data are processed strictly in accordance with the instructions of the principal (job control),

(vii) to ensure that Relevant Personal Data are protected from accidental destruction or loss (availability control),

(viii) to ensure that data collected for different purposes is processed separately, and

(ix) to include a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(j) take the following measures and any additional appropriate measures:

(i) (**access control to premises and facilities**) technical and organisational measures to control access to premises and facilities, particularly to prevent unauthorised persons from gaining access to data processing systems for processing or using Relevant Personal Data, in particular but not limited to access control system (such as ID reader, magnetic card, chip card, security gate) and keys (and the issue thereof) and corresponding documentation;

(ii) (**access control to systems**) measures to prevent data processing systems from being used without authorisation, in particular but not limited to password procedures (including special characters, minimum length, change of password), firewall and anti-virus protection;

(iii) (**access control to data**) measures to ensure that persons authorised to use data processing systems have access only to those data they are authorised to access, and that Relevant Personal Data cannot be read, copied, altered or removed without authorisation during or after processing, in particular but not limited to individual authorisation profiles and data media storage in lockable facilities;

(iv) (**disclosure control**) measures to ensure that Relevant Personal Data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media, and that the target entities for any transfer of Relevant Personal Data by means of data transmission facilities can be established and verified, in particular but not limited to, the encryption of sensitive data;

(v) (**input control**) the establishment of an audit trail to document whether and by whom Relevant Personal Data have been entered into, modified in, or removed from data processing systems, in particular but not limited to access rules and authorisation rules.

(vi) (**control of instructions**) measures to ensure that Relevant Personal Data are processed solely in accordance with the Relevant Controller's instructions, in particular but not limited to periodic reviews of sub-contractors by the Data Protection Trustee and written or electronic documentation of the Relevant Controller's instructions;

(vii) (**availability control**) measures to ensure that Relevant Personal Data are protected against accidental destruction or loss, in particular but not limited to backup procedures and firewall and anti-virus protection; and

(viii) (**segregation control**) measures to ensure that data collected for different purposes can be processed separately, in particular but not limited to user profiles and authorisation concept.

3.7 The Data Protection Trustee shall give written notice to the Relevant Controller, with reasonable details, within 48 hours of it becoming aware of, or comes to have reasonable grounds to suspect, the occurrence of any Personal Data breach or other material incident

prejudicing, or revealing a material weakness in, the security of the personal data contained in the Initial Encrypted List or Additional Encrypted List (or any other Relevant Personal Data being processed by or on behalf of the Data Protection Trustee) while in its possession or under its control (a "**Data Security Incident**").

3.8 In relation to any Data Security Incident, the Data Protection Trustee shall:

(a) take all reasonable steps to identify and correct the underlying cause of the Data Security Incident so as to eliminate or minimise the risk of its repetition and the occurrence of similar Data Security Incidents;

(b) take such steps as the Relevant Controller may reasonably request and the Data Protection Trustee may reasonably be able to take to assist the Relevant Controller in addressing the adverse consequences for the Relevant Controller, and complying with the Relevant Controller's obligations under the Data Protection Rules in relation to the Data Security Incident; and

(c) report to the Relevant Controller, promptly and at regular intervals, on the steps taken under clauses 3.8(a) and 3.8(b) and their results.

3.9 The duration of the data processing under this Agreement is for the duration of this Agreement.

4. DELIVERY OF THE PORTFOLIO DECRYPTION KEY BY THE DATA PROTECTION TRUSTEE

The Data Protection Trustee shall immediately surrender the Portfolio Decryption Key transferred to it pursuant to clause 2 (*Portfolio Decryption Key/Transfer of personal data to Data Protection Trustee*) above only in the following circumstances:

(a) at the request of the Security Trustee, to a successor Servicer appointed in accordance with the provisions of the Servicing Agreement; or

(b) to the Seller or, at the request of the Issuer, Seller or the Security Trustee, to a Qualified Replacement Data Protection Trustee upon termination of the Data Protection Trust Agreement pursuant to clause 6 (*Termination by the Data Protection Trustee*) below or upon replacement of the Data Protection Trustee pursuant to clause 7 (*Replacing the Data Protection Trustee*) below;

unless any such recipient under paragraphs (a) or (b) above is prohibited from receiving the Portfolio Decryption Key under the applicable provisions of Data Protection Rules or banking secrecy provisions (*Bankgeheimnis*). The Data Protection Trustee is under no obligation to verify whether such a prohibition applies in respect of any recipient under paragraphs (a) or (b) above and/or to verify whether or not any replacement Servicer meets the above eligibility criteria.

5. COMPENSATION

The Issuer shall remunerate the Data Protection Trustee in an amount to be determined in a separate agreement between the Issuer and the Data Protection Trustee. All expenses and costs incurred by the Data Protection Trustee in the course of fulfilling its duties under this Agreement or which otherwise arise from this Agreement shall be deemed fully compensated by such remuneration.

6. TERMINATION BY THE DATA PROTECTION TRUSTEE

6.1 The Data Protection Trustee may terminate its appointment as Data Protection Trustee for good cause (*aus wichtigem Grund*) at any time, provided that, at the same time or prior thereto, the Data Protection Trustee appoints a Qualified Replacement Data Protection Trustee, on behalf of the Issuer, to assume the Data Protection Trustee's rights and obligations under this Agreement. As soon as the Data Protection Trustee provides the Seller with notice of its intention to resign as data protection trustee, the Seller shall exercise its best efforts to name a qualified candidate to become a successor pursuant to the first sentence of this clause 6.1.

6.2 Notwithstanding the obligation of the Data Protection Trustee to appoint a Qualified Replacement Data Protection Trustee in accordance with clause 6.1, the Issuer and the Security Trustee may jointly make this appointment instead of the Data Protection Trustee.

6.3 The appointment of a Qualified Replacement Data Protection Trustee pursuant to clause 6.1 or 6.2 is permissible only if (i) the Seller consents to the appointment of the proposed Qualified Replacement Data Protection Trustee and (ii) the Issuer consents to the appointment of the proposed Qualified Replacement Data Protection Trustee. The consent referred to in (i) shall be deemed given if the Issuer or the Security Trustee or the Data Protection Trustee has requested the Seller in writing to consent to the appointment and the consent or substantiating evidence of good cause for refusal of consent is not received by the Issuer, the Security Trustee or the Data Protection Trustee (as applicable) within five (5) Business Days following receipt of the request by the Seller. The consent referred to in (ii) shall be deemed given if the Data Protection Trustee has requested the Issuer in writing to consent to the appointment and the consent or substantiating evidence of good cause for refusal of consent is not received by the Data Protection Trustee within five (5) Business Days following receipt of the request by the Issuer.

6.4 Notwithstanding a termination pursuant to clause 6.1, the rights and obligations of the Data Protection Trustee shall remain in force until a Qualified Replacement Data Protection Trustee has been effectively appointed and the Portfolio Decryption Key has been delivered to it.

6.5 The outgoing Data Protection Trustee shall, in case of a termination, reimburse (on a pro rata basis) the Issuer for any up-front fees paid by the Issuer for periods after the date on which the substitution of the Data Protection Trustee is taking effect. In case of a termination by the Issuer for good cause (*aus wichtigem Grund*) as a result of a breach of obligation by the Data Protection Trustee acting with gross negligence (*grobe Fahrlässigkeit*) or wilful misconduct (*Vorsatz*), the outgoing Data Protection Trustee shall reimburse the Issuer for the costs (including legal costs and administration costs) or pay any costs incurred for the purpose of appointing a new Data Protection Trustee up to a maximum amount of GBP 20,000 (the "**Replacement Cost**"). For the avoidance of doubt, such Replacement Cost shall cover any and all replacement costs incurred in respect of the replacement of Data Custody Agent Services B.V. as Data Protection Trustee.

7. REPLACING THE DATA PROTECTION TRUSTEE

The Issuer or the Security Trustee may replace the Data Protection Trustee by a Qualified Replacement Data Protection Trustee, for good cause grounded in the conduct of the Data Protection Trustee, especially if the Data Protection Trustee has materially breached its duties under this Agreement and the Seller consents to the appointment of the proposed Qualified Replacement Data Protection Trustee by the Issuer.

8. **ON-DELIVERY OF THE PORTFOLIO DECRYPTION KEY**

In situations involving a replacement of the Data Protection Trustee pursuant to clause 6 or clause 7, the Data Protection Trustee shall promptly deliver the Portfolio Decryption Key pursuant to this Agreement to the Qualified Replacement Data Protection Trustee.

9. **LIABILITY OF THE DATA PROTECTION TRUSTEE**

The Data Protection Trustee shall be liable for breach of its duties under this Agreement only if and to the extent it fails to meet the standard of care that it would exercise in its own affairs (*Sorgfalt wie in eigenen Angelegenheiten*).

IN WITNESS WHEREOF, this Agreement is duly executed and delivered on the date and the year first above written.

SIGNATURE PAGES TO THE DATA PROTECTION TRUST AGREEMENT DATED 27 NOVEMBER 2023

DRIVER UK MASTER S.A., acting for and on behalf of its Compartment 7

as Issuer

Signed by: _____ Signed by: _____

Title: _____ Title: _____

VOLKSWAGEN FINANCIAL SERVICES (UK) LIMITED

as Seller and Servicer

Signed by: _____

Title: _____

Intertrust Trustees GmbH

as Security Trustee

Signed by: _____

Title: _____

Data Custody Agent Services B.V.

as Data Protection Trustee

Signed by:_____

Title: _____

Signed by:_____

Title: _____