Data Privacy and Security Addendum ("DPSA")

Between Volkswagen Group of America ("VWGoA") and _____ ("Supplier")

This DPSA between Volkswagen Group of America, Inc. (VWGoA) and _____ (Supplier) shall be effective as of the date executed below. The DPSA applies to all Processing of VWGoA Personal Information by Supplier, including under the _____ with the effective date of _____ (which this DPSA amends and is incorporated into) and all other agreements between VWGoA and Supplier unless otherwise specified in an agreement (collectively, the "Agreement"). In the event of a conflict between the DPSA and the Agreement, the terms and conditions of the DPSA shall prevail. The parties' obligations under this DPSA shall survive the termination or expiration of any underlying agreement between the parties to the extent that Supplier lawfully continues to retain or Process any VWGoA Data.

Nothing in this DPSA limits or restricts VWGoA's rights or Supplier's obligations under the Agreement in relation to the protection of Personal Information (defined below) or permits Supplier to Process (defined below) (or permit the Processing of) Personal Information in a manner which is prohibited by the Agreement. All VWGoA Data (defined below) shall be deemed "Confidential Information" under the Agreement.

1. Definitions.

1.1 "Applicable Law" shall mean all applicable state, federal and international privacy, data protection and security laws and regulations applicable to Personal Information, such as the California Privacy Rights Act of 2020 (CPRA), California Consumer Privacy Act (CCPA), Virginia Consumer Data Act (VCDPA), Colorado Privacy Act (CPA), US state security and breach notification laws, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA), the EU General Data Protection Regulation 2016/679 (GDPR), the United Kingdom (UK) Data Protection Act 2018, the UK GDPR and the Swiss Federal Act on Data Protection (FADP), as amended or replaced from time to time.

1.2 "Authorized Persons" shall mean Supplier's employees, contractors, subcontractors, or other agents who need to access VWGoA Data or VWGoA Systems to enable Supplier to perform the Services and who are bound by confidentiality and other obligations sufficient to protect VWGoA Data in accordance with the terms and conditions of this DPSA and Applicable Law.

1.3 "Standard Contractual Clauses" or "SCCs" shall mean (i) the standard contractual clauses for the cross-border transfer of Personal Information to Controllers and Processors established in Third Countries approved and published by the European Commission and adopted by the Swiss Federal Data Protection and Information Commissioner ("Swiss FDPIC"), incorporated herein by reference (collectively, the "EU Area SCC's"); (ii) the UK International Transfer Addendum adopted by the UK Information Commissioner's Office (UK ICO) for data transfers from the UK to Third Countries; or (iii) any similar such clauses approved by a data protection regulator relating to data transfers to Third Countries, including without limitation any successor clauses thereto.

1.4 "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, and any other information regulated by Applicable Law, such as, "Personal Information," "Personal Data," "Non-Public Personal Information," "Protected Health Information," "Sensitive Information," "Sensitive Personal Information," "Special Categories of Personal Information," or "Special Categories of Personal Data."

1.5 "Process" or "Processed" or "Processing" shall mean any operation or set of operations which is performed on Personal Information or sets of Personal Information, whether or not by automated means,

such as, access, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.6 "Security Breach" shall mean the accidental or unlawful destruction, loss, alteration, unauthorized use, disclosure, acquisition, or access to VWGoA Data or VWGoA Systems that compromises the availability, confidentiality or integrity of VWGoA Data or VWGoA Systems.

1.7 "Sell," "Selling," "sale," or "sold" and "share," "shared," or "sharing" shall have the meanings set forth in Applicable Law, including the CCPA and CPRA.

1.8 "Services" means the products or services provided or to be provided under the Agreement.

1.9 "Third Country" means countries that have not received an adequacy decision from an applicable authority relating to data transfers where required by applicable Data Protection Laws, including by such regulators such as the European Commission, UK ICO, or Swiss FDPIC relating to data transfers

1.10 "UK International Transfer Addendum " means the international data transfer addendum to the Standard Contractual Clauses adopted by the UK Information Commissioner ("UK ICO") for cross-border transfers of Personal Information to Third Countries and incorporated herein by reference, as amended by the UK ICO, and as may be amended or replaced by the UK ICO or/and UK Secretary of State from time to time.

1.11 "VWGoA Data" shall mean any VWGoA non-public or proprietary information and data in any form, ***including Personal Information***, provided by VWGoA and its authorized agents or subcontractors or otherwise Processed by Supplier in connection with the provision of Services under the Agreement.

1.12 "VWGoA Systems" shall mean any VWGoA system or network to which Supplier has access in order to perform Services for VWGoA.

2. Compliance with Laws

2.1 Supplier shall comply with Applicable Law relating to the privacy and security of VWGoA Data Processed by Supplier for or on behalf of VWGoA, and its affiliates, including, without being limited to, the laws of the countries whose citizens' or residents' Personal Information Supplier Processes in performing the Services. In the event of a claim against Supplier alleging a violation of a state or country specific Applicable Law, Supplier agrees to submit to a court of competent jurisdiction in that state or country.

2.2 To the extent that Supplier shares Personal Information, as defined by applicable law, with VWGoA, Supplier will do so in compliance with Applicable Law, including providing appropriate notice (including notice regarding the sharing of Personal Information with third parties) and obtaining consent if required; or, if Supplier is not the first party collector of such Personal Information, ensuring that suppliers of such data have provided appropriate notices and obtained any required consents to share such data. Supplier agrees to make available, upon request, information to demonstrate compliance, including a copy of the compliant notices or consents.

2.3 GLBA. To the extent the Gramm-Leach-Bliley Act applies, Supplier expressly understands and acknowledges that Supplier may have access to, or VWGoA may disclose to Supplier, "non-public personal information" ("NPPI"), as such term is defined in Regulation P issued by the Consumer Financial Protection Bureau. Without limiting any other obligations in this Addendum, the following shall apply to NPPI:

(a) Supplier will use or disclose NPPI only as strictly necessary to carry out the purposes for which VWGoA is disclosing the information to Supplier.

(b) Supplier has implemented and will continue to maintain safeguards reasonably designed to (i) ensure the security and confidentiality of NPPI; (ii) protect against any anticipated threats to or hazards to the security or integrity of NPPI; and (iii) protect against unauthorized access to or use of NPPI that could result in substantial harm or inconvenience to any individual.

2.4 As between the parties, all VWGoA Data remains, at all times, the property and Confidential Information of VWGoA, and VWGoA has the right to direct Supplier in connection with Supplier's Processing of such VWGoA Data.

2.5 Supplier shall immediately inform VWGoA if it cannot comply with an instruction or, in its opinion, an instruction infringes any law applicable to VWGoA or Supplier, or if Supplier can no longer meet its obligations under Applicable Law.

2.6 VWGoA hereby instructs Supplier to Process Personal Information as necessary for the provision of the Services.

3. Supplier's Obligations

3.1 Supplier shall Process VWGoA Data and access VWGoA Systems solely for the purpose of providing the Services in accordance with the Agreement and upon VWGoA's written instructions, and not for any other purpose. Supplier shall not retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services specified in the Agreement or as otherwise permitted by law, including retaining, using, or disclosing the Personal Information for a commercial purpose other than performing the Services. Without limiting the generality of the foregoing, Supplier agrees it shall not: (i) Sell or Share the Personal Information; (ii) retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services in accordance with the Agreement, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing Services specified in the Agreement; (iii) retain, use, or disclose the Personal Information outside of the direct business relationship between Supplier and VWGoA, or (iv) combine VWGoA Data, including Personal Information, with Personal Information it receives from another source except to perform business purposes permitted by Applicable Law. Supplier hereby certifies that it understands the restrictions set forth in this Section and will comply with them.

3.2 Supplier shall maintain records of Processing activities carried out pursuant to this DPSA, containing all relevant details required by Applicable Law, but at a minimum, the following:

- the name and contact details of the Supplier and any other subcontractors and, where applicable, of the VWGoA' or Supplier's representative;
- the categories of Processing carried out on behalf of VWGoA;
- where applicable, information on cross-border transfers, including transfers of Personal Information to a third country or an international organization, including the identification of

that third country or international organization and, in the case of transfers outside of the legally specified transfer mechanisms, the documentation of suitable safeguards for the Personal Information;

- where possible, a general description of the technical and organizational security measures.

- Supplier agrees to make such records available upon request to VWGoA and any relevant government authority.

3.3 Supplier shall provide information about Supplier and its Processing of VWGoA Data as reasonably requested by VWGoA for the purpose of assisting VWGoA in complying with its obligations under Applicable Law or contracts, including the exercise of Data Subject Rights (as defined in section 3.5 below) and Security Breach notification obligations as well as investigations. Supplier also shall provide VWGoA with reasonable assistance in complying with its obligations under Applicable Laws, including without limitation conducting data protection, privacy, or security risk assessments and consultations with VWGoA's supervisory or regulatory authorities.

3.4 Supplier shall immediately notify VWGoA of any requests, inquiries or complaints received about the Processing of Personal Information from third parties, including regulators, authorities, data subjects and law enforcement authorities. Supplier shall not respond to any such requests, inquiries or complaints except on the documented instructions of VWGoA or as required by Applicable Law and in all cases subject to the obligations in Section 3.6.

3.5 If VWGoA responds or allows the response to a request, inquiry or complaint (whether received through Supplier or by VWGoA directly), Supplier shall provide VWGoA with reasonable cooperation and assistance in responding to any such request, inquiry or complaint in a manner that allows VWGoA to meet the legal timelines for response, including requests by data subjects to access, amend, transfer, opt out of Sale or Sharing, delete or exercise other data subject rights around Personal Information (collectively, "Data Subject Rights"). In the event that VWGoA requests that Supplier delete Personal Information in connection with a Data Subject Rights' request, Supplier shall notify its own subcontractors to delete such Personal Information about the data subject, which is collected, used, Processed or retained by such subcontractor.

3.6 If disclosure of VWGoA Data is required by Applicable Law or a compulsory legal process, Supplier shall, unless prohibited by Applicable Law or compulsory legal process: (i) notify VWGoA promptly in writing before complying with any such disclosure request in order to provide VWGoA an opportunity to intervene, if appropriate; and (ii) disclose the minimum amount of VWGoA Data necessary to comply with Applicable Law or a compulsory legal process.

4. Sub-processing

4.1 VWGoA on its own behalf grants Supplier a general consent to engage Authorized Persons, including subcontractors, to perform the Services as needed. The list of authorized subprocessors at the date of the signature of this DPSA is included in Annex 2 to this DPSA unless otherwise specified in the Agreement.

4.2 If Supplier uses subcontractors to fulfill its obligations under the Agreement, it will:

- Conduct reasonable due diligence to ensure that the subcontractor is capable of providing the level of protection for the VWGoA Data or Systems as required by the DPSA and Applicable Law;

- Execute a written contract detailing the terms of the sub-processing activities and providing for provisions which offer at least the same level of protection of VWGoA Data or VWGoA Systems as this DPSA and provide a copy to VWGoA;

- Ensure no transfer outside the jurisdiction in which the Personal Information was collected without prior authorization from VWGoA;

- Ensure that no Personal Information from the European Economic Area (EEA), Switzerland or the United Kingdom (UK) is transferred to countries and territories, which the EEA, Switzerland and the UK have not granted an adequacy status, without the execution between the Supplier and subcontractor of a valid transfer mechanism, such as the EU Standard Contractual Clauses (SCCs) Module 3 (Processor to Processor) and/or the UK International Transfer Addendum;

- Ensure any subcontractor adheres to the terms of this DPSA as if it were a party to it;

- Keep a list of subcontractor agreements, which shall be updated regularly and made available to VWGoA upon request;

- Ensure that the subcontractor performs the obligations under this DPSA, as if it were a party to the DPSA in place of Supplier, except that Supplier will coordinate communication with VWGoA and is entitled to make and receive communication in relation to this DPSA on behalf of any subcontractors. Supplier shall obtain the necessary authorization from the subcontractors in this regard.

- Ensure that Supplier notifies VWGoA of any subcontractors hired by its subcontractors and that such additional subcontractors are bound by written agreement to the terms of this DPSA, Applicable Law and offer the same level of protection to VWGoA Data or VWGoA Systems as Supplier and its subcontractors.

4.3 Supplier shall give VWGoA prior written notice of the appointment of any subcontractor, including full details of the Processing to be undertaken by the subcontractor, the name and contact details of the subcontractor and the date of the subcontracting agreement. If, within 4 weeks of receipt of that notice, VWGoA notifies Supplier in writing of any objections (on reasonable grounds) to the proposed appointment, Supplier shall not appoint that proposed subcontractor except with the prior written authorization of VWGoA. Should Supplier choose to retain the objected-to subcontractor, Supplier will notify VWGoA at least fourteen (14) days before appointing the subcontractor and VWGoA may immediately discontinue using the relevant portion of the Service and VWGoA may terminate the relevant portion of the Service within thirty (30) days. Upon termination by VWGoA pursuant to this section, Supplier shall refund VWGoA any prepaid fees for the terminated portions of the Service that were to be provided after the effective date of termination.

4.4 Where subcontractor fails to fulfil its obligations with respect to VWGoA Data or Systems, Supplier shall remain fully liable to VWGoA for that subcontractor.

5. Disclosure of and Access to Personal Information.

5.1 Supplier shall take reasonable steps to ensure the reliability of any Authorized Persons who may have access to VWGoA Data or VWGoA Systems, ensuring in each case that access is strictly limited to those Authorized Persons who need to know / access the relevant VWGoA Data or VWGoA Systems, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Law in the context of that Authorized Persons' duties to VWGoA, ensuring that all such Authorized Persons are subject to confidentiality undertakings or professional or statutory obligations of confidentiality and do not Process VWGoA Data or access VWGoA Systems except on the written instructions of VWGoA and in accordance with the Agreement and this DPSA.

5.3 Supplier shall instruct all Authorized Persons to whom it provides VWGoA Data or allows access to VWGoA Systems to implement appropriate safeguards to protect the VWGoA Data or VWGoA Systems, which provide at least the same degree of protection as the terms of this DPSA, and to immediately report to Supplier any actual or potential Security Breach involving VWGoA Data or VWGoA Systems of which they become aware. Supplier shall be responsible for and remain liable for each Authorized Person's compliance with the terms of this DPSA.

5.4 Supplier shall limit access to VWGoA Data and VWGoA Systems by Authorized Persons to ensure that any given Authorized Person receives only the level of access necessary to perform their job functions to provide the Services to VWGoA.

5.5 Supplier shall provide VWGoA with the name and contact details of the person who is responsible for compliance with this DPSA within Supplier.

5.6 Supplier shall not disclose the VWGoA Data or allow access to VWGoA Systems to any third party beyond Authorized Persons, unless required to do so by law to which the Supplier is subject; in such a case, the Supplier shall inform VWGoA of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

6. Return or Destruction of VWGoA Data

6.1 Upon termination or expiration of the Agreement for any reason, or if any part of the VWGoA Data retained by Supplier ceases to be required by Supplier to perform its obligations under the Agreement, Supplier shall, and shall use reasonable means to ensure that all Authorized Persons, as requested by VWGoA, either destroy all VWGoA Data Processed under this Agreement and in its possession or control (including all originals and copies) as soon as practicable, and no later than 30 days after termination or expiration or it is no longer required or, return all such VWGoA Data to VWGoA in any manner reasonably requested by VWGoA, within 30 days.

6.2 Upon VWGoA' request, Supplier must promptly certify in writing to VWGoA that it has destroyed or returned, as applicable, all VWGoA Data. In the event that Supplier is unable to return or destroy all VWGoA Data, Supplier shall, and shall ensure that each affected Authorized Person, retain VWGoA Data only to the extent and for such period as required by Applicable Law, maintain the security and confidentiality of all such retained VWGoA Data in accordance with the protections of this DPSA, and ensure that such VWGoA Data is only Processed as necessary for the purposes specified in the Applicable Law requiring its storage and for no other purposes.

7. Security Measures.

7.1 Supplier warrants and undertakes to have in place and shall maintain physical, organizational and technical processes and procedures and measures to protect against any unauthorized or unlawful access, Processing, loss, destruction, theft, damage, use, disclosure or other compromise of VWGoA Data or

VWGoA Systems (collectively, "Appropriate Safeguards"), including, at a minimum, the technical and organizational security measures set forth as **Annex 3** to this DPSA. Such Appropriate Safeguards shall, in all material respects, be in accordance with good industry practice and not less stringent than the measures Supplier applies to its own equivalent of VWGoA Data or VWGoA Systems of similar kind. These Appropriate Safeguards shall be appropriate to the harm that might result from any risks to VWGoA Data or VWGoA Systems and having regard to the nature of the VWGoA Data or VWGoA System which is to be protected and shall take into consideration the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing and the risks to the individuals whose Personal Information it Processes on behalf of VWGoA.

7.2 PCI Compliance. To the extent applicable, Supplier agrees to fully comply with the PCI Standards and provide to VWGoA a Report of Compliance completed by a qualified security assessor no less than once annually. For purposes of this section, "PCI Standards" shall mean all applicable standards, guidance, and requirements issued by the PCI-SSC, including but not limited to the Payment Card Industry Data Security Standard ("PCI-DSS"), Payment Application Data Security Standard ("PA-DSS"), Tokenization Product Security Guidelines, and any additional applicable standards, guidelines, or requirements established from time to time by a major payment card network with respect to the security of Account Data. Any reference to a standard, guideline, or requirement document means the operable version of the document, as its issuing organization may amend it from time to time.

8. Security Breach and Response

8.1 Supplier shall promptly notify VWGoA without undue delay and no later than 24 hours upon Supplier becoming aware of an actual or potential Security Breach. Supplier should notify VWGoA by telephone to Supplier's primary business contact and via email at **both** privacy@vw.com and cybersecurity@vw.com if it has knowledge that there is, or reasonably believes that there has been, an actual or potential Security Breach. Notice must include the following:

- the nature of the Security Breach,
- the categories and numbers of data subjects concerned, and the categories and numbers of records concerned;
- the name and contact details of the Supplier contact from whom more information may be obtained;
- describe the likely consequences of the Security Breach; and
- describe the measures taken or proposed to be taken to address the Security Breach.
- Other information as VWGoA may reasonably request

8.2 Supplier shall (i) cooperate with VWGoA in the manner reasonably requested by VWGoA and in accordance with law to investigate and resolve the Security Breach, and mitigate any harmful effects of the Security Breach; (ii) promptly implement any necessary remedial measures to ensure the protection of VWGoA Data or VWGoA Systems; and (iii) properly document responsive actions taken related to any Security Breach, including, without limitation, post-incident review of events and actions taken to make changes in business practices to ensure the protection of VWGoA Data or VWGoA Systems.

8.3 Except as required by Applicable Law or regulation, Supplier agrees that: (i) it shall not inform any third party of any Security Breach without first obtaining VWGoA' prior written consent, other than to inform a complainant that VWGoA shall be/has been informed of the Security Breach; and (ii) VWGoA shall have the right, but not the obligation, to determine whether notice of the Security Breach is to be provided to any individuals, authorities, regulators, law enforcement agencies, consumer reporting agencies, or others and the contents of any such notice.

8.4 If the Security Breach was a result of Supplier's or Authorized Persons' negligence or breach of the requirements of this DPSA, Supplier shall bear all costs associated with (i) any investigations and resolution of the Security Breach, including, but not limited to, internal investigations as well as investigations by regulators or other authorities; (ii) notifications to individuals, authorities, regulators, or others; (iii) defense of any and all claims based on the Security Breach; (iv) any remedial actions required by law, recommended by an authority, regulator, governmental body or agreed to by the Parties; (v) any other costs associated with the Security Breach. For a Security Breach resulting from Supplier's or Authorized Persons' negligence or breach of the requirements of this DPSA that results in a breach defined by Applicable Law, in addition to the above and where available, Supplier agrees to bear the costs associated with i) the provision of two years of credit monitoring by a reputable provider; and (ii) establishing a toll-free number and call center for affected individuals to receive information.

9. Cross-Border Transfer of Personal Information

9.1 Supplier shall not Process Personal Information in a jurisdiction outside of the jurisdiction in which it was collected without providing notice to VWGoA and an opportunity to object as further described in Annex 1. To the extent that VWGoA does not object to the Processing of Personal Information outside of the jurisdiction in which it was collected is provided, Supplier agrees to comply with Applicable Law governing the cross-border transfer of Personal Information.

9.2 If the activities of the Supplier involve the Processing of Personal Information from the EEA, the UK, or Switzerland to Third Countries, Supplier agrees to comply with a legally valid data transfer mechanism, including Supplier's EU- or UK-approved Binding Corporate Rules for Processors (and related obligations) or to execute Standard Contractual Clauses with VWGoA to ensure compliance with restrictions on cross-border transfers.

9.3 If the activities of the Supplier involve the Processing of Personal Information from the EEA Third Countries, or the Supplier does not have EU-approved Binding Corporate Rules for Processors, the Parties hereby incorporate the Standard Contractual Clauses (Module 2: Transfers Controller to Processor) as further described in Annex 1.

9.4 If the activities of the Supplier involve the Processing of Personal Information from the UK to Third Countries or the Supplier does not have UK-approved Binding Corporate Rules for Processors, the Parties hereby incorporate the UK International Transfer Addendum as described in this 9.4 and Annex 1: as follows:

a. Each Party agrees to be bound by the terms and conditions set out in the UK International Transfer Addendum, in exchange for the other Party also agreeing to be bound by the UK International Transfer Addendum;
b. The Standard Contractual Clauses will be interpreted in accordance with Part 2 of the UK International Transfer Addendum;
c. Sections to 9 of the UK Transfer Addendum override Clause 5 (Hierarchy) of the 11Standard Contractual Clauses;
d. For the purposes of Section 12 of the UK International Transfer Addendum, the Standard Contractual Clauses will be amended in accordance with Section 15 of the UK International Transfer Addendum;
e. Information required by Part 1 of the UK International Transfer Addendum is provided as Exhibit 1 to this DPSA;
f. To the extent that any revised transfer addendums or mechanisms are issued by the UK ICO,

the Parties agree to incorporate such revisions in accordance with Section 18-20 of the UK Transfer Addendum.

9.5 If the activities of the Supplier involve the Processing of Personal Information from Switzerland to Third Countries, the Parties hereby incorporate the C2P EU SCC's by reference. These EU SCC's will be deemed completed as outlined in Section 9.3 above and Annex 1 with the following changes:

- References to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the UK GDPR or Swiss DPA.
- References to "EU", "Union" and "Member State" shall be interpreted to include references to the "UK" or "Switzerland
- .

9.6 With respect to any onward transfers or Subprocessing conducted under the C2P Standard Contractual Clauses, Supplier understands and agrees that it is subject to all the obligations under this DPSA and the C2P Standard Contractual Clauses pursuant to Clause 9 of the C2P Standard Contractual Clauses. In particular, data subjects can enforce against the Supplier as third-party beneficiaries the clauses in the underlying C2P Standard Contractual Clauses as laid down in Clause 3 of the C2P Standard Contractual Clauses. Similarly, with respect to any Subprocessing conducted under the C2P UK International Transfer Addendum, Supplier understands and agrees that it is subject to all the obligations under this DPSA and the C2P UK International Transfer Addendum pursuant to Clause 11 of the C2P UK International Transfer Addendum. . In particular, data subjects can enforce against the Supplier as third-party beneficiaries the clauses in the underlying C2P UK International Transfer Addendum as laid down in Clause 3 of the C2P UK International Transfer Addendum.

9.6 The Parties agree to amend this DPSA or put in place additional safeguards, to enable them to comply with any international data transfer restrictions pertaining to the Personal Information, in case a data transfer mechanism is no longer deemed adequate.

10. Audit Rights

10.1 Supplier shall make available to VWGoA on request all information necessary to demonstrate compliance with this DPSA, and shall allow for and contribute to audits, including inspections at least once every twelve (12) months, by VWGoA or an auditor mandated by VWGoA in relation to the Processing of the VWGoA Data or access to VWGoA Systems by Supplier.

10.2 VWGoA shall give Supplier reasonable notice of any audit or inspection to be conducted under this section and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to Supplier's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

10.3 Supplier shall cooperate with and provide reasonable assistance to VWGoA, allowing VWGoA to satisfy its obligations under Applicable Law, taking into account the nature of the Processing and the information available to Supplier (and its Subcontractors). Supplier shall also cooperate with VWGoA and provide any required information to VWGoA in any investigation of VWGoA or Supplier by an authority or governmental or regulatory authority, any internal investigation by VWGoA or any legal proceedings regarding the Processing of Personal Information. Supplier will inform VWGoA immediately of any inspections, proceedings or measures conducted by a governmental or regulatory authority, court or tribunal and coordinate with VWGoA before responding to the extent legally permitted.

11. Remedies for Failure to Comply with DPSA

In the event that Supplier materially breaches this DPSA or fails to comply with Applicable Law, VWGoA shall have the right to terminate the Agreement immediately, or stop Supplier Processing and demand remediation of any unauthorized use of Personal Information.

12. Severance

Should any provision of this DPSA be invalid or unenforceable, then the remainder of this DPSA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

By signing this DPSA, Supplier certifies that it understands the restrictions set forth in this DPSA and will comply with them.

VWGoA Corporation	Supplier:
By:_____	By:_____
Date: _____	Date: _____

ANNEX 1:

Description of Processing and Transfer Details

A. List of Parties

Name (Data Exporter)	VWGoA
Address	*2200 Woodland Pointe Avenue, Herndon, VA 20171*
Contact person's name, position and contact details	*[Insert VWGoA's contact information]*
Activities relevant to the data transferred under the Clauses	In addition to the information described below (Section B. Description of Transfer), the activities relevant to the data transferred for Supplier's performance of the Services more fully described in the Agreement and applicable ordering documents
Signature and date	*See* at the end of this DPSA.
Role (controller / processor)	The indicated data exporter(s) each serve as data controller.

Name (Data Exporter)	Supplier, as specified at the beginning of this DPSA.
Address	*[Insert Supplier's address]*
Contact person's name, position and contact details	*[Insert Supplier's contact information]*
Activities relevant to the data transferred under the Clauses	In addition to the information described below (Section B. Description of Transfer), the activities relevant to the data transferred for Supplier's performance of the Services more fully described in the Agreement and applicable ordering documents
Signature and date	*See* at the end of this DPSA.
Role (controller / processor)	Processor

B. Description of Transfer:

1. Processing Information.

Categories of individuals/data subjects affected by the processing	☐ current employees; ☐ former employees; ☐ trainees/interns; ☐ contractors; ☐ family members/relatives (usually relevant in the context of pension/benefits); ☐ job applicants; ☐ customers; ☐ employees of vendors; ☐ dealer employees; ☐ website visitors/prospective customers/leads; ☐ Other (please list):

Categories of Personal Information that will be processed by Supplier	☐ Identifiers, characteristics and other information you provide (for example - personal identification data including contact information, authentication information you create, account information, billing data, photographs and other user-generated content); ☐ Commercial information regarding vehicle purchase, lease and service, as well as other purchasing and consuming histories or tendencies. ☐ Commercial and electronic activity information, such as vehicle data transmitted from your vehicle, including general status data, service history, vehicle performance data, information that you provide when using connected services and driver behavior data ☐ Electronic activity, such as data gathered by technology when you visit our websites or use mobile applications ☐ Audio, electronic, visual, thermal, olfactory or similar information, such as call recording for emergency and customer service and voice command data ☐ Geolocation data ☐ Inferences ☐ Sensitive Personal Data ☐ Professional or employment-related information, including educational information, career history, performance review ☐ Other (please list):
Categories of Sensitive Personal Information that will be processed by Supplier	☐ Social security number, passport number, driver's license or state ID data; ☐ geolocation data ☐ health data; ☐ racial or ethnic origin; ☐ trade union membership; ☐ membership of a professional or trade association; ☐ genetic or biometric data, including biometric templates; ☐ criminal convictions and offences; ☐ Other (please list):
Frequency of the transfer	Continuous and for so long as VWGoA uses the Supplier's services, and for the termination and transition period thereafter, if any is set forth in the DPSA and/or the Agreement.
Nature of the Processing Purpose of the data transfer and further processing	The Processor shall collect, Process and use all Personal Information solely for the purpose of the processing as specified in the Agreement and accompanying ordering documents and according to documented instructions on behalf of the Controller.
Period for which the personal data will be retained or criteria used to determine that period	The retention period of the Personal Data is for the duration of the Service Agreement or as otherwise described therein
Subprocessor transfers – subject matter, nature, and duration of processing	Subprocessors shall Process Personal Information solely for the purpose of the processing as specified in the Agreement and accompanying ordering documents and according to documented instructions on behalf of the Controller and subject to obligations essentially equivalent to those described in this DPSA.

2. Signatures and Start Date

Signatures	The Parties agree that the EU SCCs and the UK International Transfer Addendum are incorporated by reference and that by executing the DPSA, each party is deemed to have executed the SCCs and the UK Transfer Addendum.
Start Date	As indicated in the Agreement and accompanying order forms.

3. EU SCCs and UK Transfer International Addendum Information

SCC Clause	GDPR	Swiss DPA	UK Data Protection Law
Clause 7 – Docking Clause	**Module Two** An entity that is not a party to these clauses may, with the agreement of the parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A		
Clause 9(a) – use of sub-processors	**Module Two** Clause 9(a) (General Written Authorisation) is selected, and will be enforced in accordance with Section 4.3 of this DPSA;		
Clause 11 (Redress)	**Module Two** Optional language in Clause 11 shall not apply.		
Clause 17 – Governing Law	**Module Two** These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.	**Module Two** These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.	**Module Two** These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales.
Clause 18 – Choice of Forum and Jurisdiction	**Module Two** (b) The parties agree that those shall be the courts of Germany	**Module Two** (b) The parties agree that those shall be the competent courts of Switzerland.	**Module Two** The parties agree that those shall be the courts of England and Wales.
Annex 1A – List of Parties	**Module Two** The name, address, and contact person's name, position, and contact details, and each party's role in processing personal data are provided in Section A above		

Annex 1B – Description of Transfer	**Module Two** This information can be found in Section B above. To the extent applicable, the descriptions of safeguards applied to the special categories of Personal Information can be found in Annex 3 to this DPSA.		
Clause 13 and Annex 1C – Competent Supervisory Authority	**Module Two** Identify the competent supervisory authority/ies in accordance with Clause 13: Germany	**Module Two** Identify the competent supervisory authority/ies in accordance with Clause 13: FDPIC	**Module Two** Identify the competent supervisory authority/ies in accordance with Clause 13: UK ICO
Annex II – Technical and Organizational Measures	**Module Two** The description of technical and organization measures designed to ensure the security of Personal Data is described more fully in Annex 3 to this DPSA.		
Annex II – Technical and Organizational Measures – Subprocessors	**Module Two** The description of technical and organization measures designed to ensure the security of Personal Data processed by Sub-processors is described more fully in Annex 3 to this DPSA.		
Annex III – List of Subprocessors	Module Two See Annex 2		
Ending the UK Transfer Addendum when the Approved Addendum changes	N/A		Module One and Two Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☒ Importer ☒ Exporter ☐ neither Party

ANNEX 2

Approved Subprocessors

Subprocessor's Name and Address	*Contact Person's Name, Title and Contact Details*	*Nature and Subject Matter of the Processing*	*Duration of the Processing*

ANNEX 3:

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Cybersecurity Introduction and Relevant Definitions

Supplier shall implement appropriate organizational, programmatic, and technical cybersecurity measures to ensure a level of cybersecurity appropriate to the risk in order to protect VWGoA data or systems relevant to VWGoA operations against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. At a minimum, the Supplier has implemented and shall maintain the cybersecurity measures as stated. It is the Supplier's responsibly to also ensure that its subcontractors or subprocessors (e.g., vendors, suppliers, partners), if approved, have similar measures implemented.

In the sections below, the following definitions apply:

"Cybersecurity" shall mean the act of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. This intrinsically includes Information Technology security (IT security) and Information Security.

"Supplier Systems" refers to Supplier systems that connect to VWGoA's systems, which are a part of the Supplier's services to VWGoA, which are critical to VWGoA's operations, or that process or store VWGoA data.

"Supplier product" refers to any product that contains software, hardware, or combination of hardware and software, which VWGoA procures from the Supplier.

Any questions regarding VWGoA's technical interpretation of this Annex 1 can be sent to cybersecurity@vw.com.

Cybersecurity Program and Cybersecurity Governance

Supplier must have a formal cybersecurity program, based on an industry recognized cybersecurity framework, in place to support the protection of Supplier Systems and any connection to VWGoA Systems, VWGoA data, and services provided to VWGoA. A single accountable individual must be assigned to lead and manage this program. The program must include program level risk management to aggregate system/asset risks and programmatic risks in order to understand, document, mitigate, and manage the Supplier's complete risk profile.

Supplier must maintain documented cybersecurity policies, standards, and processes, including but not limited to the topics listed in this Annex 1. These documents are made available by Supplier to its employees via the corporate intranet or similarly accessible platform and are reviewed and updated at least annually.

Supplier must distribute cybersecurity and privacy awareness and training to all relevant employees based on their role. It is the Supplier's responsibility to ensure that employees complete assigned training.

An asset inventory of Supplier Systems must exist and include at least the following information: patch level, operating system, software and hardware bills of material, Supplier business owner, and Supplier technical owner.

Internal and external audits and/or assessments must be performed to review the program's effectiveness. Issues identified must be documented, tracked, and remediated as appropriate.

Business Continuity and Disaster Recovery

A Business Continuity (BC) plan and Disaster Recovery (DR) plan both must be in place in order to ensure the Supplier's resilience following an event (e.g., natural disaster, cyber-attack). The BC/DR plans must:

- Include the identification and documentation of critical systems and components relevant to VWGoA
- Be reviewed, tested, and updated at least yearly
- Contain notification procedures to alert customers, including VWGoA, of relevant issues related to Supplier Systems

As a part of the BC/DR plans, back-ups of Supplier Systems relevant to VWGoA must be:

- Fully backed-up on a weekly basis
- Stored encrypted using encryption following industry best practices
- Copied to offline storage facilities
- Be immutable (i.e., unable to be changed once backed-up)

Infrastructure and Network Cybersecurity

There must be policies, procedures, and mechanisms in place for Supplier Systems and associated infrastructure that cover antivirus and malware protection, intrusion detection and prevention systems, network and application firewalls configured to deny all access except authorized documented business services, data loss prevention tooling, and multi factor authentication (e.g., NIST 800-63B AAL2).

Identity & Access Management

There must be documented identity and access management processes and mechanisms in place to manage employee access to Supplier Systems. Access to Supplier Systems must be: allocated to users/groups based on the principal of "least privilege" and restricted to employees whom have a business, removed when a user no longer needs access to perform their role or is removed from the Supplier's organization, logged and tracked for accountability, and revalidated at least annually or quarterly for privileged accounts.

Remote access policies and mechanism for secure remote access must exist and be enforced. Two-factor authentication (2FA) is required for remote access and privileged account access.

User accounts and credentials must be unique and users must be prohibited from sharing their user account and credential information with others. Password policies for Supplier Systems must include industry best practices (e.g., NIST 800-63B Appendix A) such as minimum password lengths and user password changes at defined intervals.

If applicable, Supplier guarantees that their connection to any VWGoA Systems including any automation (e.g., scripts) to pull VWGoA data, as a part of the agreement, will be severed immediately upon contract cancelation or completion.

VWGoA Data Protection and Usage on Supplier Systems

Supplier must have a documented information classification (e.g. public, internal, confidential, secret) scheme must be in place to ensure proper classification, protection, use, and destruction of VWGoA data. Supplier must view all data on any system outside of the VWGoA environment, including on Supplier Systems, that contains Volkswagen specific information as private and confidential.

Supplier must handle VWGoA data in a secure manner taking every reasonable precaution to prevent the data from being shared, manipulated or stolen. Non-public VWGoA data must be encrypted during transmission and storage on all devices including but not limited to servers, mobile devices, handhelds, laptops, workstations, and removable media following industry best practices for encryption (e.g., FIPS 140-2). VWGoA data cannot be stored on or shared using unsecured systems or removable media, including in Software as a Service (SaaS) or Platform as a Service (PaaS) solutions being provided to VWGoA. All transfers of VWGoA data are mandated to occur using secured means approved by VWGoA.

Supplier shall not make copies of VWGoA data on Supplier Systems unless required to fulfill the agreement. VWGoA prohibits posting or disseminating VWGoA data outside of VWGoA or the Supplier, including, without limitation, or on the Internet, unless otherwise agreed upon in the agreement

Supplier agrees that all VWGoA data available to Supplier remains the sole and absolute property of VWGoA.

Supplier must guarantee immediately upon the completion or cancelation of the contract all VWGoA data in the Supplier's possession will be returned to VWGoA and then deleted. VWGoA data must be purged or destroyed using a documented process that follows industry best practices (e.g., NIST 800-88). Logs must be made available upon request to VWGoA proving all VWGoA data has been transferred and/or deleted.

Customer and Personal Information

Supplier systems containing VWGoA data that includes Personal Information (PI) must be inventoried, including cybersecurity and privacy controls. For such systems, documentation must exist that shows the flow of Personal Information through systems and business processes.

Secure Development Lifecycle

Supplier Systems, including customization of third party platforms, must have been designed, developed, and implemented using a documented Secure Development Life-Cycle (SDLC) or other development lifecycle (e.g., System Development Lifecycle) that includes cybersecurity. The applicable lifecycle that such systems and applications have gone through must include at a minimum the following cybersecurity activities with applicable support documentation (e.g., procedures, templates, tooling): cybersecurity requirements and controls, cybersecurity risk assessments, technical cybersecurity testing, and third party (supplier) cybersecurity assessments. Prior to deployment, Supplier Systems must be reviewed to verify implementation of required requirements, controls, and configurations.

Supplier must harden their systems using industry best practices (e.g., Center for Internet Security (CSIS) OWASP, NIST) based on the system. Cybersecurity configurations of Supplier Systems must be documented and be made available to VWGoA upon request.

Supplier Systems applicable to the agreement must have a penetration test performed at least annually or when applicable changes to the Supplier Systems are made. Finding from the test must be documented and tracked. Findings higher than Supplier defined thresholds must be remediated and retested to verify remediation. A summarized test report will be provide to VWGoA as evidence upon request.

Monitoring and Vulnerability Management

Supplier is responsible for monitoring Supplier Systems including monitoring of network traffic, access requests, logs, threat intelligence, social media, coordinated disclosure mechanisms, event alerts, and vulnerability databases. Supplier must investigate event alerts appropriately. To support monitoring, sufficient logs must be generated for Supplier Systems. These logs must be tamper proof and be retained for a minimum of twelve (12) months.

Supplier Systems must have documented configuration management, patch management, vulnerability management, change management, and incident management processes, or be a part of a larger program or programs around these capabilities. These capabilities and associated processes must include the prompt application of security patches, service packs, and hot fixes.

In addition, Supplier Systems must have a vulnerability scanning performed at least monthly. Findings from these tests must be promptly remediated.

Incident Response Process

Third party must have a documented incident response (IR) process and dedicated team in place to assess, respond, contain and remediate, as appropriate) identified cybersecurity issues. Supplier will review and update the IR process and associated playbooks annually to reflect emerging risks and lessons learned from incidents.

Physical Security

A documented physical security function and/or program must exist with policies and procedures meant to physically protect VWGoA data where it is stored (e.g., physical documents, data centers, individual computers). Access to physical locations that have VWGoA data in any form, physical or digital, are restricted per the identity and access management criteria as stated in this agreement. The physical security program must include that employees wear identification badges, visitors are documented and escorted throughout facilities, physical protections are in place (e.g., fences, locked doors), and premises are monitored (e.g., video recording, review of access logs).

Product Cybersecurity (to the extent applicable)

Supplier must have a product cybersecurity program in place for products that VWGoA purchases. This program must govern the cybersecurity controls and protections for the full lifecycle of the product that includes conception, design, development, manufacturing, production, maintenance, and end of support/end of life.

Supplier products must be designed, developed and implemented using a documented Secure Development Life-Cycle (SDLC) or other development lifecycle (e.g., System Development Lifecycle) that includes cybersecurity. The applicable lifecycle that such systems and applications have gone through must include at a minimum the following cybersecurity activities with applicable support documentation (e.g., procedures, templates, tooling): cybersecurity requirements and controls, cybersecurity risk assessments, technical cybersecurity testing, and third party (supplier) cybersecurity assessments. Prior to being sold or shipped to VWGoA, Supplier must review their products to verify implementation of required requirements, controls, and configurations.

Supplier must harden their products using industry best practices (e.g., Center for Internet Security (CSIS) OWASP, NIST) based on the product.

Supplier products that are being purchased applicable to the agreement must have a penetration test performed prior to purchase or prior to major updates being released. Finding from the test must be documented and tracked. Findings higher than Supplierdefined thresholds must be remediated and retested to verify remediation prior to being sold to VWGoA. A summarized test report will be provide to VWGoA as evidence upon request.

A product cybersecurity bill of materials must be provided to VWGoA upon purchase of a product and include at least the following: software and/or hardware components, patch levels, sources of the components (e.g., open source, off the shelf, customer build by a third party). Open source software must be documented and disclosed to VWGoA prior to purchase.

Product vulnerabilities and incidents that affect products VWGoA purchases must be reported to VWGoA in a timely manner to the same email in the "Incident Response" section of this agreement.

Supplier must have a coordinated vulnerability disclosure program to allow submission of product cybersecurity vulnerabilities and incidents, include those products which VWGoA purchases.

Access to VWGoA Systems and/or Infrastructure (to the extent applicable)

To the extent applicable:

Supplier must execute VWGoA's Third Party Usage Agreement, and employees seeking access to VWGoA systems must sign VWGoA's Authorized Vendor Employee Acknowledgement form to access the VWGoA internal systems and/or gain privileged account access (e.g. system administrator access).

Changes

VWGoA may change the above cybersecurity requirements by providing new requirements in writing to the Supplier. Supplier shall comply with such new cybersecurity requirements within thirty (30) days after receipt of notice. In the event Third Parties compliance with the new requirements materially increases Third Parties cost to provide services under the Service Agreement, Supplier shall notify VWGoA of the amount Supplier believes is necessary to reimburse Supplier for its actual and reasonable additional costs and the Parties will negotiate in good faith to determine if reimbursement to Supplier for such increased costs are warranted. If the Parties cannot reach agreement, either Party may terminate the Agreement by providing thirty (30) days' written notice to the other.