Data Protection Agreement (to be used when a VGC entity makes available personal data to a domestic non-affiliate entity)

Data Protection Agreement

1. Preamble

(a) This Data Protection Agreement (this "**Agreement**"), dated as of [24 Feb, 2022] (the "**Effective Date**") is entered into in Beijing by and between:

[Volkswagen Group Import Co., Ltd.], duly registered and validly existing under the laws of the PRC, with its domicile at [Room 316, Kaili Building, No.188, Tianbao Avenue, Tianjin Pilot Free Trade Zone (Tianjin Port Free Trade Zone)], PRC ("**Data Provider**");

and

[EventPlus Marketing Services Co., Ltd.], duly registered and validly existing under the laws of the PRC, with its domicile at [C106A, Shangba Design+ AD Park, Sihui Bridge, Chaoyang District, Beijing], PRC ("**Data Receiver**").

Data Provider and Data Receiver collectively referred to as the "**Parties**", individually a "**Party**".

(b) This Agreement applies to all activities in connection with the Processing by the Data Receiver (including the Data Receiver Staff or its subcontractors (if any)) of the Personal Data made available to it by the Data Provider. Personal Data made available to the Data Receiver by the Data Provider includes, if any, Personal Data collected or received by the Data Receiver on behalf of the Data Provider. The description of the respective project/matter for and in relation to which the Personal Data is made available and Processed, the purpose of the Processing, type of Personal Data as well as the categories of the Data Subjects shall be stipulated in writing in the Appendix to this Agreement.

(c) Each party must appoint and notify in writing to the other party an individual who is authorized to respond to any enquiries concerning the Processing of the Personal Data. The detailed information of each Party's contact person is specified in the Appendix.

2. Definitions

For the purpose of this Agreement:

"**Adequate Safeguards**" means measures that afford the highest standard of protection in respect of Processing of Personal Data by the

Data Receiver, such measures being any measures required to ensure compliance with Data Protection Laws and Regulations, guidance that may be issued by relevant government body in the PRC relating to Processing of Personal Data, and any additional measures as notified to the Data Receiver by the Data Provider from time to time.

"**Data Protection Laws and Regulations**" mean all applicable laws, regulations and national standards with respect to the protection and Processing of Personal Data. "**Data Protection Law or Regulation**" shall be construed accordingly.

"**Data Provider**" means the entity mentioned in the Preamble which, for business needs, transfers, shares or otherwise makes available Personal Data (either directly or indirectly) to the Data Receiver in accordance with this Agreement as well as Data Protection Laws and Regulations.

"**Data Receiver**" means the PRC-located individual or entity mentioned in the Preamble which agrees to Process, in accordance with this Agreement and Data Protection Laws and Regulations, the Personal Data made available by the Data Provider.

"**Data Subject**" means an identified or identifiable natural person to whom Personal Data relate.

"**Personal Data**" **or "Personal Information"** means any and all information that can be used separately or in combination with other information to identify a natural person or reflect the activities of an identified or identifiable natural person. Personal Information includes (but not limited to) names, dates of birth, addresses, contact information, identification numbers, biometric information, records and content of communications, accounts and the passwords, property information, credit reference information, whereabouts and tracks, hotel accommodation information, information concerning health and physiology, information on transactions, online identifier and other relevant information.

"**PRC**" means the People's Republic of China (excluding Hong Kong, Macau and Taiwan for the purpose of this Agreement).

"**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 acquisition, adaptation, alignment, alteration, blocking, collection, combination, comparison, consultation,

deletion, destruction, disclosure, dissemination, erasure, filing, inputting, linking, making available, marking, mining, modification, organisation, provision, recording, restriction, retrieval, sharing, storage, structuring, transfer, transmission, use, etc. "**Process**", **Processes**" and "**Processed**" shall be construed accordingly.

"Sensitive Personal Data/Information" means Personal Information that, once leaked, disclosed, or abused, may lead to personal injury, property damage, reputational damage, harm to physical or mental health, or discriminative treatment of an individual, including, without limitation, (a) property information, such as payment card numbers, verification information, savings information, and real property information; (b) health information, such as medicine and food allergy information, reproductive information, medical history, medical treatment, family medical history, and clinical data; (c) biometric information, such as fingerprints, iris scan, DNA profile, and facial recognition information; (d) identification information, such as identity card number and passport number; and (e) other information, such as precise geolocation information, sexual orientation, marriage history, religious or philosophical beliefs, phone records and unpublished criminal records.

3. Obligations of the Data Receiver

3.1. Compliance with Data Protection Laws and Regulations.
The Data Receiver must comply with all the Data Protection Laws and Regulations applicable to the Processing of the Personal Data by the Data Receiver under this Agreement. The Data Receiver shall not by any act or omission put the Data Provider in breach of any of the Data Protection Laws and Regulations.

3.2. Compliance with instructions of the Data Provider
The Data Provider has the right to issue instructions to the Data Receiver. These instructions concern the extent, the nature and the procedure for Processing of Personal Data with respect to the project/matter specified in the Appendix. The individual at the Data Provider who is authorised to issue instructions and the recipient of the instructions at the Data Receiver are listed in the Appendix. Such instructions, any change, cancelation or supplement of/to the instructions shall be made in written form. The Data Receiver shall Process the Personal Data solely within the scope of the instructions issued by the Data Provider, unless required to deviate by any Data Protection Law or Regulation to which the Data Receiver is subject; in such a case, the Data Receiver shall inform the Data Provider of these legal requirements prior to Processing, unless that law prohibits such information on important grounds of public interest.

3.3. The Data Receiver shall inform the Data Provider without undue delay if an instruction issued by the Data Provider violates any Data Protection Laws and Regulations in the Data Receiver's opinion. The Data Receiver shall justify its opinion to an extent that allows the Data Provider to review and understand the Data Receiver's opinion. In such a case, the Data Receiver is authorized to suspend execution of the instruction, after timely prior notification, until the Data Provider has changed the instruction or the parties, in accordance with their respective escalation procedures, have mutually agreed that there is no violation of Data Protection Laws and Regulations.

3.4. Data Processing
The Data Receiver shall in any event set up and observe, and ensure that its sub-contractors carrying out any data Processing on behalf of the Data Receiver set up and observe, Adequate Safeguards to carry out any data Processing. Each act or omission of the Data Receiver's sub-contractors in relation to the obligations set forth in the Adequate Safeguards shall be deemed to be an act or omission of the Data Receiver for which the Data Receiver shall be responsible. The Data Receiver shall not carry out any data Processing before such Adequate Safeguards have been set up. The Data Receiver shall not Process any Personal Data made available by the Data Provider under this Agreement on private data Processing devices of the Data Receiver Staff. In the event that the Data Receiver or its sub-contractors does not comply with any part of this section, the Data Provider has the right to terminate the Agreement.

3.5. Purpose of Processing.
The Data Receiver acknowledges that it is in the Data Provider's sole and absolute discretion to determine the purposes of the Processing of Personal Data, such purpose being defined in the Appendix of the Agreement. The Data Receiver must carry out the Processing solely for the purposes agreed upon in the Agreement and that it must not otherwise Process any Personal Data at any time, especially not for its own purposes. It is not permitted to anonymize and further Process the Personal Data under this Agreement without a written instruction from the Data Provider.

3.6. NO CROSS-BORDER TRANSFER: THE PROCESSING OF PERSONAL DATA UNDER THIS AGREEMENT SHALL EXCLUSIVELY TAKE PLACE WITHIN THE TERRITORY OF PRC. WITHOUT THE PRIOR WRITTEN CONSENT OF THE DATA PROVIDER, THE DATA RECEIVER MUST NOT ACCESS OR PROVIDE ACCESS TO

PERSONAL DATA OUTSIDE PRC OR PROVIDE OR ALLOW THE PROVISION OF ANY PERSONAL DATA FROM PRC TO ANY OTHER COUNTRY OR AREA. IN THE EVENT THAT THE DATA RECEIVER DOES NOT COMPLY WITH ANY PART OF THIS SECTION, THE DATA PROVIDER HAS THE RIGHT TO TERMINATE THE AGREEMENT.

3.7. Data Receiver's staff and other persons acting under Data Receiver's supervision

The Data Receiver shall undertake all reasonable actions to ensure its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process, the Personal Data ("**The Data Receiver Staff**") are fully skilled, competent, experienced and reliable. The Data Provider may instruct the Data Receiver to remove any staff that the Data Provider reasonably believes may breach or have breached any Data Receiver obligation detailed in this Agreement and the Data Receiver shall comply immediately with any such instruction. The Data Receiver shall ensure that:

(i) It has conducted appropriate vetting on the Data Receiver Staff, including carrying out check on their identity, criminal record, credit and right to work.

(ii) any person it authorizes to access or Process the Personal Data is bound by contract or otherwise to respect the confidentiality and security of the Personal Data; and

(iii) any person acting under the authority of the Data Receiver is made aware of and complies with the Data Receiver's obligations under this Agreement and that the Data Receiver has the right to impose effective sanctions on any such person in case of non-compliance.

The Data Receiver shall provide regular (but no less frequent than annual) training on the Data Protection Laws and Regulations requirements to its staff. Such training must include but not be limited to the specific processes and procedures to satisfy requirements of the Data Receiver under this Agreement. Upon request, the Data Receiver agrees to provide details of the training program to the Data Provider for review and approval.

3.8. The Data Receiver shall support the Data Provider in relation to safeguarding the rights and fulfilling the requests of the Data Subjects, in particular in relation to the rectification, erasure and restriction of the Processing of Personal Data as well as in relation to the provision of information and data for Data Subjects, particular by means of

appropriate technical and organizational measures set forth in Article 5, and acting in accordance with the instructions of the Data Provider.

3.9. Information requests from Data Subjects and authorities
The Data Receiver shall promptly notify the Data Provider of any queries from a Data Subject, regulator or any other authority in relation to the Processing of any Personal Data under this Agreement and coordinate all further steps with the Data Provider. The Data Receiver may only issue information to the Data Subjects after prior instruction from the Data Provider, except that the Data Receiver is legally obliged to provide any such information to the Data Subjects.

3.10. Confidentiality / Non-Disclosure

(i) General rule: As a matter of principle, the Data Receiver must treat all non-public information obtained in connection with the Agreement confidentially in line with the applicable confidentiality obligations, which applies in particular to (1) all information concerning customers of the Data Provider, including knowledge of whether or not someone is a customer of the Data Provider, (2) any Personal Data of a person be it a customer or any other person such as an employee of the Data Provider (data protection / privacy) and (3) non-public information about the business of the Data Provider, such as its organization, operational and technical processes, infrastructure and systems (including hardware and software), products and services, information on employees and contractual relations with third parties (trade and business secrecy). The Data Receiver is obliged to preserve data secrecy and preserve confidentiality while Processing the Personal Data under this Agreement.

(ii) No transfer, sharing or disclosure of Personal Data: The Data Receiver must not transfer, share or disclose the Personal Data to any third party except: (i) with the written consent of the Data Provider; or (ii) when required by applicable mandatory PRC law, in which case the Data Receiver must, where permitted by such law, give the Data Provider written notice prior to such transfer, sharing or disclosure so that the Data Provider can determine if it wishes to challenge such transfer, sharing or disclosure. The Data Receiver has to take all reasonable measures to prevent the transfer, sharing or disclosure if such transfer, sharing or disclosure is not in compliance with applicable PRC law and to protect the Data Provider's rights and position.

3.11. Security of Processing

(i) The Data Receiver shall ensure and provide sufficient guaranties that appropriate technical and organisational measures set forth in Article 5 are implemented in such a manner that the Processing is conducted in accordance with the requirements of the Data Protection Laws and Regulations and industry best practices for companies that Process the types of Personal Information that will be Processed under this Agreement, including if applicable Sensitive Personal Information, and that the protection of rights of Data Subjects is guaranteed as well as configure the Data Receiver's internal operational organisation in such a manner that it satisfies the particular requirements of data protection. The Data Receiver shall especially ensure appropriate security of Processing, in particular confidentiality (including pseudonymisation and encryption), availability, integrity, and resilience of the systems and services used for the data Processing.

(ii) The technical and organizational measures can be adjusted during the course of the contractual relationship to adapt to further technical and organizational developments. Material changes shall be agreed in written form.

3.12. Obligation to notify.

(i) The Data Receiver shall inform the Data Provider without undue delay about any Processing of Personal Data outside of the scope of this Agreement as well as about any violations of any Data Protection Laws and Regulations or of the specifications stipulated in this Agreement, especially malfunctions, suspected breaches of data protection or other adverse effects or changes in the Processing of Personal Data by the Data Receiver or a sub-contractor or personnel of the Data Receiver or a sub-contractor.

(ii) If the Personal Data that is Processed pursuant to this Agreement should be threatened at the Data Receiver by means of a lien or seizure, by a bankruptcy proceeding or similar proceeding or by other events or measures on the part of third parties, then the Data Receiver shall immediately inform the Data Provider of this. The Data Receiver shall also immediately inform all relevant agencies in this context that the Data Provider is the owner of the data.

(iii) If audits are performed by the data protection supervisory authorities, the Data Receiver is obligated to disclose the result

to the Data Provider to the extent that such concerns the Processing of Personal Data pursuant to this Agreement. The deficiencies determined in the audit report shall be immediately corrected by the Data Receiver and the Data Provider shall be informed of such.

3.13. Data protection impact assessment
The Data Receiver shall support the Data Provider with carrying out the data protection impact assessment.

3.14. The Data Receiver shall provide the Data Provider with all information which is necessary for the records of Processing activities.

3.15. Copies of Personal Data.
The Data Receiver must not and shall ensures the Data Receiver Staff not to copy, duplicate, download or store Personal Data or other documents relating to the Personal Data without the Data Provider's previous written consent, unless they are required in order to guarantee proper data Processing.

3.16. Ownership and retention rights.

(i) The Personal Data, any copies or reproductions made thereof remain the Data Provider's property. Any right of retention of the Data Receiver in relation to the Personal Data without the express written consent of the Data Provider is excluded.

(ii) Documents, Personal Data and data carriers that have been made available (either directly or indirectly) by the Data Provider as well as all data, which the Data Receiver Processes on behalf of the Data Provider in accordance with this Agreement, all documents in the possession of the Data Receiver or the Data Receiver’s sub-contractors, which contain data made available by the Data Provider, results of the data Processing, databases that contain data made available by the Data Provider, as well as all copies, shall be generally either erased or destroyed or returned by the Data Receiver, at the Data Provider’s option, if the Data Receiver does not have an obligation for retention of the Personal Data pursuant to applicable mandatory PRC laws and regulations. If there exists an obligation for further retention of the data, the Data Receiver shall restrict the Processing of the Personal Data and only use the data for the purposes, for which the obligation for retention exists. The obligations regarding confidentiality and security of Processing shall continue to be in force for the time

period of the retention. The Data Receiver shall immediately erase the data as soon as the obligation for retention expires. The Data Provider may also request prior erasure or surrender at any time. Upon request by the Data Provider, the Data Receiver must confirm in writing that it has complied with the obligations of this sub-section.

3.17. The Data Receiver shall ensure that the Personal Data Processed pursuant to this Agreement is Processed separately from the data of other partners/clients of the Data Receiver. Data collected for different purpose shall be Processed separately. This requires separation at all times (physical or logical) and mutual isolation of the data sets Processed for the respective Processing purposes and clients.

3.18. If not otherwise expressly specified, the Data Receiver shall bear all costs incurred by the Data Receiver due to compliance with and realization of its obligations pursuant to this Agreement.

4. Sub-contractors

4.1. The Data Receiver may use a sub-contractor to carry out the Processing only with prior written consent from the Data Provider. The sub-contractors which have been agreed by the Data Provider are listed in the Appendix.

4.2. The Data Receiver must ensure that each sub-contractor: (i) prior to carrying out any Processing of any Personal Data under this Agreement has entered into a written contract with the Data Receiver which includes terms equivalent to those in this Agreement; and (ii) does not Process any Personal Data in contravention of this Agreement and the Data Protection Laws or Regulations or other applicable laws.

Where the sub-contractor fails to fulfill its data protection obligations under such contract, the Data Receiver shall remain fully liable to the Data Provider for the non-compliance of that sub-contractor with their data protection obligations.

5. Technical and organisational security measures

5.1. The Data Receiver must implement adequate technical and organizational security measures to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar incidents when Processing any Personal Data as provided in the Agreement. The Data Receiver must upon request from the Data

Provider provide evidence of the implementation of such measures for review and approval of the Data Provider.

5.2. The Data Provider may require additional measures if it believes that such additional measures are required under the applicable Data Protection Law or Regulation.

5.3. If the Data Receiver's technical and organizational measures have been compromised which might led to a failure to fulfill its obligations described under this Agreement, then the Data Receiver shall, immediately inform the Data Provider and the Parties shall discuss and solve the problem as soon as possible; before such problem is solved, any Processing of the Personal Data by the Data Receiver must be suspended.

5.4. The Data Receiver warrants that it has in place and shall maintain at least the following technical and organizational security measures commensurate with the risks associated with the Processing of Personal Data:

(i) Premises Access Control: Unauthorized persons must be prevented from gaining physical access to premises, buildings or rooms, where data Processing systems are located which Process the Personal Data under this Agreement; persons are unauthorized if their activity does not correspond to tasks assigned to them (examples of measures: specifying authorized individuals; using badge readers; locking of rooms; video surveillance and alarm devices with reference to access areas); exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by the Data Receiver and do not get access to the Personal Data itself.

(ii) Remote access: Data Receiver's information systems shall be designed to prevent unauthorized access by remote means including via internet or otherwise.

(iii) Electronic Data Processing (EDP) System Access Control: Data Processing systems must be prevented from being accessed or used without authorization (examples of measures: assignment of user IDs for identification and user passwords for authentication; firewalls).

(iv) Data Access Control: Persons entitled to use a data Processing system must gain access only to the data to which they have right

and necessity of access in order to perform their duties, and that they are only able to access the Personal Data within the scope and to the extent covered by their respective access right. Personal Data must not be read, copied, modified or removed without authorization in the course of Processing or use and storage (examples of measures: restriction on access to files and programs based on a "need-to-know-basis"; prevention of use/installation of unauthorized hardware and/or software; storing data carriers in secured areas; establishing rules for the safe and permanent destruction of data carriers that are no longer required).

(v) Destruction of printed documents: the Data Receiver shall implement and maintain appropriate security measures and procedures to secure confidential disposal of all Personal Data generated in the performance of the project/matter stipulated in the Appendix by cross shredding with appropriate shred size. The destruction process shall be designed as closed cycle with a minimal manual interference or access possibilities to data carriers.

(vi) Data Transmission Control: Except as necessary for the performance of the project/matter specified in the Appendix and the obligations of the Data Receiver under the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transmission or storage and it must be possible to establish to whom Personal Data was transmitted to (examples of measures: instructions for online or offline transmissions; encryption of data or transportation of data carriers in sealed containers, shipping and delivery notes).

(vii) Data Entry Control: It must be possible retrospectively to examine and establish whether and by whom Personal Data have been entered into data Processing systems, accessed, modified, copied or removed (examples of measures: logging of administration and user activities).

(viii) Contractual Control: Personal Data must be Processed solely in accordance with the Agreement and related instructions of the Data Provider and this shall be reflected in the contract of the Data Receiver with its respective sub-contractors (if any) (examples of measures: written instructions or contracts; control of the contractual performance).

(ix) Availability Control: Personal Data must be protected against accidental destruction or loss (examples of measures: creating back-up copies stored in specially protected environments or building reliable redundancies; implementation of anti-virus software; creation of contingency plans or business recovery strategies in case of water damage, lightning strike, power failure, deficits of Data Receivers).

(x) Organizational Requirements: The internal organization of the Data Receiver must meet the specific requirements of data protection (examples of measures: designation of data protection officers; commitment of the employees to maintain confidentiality; training of staff on data privacy and data security; realization of IT security concepts; notifications / authorizations regarding data protection authorities, as far as applicable). In particular, to avoid accidental mixing of Personal Data, the Data Receiver separates other data than that belonging to the Data Provider by technical and organizational measures from the Data Provider's data (examples of measures: physical or logical separation of data).

6. Right to audit and monitor

6.1. Upon request from the Data Provider, for the purposes of audit or certification, or upon request from the Data Provider's regulator in relation to the supervision of the Data Provider, the Data Receiver must provide relevant information on its data Processing facilities, procedures, technical and organization measures, and personnel who work on the project/matter specified in the Appendix and the Data Receiver's obligations under this Agreement.

6.2. Data Receiver shall promptly provide the Data Provider with a copy of any operational audit reports which have been completed by any independent bodies. Without prejudice to any clauses in the Agreement dealing with the right to audit and monitor, the Data Provider shall be entitled (together with its external auditors or any regulatory authority), in consultation with the Data Receiver and observing a reasonable notice period, to inspect any aspect of Data Receiver's security measures and procedures and to conduct its own security tests (including penetration tests) with respect to the Personal Data. Data Receiver shall co-operate fully with any such inspections and tests and shall implement any resulting recommendations within an agreed timeframe thereafter. Where in the Data Provider's reasonable opinion, it is necessary to have the Data Provider staff be present on Data Receiver premises, Data Receiver agrees to accommodate the presence of any the Data Provider staff.

6.3. The Data Provider shall in particular be entitled, in consultation with the Data Receiver and observing a reasonable notice period, to audit and inspect the Data Receiver's working premises during normal business hours and without creating a business interruption, to satisfy itself that adequate measures are being taken to meet the technical and organizational requirements of the Data Protection Laws and Regulations. The Data Provider acknowledges that Data Receiver owes a duty to its other partners/clients to maintain information relating to them confidential. Should Data Receiver need to limit the Data Provider access rights as a result of Data Receiver's confidentiality obligations to its other partners/clients, Data Receiver agrees to use all reasonable endeavors to provide such alternative evidence as is necessary to allow the Data Provider to perform a satisfactory audit under this provision.

7. Term and Termination

7.1. This Agreement is concluded for an indefinite period of time and can be terminated by the Data Provider with a prior written notice of 3 months.

7.2. The Data Provider may terminate this Agreement at any time without adherence to a notice period if there has been a severe breach of the provisions of this Agreement on the part of the Data Receiver, the Data Receiver is not able to or is not willing to carry out an instruction from the Data Provider or the Data Receiver refuses to allow the Data Provider access in breach of this Agreement.

8. Liability

Without prejudice to any other rights or remedies available to the Data Provider, its affiliates and their respective employees, agents, contractors, officers and directors under PRC laws or in relation to this Agreement, the Data Receiver shall indemnify, defend and hold harmless the Data Provider, its affiliates and their respective employees, agents, contractors, officers and directors from and against all losses, expenses, liabilities, claims, damages and costs they may incur or suffer as a result of or in relation to any breaches by the Data Receiver, including legal fees or loss of profits or revenues, and/or any claims or allegations made by a Data Subject or a government authority over the Processing of Personal Data.

9. General Provisions

9.1. Changes to Agreement. Changes, supplements and amendments to this Agreement and any part thereof require written agreement of the Parties.

9.2. Governing Law. The execution, interpretation and performance of this Agreement and any dispute arising from or in relation to this Agreement shall be governed by PRC laws.

9.3. Disputes. The Parties shall settle all dispute arising from the interpretation, performance, dissolution or termination of this Agreement or in connection of this Agreement through friendly consultation. In case no agreement can be reached to resolve the dispute, the Parties agree that each Party shall have the right to submit all disputes arising from or in relation to this Agreement to China International Economic and Trade Arbitration Commission ("CIETAC") for arbitration in Beijing in accordance with the arbitration rules of CIETAC in effect at the time of the application for arbitration. The language of the arbitration shall be English. Any arbitration award will be final and binding upon the Parties. In the course of dispute resolution, this Agreement shall be continuously valid and binding upon both Parties except for the part under arbitration.

9.4. Severability. If any provision of this Agreement is found to be invalid or unenforceable, the invalidity of such provision shall not affect the other provisions of this Agreement, and all provisions not affected by such invalidity shall remain in full force and effect.

9.5. Appendix. The Appendix of this Agreement shall be regarded as integral parts of this Agreement.

9.6. Originals.

[For DPA as an appendix of Purchasing Agreement] This Agreement shall be executed in Three (3) originals, two for Data Provider, one for Data Receiver. Each of the originals shall have same legal effect.

The rest of this page is intentionally left open.

(Signature Page)

Volkswagen Group Import Co., Ltd.
(Company Seal)

Signed By: _____ _____

Names: Zhang, Haozhi Shen, Xiaojie

Titles: Managing Director Group Managing Director
VW Import Passenger Cars &
Commercial Vehicle

EventPlus Marketing Services Co., Ltd.
(Company Seal)

Signed By: _____

Name: _____

Title: _____

Appendix to the Data Protection Agreement

1. Description of the Project/Matter and Data Processing

1.1. The project/matter:
(Description of the project/matter for and in relation to which the Personal Data is made available by the Data Provider to the Data Receiver for Processing)

2022 VW Import annual dealer conference
……

1.2. Purpose of the Processing:

To design and execute the 2022 VW Import annual dealer conference, incl. program design, RSVP, hotel booking, meal and logistics arrangement, etc.
……

1.3. Types of data:

	Data categories	**List of specific data used**	**Example for data**
☒	Job-related contact and (work) organization data		Surname, given name, sex, address, email-address, phone number, mobile phone number, company, area, department, cost center, personnel number, responsibilities, functions, presence (yes/no), etc.
☐	IT usage data		User ID, roles, rights, log-in-times, computer name, IP address, GID, Legic-no. etc.
☐	Special category: picture of the employee		Portrait photo voluntarily published by the employee (intranet, telephone book, social media platform etc.)

☒	Private contact and identification data		Surname, given name, sex, address, email address, phone number, mobile phone number, date/place of birth, identification numbers, nationality etc.
☐	Contract data		Purchased products, (financial) services, date of contract, purchase price, extras, warranties, etc.
☐	Vehicle usage data with VIN / license plate number. *Guarantee, warranty, product liability, safe vehicle operation*		Vehicle usage data associated with VIN/license plates and associated with workshop repairs, guarantee and, warranties or product liability, or whose availability is required for safe operation of the vehicle.
☐	Vehicle usage data with VIN / license plate number Comfort settings, multimedia, navigation		Vehicle usage data associated with VIN / license plates and related comfort settings, such as seat adjustment, preferred radio stations, climate settings, navigation data, email / SMS contact information etc.
☐	Vehicle usage data with VIN / license plate number *driving behavior, assistance systems*		Vehicle usage data associated with VIN / License plates and related to driving behavior or the use of assistance systems and their specific operational data, etc.

☐	Position data		GPS, radio circuit positioning, movement profile, WLAN hotspot positioning etc.
☒	Data regarding personal / professional circumstances & characteristics		Data of spouse or children, marital status, portrait photo, honorary post, job title, career, period of employment, tasks, activities, log-file analyses, entry and exit data, qualifications, measurements / assessments, etc.
☐	Payment and time management data		Wage group, payroll accounting, special payments, garnishment, daily attendance times, absence reasons, etc.
☐	Data of reliability and finance		Payment behavior, balance sheets, data of commercial agency, scorings, financial circumstances, bank account, credit card number, etc.
☒	Sensitive Personal Data		Personal identity information: Personal ID number, passport number, driver license, social security number, etc. Personal property information: Bank account number, credit information, real estate, virtual assets, transaction information, etc.

			Personal healthy and physiology information: Data concerning health, disease of a person, medical records, etc. Biometric data: Biometric data for the purpose of uniquely identifying a natural person data, e.g. genetic data, fingerprints, iris information, etc. Others: Personal information of minors under 14 years old, communication records and content, record of whereabouts, accommodation information, marriage history, racial and ethnic origin, political opinions, religious or philosophical convictions, data concerning a natural person's sex life or sexual orientation, undisclosed criminal record, browsing history of websites, accurate location information, etc.
☐	Crimes / Offenses		Data relating to criminal offences or the suspicion of criminal offences
☐	Other		

1.4. Categories of Data Subjects:

	Data Subject	Description	Examples
☒	Employees	Employees of the Group Company (in terms of the responsible unit)	e.g. jobholder, trainee, applicant, former employees
☒	Group Employees	Employee of another Group Company (in terms of a member of the Volkswagen Group, but not of the responsible unit)	e.g. from Volkswagen AG point of view: Employees of AUDI, FSAG, PORSCHE etc
☐	Partner Companies Employees	Employees of a supplier, service provider, Joint-Venture, temporary employment agency	e.g. employees of IT service providers, suppliers, employees of Joint-Ventures, temporary workers
☐	Customers	Each person that has a business relationship (with the respective responsible unit)	e.g. purchasers of cars, Bank customers, policyholders, renters
☒	Other Business Partners	Each (natural or legal) person that has a business relationship (with the respective responsible unit), except customers)	e.g. suppliers, importers, or service partners themselves; intermediator, shareholders, freelancers, etc.
☐	Outsiders	Each person that has no business relationship with the respective Group Company (responsible unit)	e.g.visitors, guests, interested persons
☐	Children	Persons under 16 years of age	

1.5. Reference to the service agreement / main agreement between the parties (if any)

……
(Agreement name, number, date)

2. Individuals authorized to provide instructions

2.1. The individuals at the Data Provider who are authorized to provide instructions are:

Feng, Congmiao, Dealer Network Dept. VW Import, VGIC.
Congmiao.feng@volkswagen.com.cn
……
(Name, organisational unit, function, telephone number, e-mail)

2.2. The individuals who are authorized to receive instructions at the Data Receiver are:

Gao, Yang, EventPlus Marketing Services Co., Ltd., Deputy General Manager, romygao@eventplus.cn
……
(Name, organisational unit, function, telephone number, e-mail)

If there is a change in or the long-term incapacitation of the contact person, the contractual partner shall be informed of the successor or the substitute in writing.

3. Sub-contractors

☒ There will be no sub-contractors engaged.

☐ The Data Receiver engages the following sub-contractors:

No.	Sub-contractors (name, address, contact)	Data categories Processed	Description of the services / data Processing activities / purpose of the sub-contracting	Place of data Processing