DATA PROCESSING ADDENDUM

1) Definitions
   a) **"Applicable Data Protection Laws"** means, to the extent applicable Vendor's provision of the Services to Customer: (i) all federal, state, provincial and local laws, rules, regulations, directives, and government requirements and guidance currently in effect and as they become effective relating to privacy, confidentiality, security, consumer protection, or breach notification that are applicable to Personal Data, including but not limited to the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020) and equivalent state privacy laws, and all other Applicable Data Protection Laws and regulations related to Personal Data.
   b) "**Breach**" means an unauthorized acquisition of Customer Data, including any "breach" of Personal Data (as the term "breach" and similar terms are defined under Applicable Data Protection Laws).
   c) "**Controller**" means the entity that determines the purposes and means of Processing Personal Data. Controller shall include the terms "Controller" and "Business" as defined under Applicable Data Protection Laws. For purposes of this DPA, Customer is the Controller.
   d) "**Customer Data**" means all Personal Data Processed by Continental on behalf of Customer to provide the Services under the Agreement.
   e) "**Processor**" means the entity that Processes Personal Data on behalf of the Controller. Processor shall include the terms "Processor" and "Service Provider" as defined under Applicable Data Protection Laws. For purposes of this DPA, Continental is a Processor.

The following terms have the definitions provided under Applicable Data Protection Laws: **Sell**, **Share**, and **Consumer**. Any other terms that are not defined herein shall have the meaning provided under the Agreement or Applicable Data Protection Laws.

2) Data Use and Disclosure
   a) Continental is acting solely as a Processor to Customer. Continental may Process Personal Data only within the framework of the Agreement and this DPA, and in accordance with the instructions of Customer. Additional details are set forth in **Annex I**.
   b) Except as otherwise stated herein, Continental is permitted to use and disclose Customer Data solely for purposes of performing the Services and for no other purpose.
      i) Without limiting the generality of the foregoing, Continental is prohibited from:
         (1) Selling or Sharing Customer Data;
         (2) retaining, using, or disclosing Customer Data for any purpose other than for the specific purpose of providing the Services under the Agreement;
         (3) retaining, using, or disclosing Customer Data outside of the direct business relationship between Customer and Continental; and
         (4) combining Customer Data with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a Consumer, except where permitted by Applicable Data Protection Laws.
      ii) Continental hereby certifies that it understands the restrictions set forth in this Section and will comply with them.
   c) Continental's may use subcontractors, agents, and third-party processors to Process Customer Data and support in the provision of the Services under the Agreement (collectively, "Subprocessors") at its sole discretion. Customer hereby grants Continental general authorization to subcontract the provision of services and Processing of Customer Data to a Subprocessor in accordance with the terms of the Service Agreement and this DPA, provided that (i) to the extent required by Applicable Data Protection Laws, Continental provides Customer a reasonable opportunity to object to the engagement of any new Subprocessor on reasonable grounds related to data protection and (ii) such Subprocessors agree in writing to be bound by terms and conditions substantially similar to those that apply to Continental through this DPA. In the event that Customer objects to the engagement of a new Subprocessor, at Continental's discretion either (a) Continental shall provide the Services without the use of the Subprocessor to whom Customer has objected, or (b) Continental and Customer shall negotiate in good faith a solution to Customer's objection. Continental's list of Subprocessors is set forth in **Annex 3** as updated from time-to-time subject to this Section 2(c).
   d) Additional Continental Obligations
      i) Continental has implemented and will maintain appropriate technical and organizational security measures ("**TOMS**"), as set forth in **Annex 2**. Continental may change the TOMS at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data. Continental will use commercially reasonable efforts to notify Customer of any such changes.
      ii) Continental shall, in performing the Services, secure Customer Data, including by: (i) complying with Applicable Data Protection Laws; (ii) providing the same level of privacy protection as is required by Applicable Data Protection Laws to Customer Data; and (iii) ensuring each person Processing Customer Data (including but not limited to employees, agents, and subcontractors) is subject to a duty of confidentiality with respect to such Customer Data;

iii) Continental shall notify Customer if it determines it can no longer meet its obligations under Applicable Data Protection Laws and allow Customer to take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Customer Data;

iv) To the extent required by Applicable Data Protection Laws, Continental shall allow and cooperate with reasonable assessments by Customer, its designated assessor, or Continental's qualified assessor of Continental's policies and technical and organizational measures in support of the obligations under Applicable Data Protection Laws using an appropriate and accepted control standard or framework and procedure for such assessment. Such assessment shall be conducted with at least thirty (30) days' advance written notice to Continental, no more than once during any twelve-month period, during normal business hours without unreasonable interference with Continental's operations, and on terms agreed to in writing by Customer and Continental in advance. Any reports or findings generated in connection with any such assessment shall be considered Continental's confidential information, and if the assessment is conducted by Customer's designated assessor, such assessor shall be subject to an appropriate duty of confidentiality with Continental. If Continental engages its own assessor, it shall provide a reasonable summary of the assessment to Customer if requested by Customer. Continental shall, if otherwise necessary under Applicable Data Protection Laws and upon the reasonable request of Customer, make available to Customer other information necessary to demonstrate compliance with its obligations under Applicable Data Protection Laws;

v) Continental shall reasonably assist Customer in meeting its obligations under Applicable Data Protection Laws. Such assistance shall include:
   (1) helping to fulfill Customer's obligation to respond to Consumer rights requests under Applicable Data Protection Laws (provided, however, that if an individual makes any such request to Continental, Continental shall direct such individual to Customer if reasonably practical and permitted by law and shall not otherwise respond to any such requests directly unless directed by Customer); and
   (2) providing necessary information to assist Customer in conducting and documenting data protection assessments and similar assessments, where required by Applicable Data Protection Laws.

3) Incident Response Obligations
   a) Continental shall report any Breach in writing to Customer without unreasonable delay, but in no event later than three (3) business days, after discovering a Breach. Continental shall cooperate with any reasonable Customer requests for information and any Customer investigation regarding such Breach.
   b) In the event that Continental experiences a Breach, Continental shall take steps to investigate, mitigate, and remediate the effects of the Breach and to prevent a similar Breach from occurring.
   c) To the maximum extent permitted by applicable law, Continental shall not be liable for any indirect, consequential, special, punitive or enhanced, exemplary, or incidental damages, or damages for loss of profits or revenues, goodwill, diminution in value, or anticipated revenues, arising from or in connection with a Breach, regardless of (a) whether such damages were reasonably foreseeable, (b) Continental was advised of the possibility of such damages, or (c) the legal or equitable theory upon which the claim is based.

4) Transfers Subject to EU Safeguards

Continental uses its affiliate Continental Reifen Deutschland GmbH, Vahrenwalder Str. 9, 30165 Hanover, Germany ("CRD") as a Subprocessor to provide the services to the Customer. CRD is and Processes Customer Data on behalf of Continental in the European Union ("EU"), and transfers such Customer Data outside of the EU back to Continental and Customer. To the extent these transfers are applicable subject to Continental's EU Binding Corporate Rules and the EU General Data Protection Regulation 2016/679, Continental, on behalf of and authorized by CRD, enters with Customer into Module Four: Transfer Processor to Controller, of EU Standard Contractual Clauses, as set out in the European Commission's Decision 2021/914 of 4 June 2021 (available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en), as amended by the European Commission from time to time ("SCCs") by reference. The SCCs shall apply as follows:

   a) Clause 7 (Optional – Docking Clause) shall not apply and shall be deemed excluded;
   b) for purposes of Clause 11 (Redress), the optional wording shall not be incorporated and shall not apply to the Parties;
   c) Clauses 14 and 15 shall not be incorporated, provided that Continental does not combine Personal Data received from Customer with other Personal Data it collected in the EU before transferring the Personal Data back to Customer;
   d) for purposes of Clause 17 (Governing law), the Parties agree that the SCCs shall be governed by the law as set forth in the Agreement;
   e) for purposes of Clause 18 (Choice of forum and jurisdiction), Parties agree that disputes arising from SCCs shall be resolved by the courts as set forth in the Agreement;
   f) Annexes I.A and I.B of the SCCs shall be deemed completed with the information set out in **Annex I** to this DPA, as appropriate.

ANNEX I: ADDITIONAL DETAILS REGARDING PROCESSING ACTIVITIES

Customer's instructions for Processing Personal Data are:

As set forth in the Agreement, including the DPA.

The nature and purpose of Continental's Processing is:

The subject matter of contract data processing emerges from the Agreement concluded between the Parties and its service description, if available.

The Type(s) and Categories of Personal Data subject to Processing by Continental is:

Categories of data subjects whose personal data is processed:

Customers, Customer employees and independent contractors, clients, Service Users, Communication participants, Suppliers and/or Service Providers (and individual contacts at these 3rd party vendors), Employees, Contact persons for businesses, Business partners, and Other data subjects specified by Customer (e.g., drivers, service personnel, fleet/workshop managers).

Categories of personal data processed

General data/ private contact details

☒ Names Personal profiles ☐ Image
☐ Private address data ☐ Date of birth
☐ ID card data (e.g. Passport, Social Security, Driving License)
☒ Other (please specify):

- **Vehicle Master data** (license plate, VIN, customer vehicle identification number, depot name);
- **Time and Location data** (GPS, location and temperature, route and road data, distance, timestamp);
- **Tire & Vehicle Dynamics Data** (telemetry data [e.g. speed, acceleration], tire related data [e.g. pressure, temperature, mileage, tread depth, yaw rate], working hours and downtime, power & fuel consumption, load, forces on the tires);
- **User & Usage Data** (User ID, login information, IP Address, usage behavior);
- **Contact Data** (Name, Customer, phone, e-mail)

Service and IT usage data

- ☒ Device identifiers ☒ Usage and connection data
- ☐ Image / video data ☒ Telecommunication data/ message content
- ☐ Audio / voice data ☒ Identification data
- ☒ Access data ☒ Authorization
- ☐ Meta data

Sensitive Personal Data and Special categories of Personal Data

☐ Race or Ethnic Origin ☐ Religious or Philosophical Beliefs
☐ Physical or Mental Health ☐ Political Opinions
☐ Biometric Data ☐ Genetic Data
☐ Trade Union Membership ☐ Sex Life/Sexual Orientation
☐ Criminal Offenses, Convictions or Judgments ☒ Specific Geolocation
☐ Other please specify: _____

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for

staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The Duration of Processing by Continental:

For the term of the Agreement and any termination/transition period thereafter, as set forth in the Agreement.

The Frequency of the transfer by Continental:

The transfer and Processing will occur continuously throughout the Term of the Agreement.

For the purposes of SCCs only:

Data Exporter(s)

Name (full legal name): **Continental Reifen Deutschland GmbH**
Address: Vahrenwalderstrasse 9, 30165 Hannover, Germany
Contact person's name, position/job title and contact details (including email): **TO BE UPDATED**
Activities relevant to the data transferred under these Clauses: As set forth in the Agreement
Role (controller/processor): Processor (as as Subprocessor of Continental)

Data Importer(s)

Name (full legal name): **Customer**, as set forth in the Agreement
Address: As set forth in the Agreement
Contact person's name, position/job title and contact details (including email): As set forth in the Agreement
Activities relevant to the data transferred under these Clauses: As set forth in the Agreement
Role (controller/processor): Controller

ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES

1. Physical Access Control

Safeguarding admission/access to processing systems with which processing is carried out against unauthorized parties (e.g. through physical property protection: fence, gatekeeper, personnel barrier, turnstile, door with card reader, camera surveillance, organizational property security, regulation on access authorizations, access registration)

The following technical and organizational measures have been implemented by the Continental for the Processing of Personal Data described in the Agreement:

☒	Alarm system
☒	Automatic access control system
☒	Locking system with code lock
☐	Biometric access barriers
☒	Light barriers/motion sensors
☒	Manual locking system including key regulation (key book, key issue)
☒	Visitor logging
☒	Careful selection of security staff
☒	Chip cards/transponder locking systems
☒	Video monitoring of access doors
☒	Safety locks
☒	Personnel screening by gatekeeper/reception
☒	Careful selection of cleaning staff
☒	Obligation to wear employee/guest ID cards
☐	Other:

2. Data Access Control/User Control

Prevention of third parties using automatic processing systems with equipment for data transmission (authentication with user and password).

The following technical and organizational measures have been implemented by the Continental for the Processing of Personal Data described in the Agreement:

☒	Authentication with user name/password (passwords assigned based on the valid password regulations)
☒	Usage of intrusion detection systems
☒	Usage of anti-virus software
☒	Usage of a software firewall
☒	Creation of user profiles

☒	Assignment of user profiles to IT systems
☒	Usage of VPN technology
☒	Encryption of mobile data storage media
☐	Encryption of data storage media in laptops
☐	Usage of central smartphone administration software (e.g. for the external erasure of data)
☐	Other:

3. Data Usage Control/Data Storage Media Control/Memory Control

Prevention of unauthorized reading, copying, changing or erasure of data storage media (data storage media control), prevention of unauthorized entry of personal data and unauthorized access to it, changing and deleting saved personal data (memory control). Ensuring that the parties authorized to use an automated processing system only have access to the personal data appropriate for their access authorization (e.g. through authorization concepts, passwords, regulations for leaving the company and for moving employees to other departments.) (data usage control).

The following technical and organizational measures have been implemented by the Continental for the Processing of Personal Data described in the Agreement:

☒	Roles and authorizations based on a *"need to know principle"*
☒	Number of administrators reduced to only the "essentials"
☒	Logging of access to applications, in particular the entry, change and erasure of data
☐	Physical erasure of data storage media before reuse
☐	Use of shredders or service providers
☒	Administration of rights by defined system administrators
☒	Password guidelines, incl. password length and changing passwords
☒	Secure storage of data storage media
☐	Proper destruction of data storage media (DIN 66399)
☐	Logging of destruction
☐	Other:

4. Transfer Control/Transportation Control

Ensuring that the confidentiality and integrity of data is protected during the transfer of personal data and the transportation of data storage media (e.g. through powerful encryption of data transmissions, closed envelopes used in mailings, encrypted saving on data storage media).

The following technical and organizational measures have been implemented by the Continental for the Processing of Personal Data described in Agreement:

☒	Establishment of dedicated lines or VPN tunnels

☒	Encrypted data transmission on the Internet (such as HTTPS, SFTP, etc.)
☐	E-mail encryption
☐	Documentation of the recipients of data and time frames of planned transmission or agreed erasure deadlines
☐	In case of physical transportation: careful selection of transportation personnel and vehicles
☐	Transmission of data in an anonymized or pseudonymized form
☐	In case of physical transportation: secure containers/packaging
☐	Other:

5. Entry Control/Transmission Control

Ensuring that it is possible to subsequently review and establish which personal data has been entered or changed at what time and by whom in automated processing systems, for instance through logging (entry control).

Depending on the system, ensuring that it is possible to review and determine to which offices/locations personal data has been transmitted or provided using equipment for data transmission, or to which offices/locations it could be transmitted (transmission control).

The following technical and organizational measures have been implemented by the Continental for the Processing of Personal Data described in the Agreement:

☐	Logging of the entry, change and erasure of data
☐	Traceability of the entry, change and erasure of data through unique user names (not user groups)
☒	Assignment of rights for the entry, change and erasure of data based on an authorization concept
☒	Creating an overview showing which data can be entered, changed and deleted with which applications
☐	Maintaining forms from which data is taken over in automated processing
☐	Other:

6. Availability Control/Restoration/Reliability/Data Integrity

Ensuring that systems used can be restored in case of a disruption (restorability). Ensuring that all system functions are available and that any malfunctions are reported (reliability). Ensuring that saved personal data cannot be damaged through system malfunctions (data integrity). Ensuring that personal data is protected from accidental destruction or loss (availability control), e.g. by implementing appropriate back-up and disaster recovery concepts.

The following technical and organizational measures have been implemented by the Continental for the Processing of Personal Data described in the Agreement:

☒	Uninterruptible Power Supply (UPS)
☒	Devices for monitoring temperature and moisture in server rooms
☒	Fire and smoke detector systems
☒	Alarms for unauthorized access to server rooms

☒	Tests of data restorability
☒	Storing data back-ups in a separate and secure location
☒	In flood areas the server is located above the possible flood level
☒	Air conditioning units in server rooms
☒	Protected outlet strips in server rooms
☒	Fire extinguishers in server rooms
☒	Creating a back-up and recovery concept
☒	Creating an emergency plan
☐	Other:

7. Separation Control/Separability

Ensuring that data processed for different purposes can be processed separately (for instance through logical separation of customer data, specialized access controls (authorization concept), separating testing and production data).

The following technical and organizational measures have been implemented by the Continental for the Processing of Personal Data described in the Agreement:

☒	Physically separated storing on separate systems or data storage media
☒	Including purpose attributions/data fields in data sets
☒	Establishing database rights
☒	Logical client separation (software-based)
☒	For pseudonymized data: separation of mapping file and storage on a separate, secured IT system
☒	Separation of production and testing systems
☐	Other:

ANNEX III: LIST OF SUBPROCESSORS

1. Subprocessors of Continental

Subprocessor **(Company Name, Address)**	**Subject matter**	**Location of data center / processing**
Continental Reifen Deutschland GmbH, Vahrenwalder Str. 9, 30165 Hannover, Germany	Provision of vehicle and tire information services	EU

2. Subprocessors of Continental Reifen Deutschland GmbH

Subprocessor **(Company Name, Address)**	**Subject matter**	**Location of data center / processing**
T-Systems International GmbH, Hahnstrasse 43D, 60528 Frankfurt/Main, Germany	Hosting	EU
Amazon Webservices EMEA SARL 5 Rue Plaetis, L-2338, Luxembourg	Hosting	EU
Azure Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown Dublin 18, D18 P521, Ireland	Hosting	EU
MessageBird B.V. Baarsjesweg 286HS, 1058 AE Amsterdam, Netherlands	SMS	EU
Questar Auto Technologies LTD 1st Aba – Even St. Herzeliya, 4672519, Israel	Telematics	EU
Cloudera, Inc. 5470 Great America Parkway Santa Clara CA 95054, US	Hosting	EU