DATA PROCESSING AGREEMENT (DPA) FOR VDO FLEET SERVICES (ANNEX C)

This DPA stipulates the legal obligations of the PARTIES regarding data protection resulting from the processing of personal data related to the respective contract about VDO FLEET SERVICES with the Customer. The following DPA is based on the official standard contractual terms established by the EU-Commission within the Commission’s Implementing Decision (EU) 2021/915.

The Customer as “Controller” and CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH as “Processor” agree as follows:

SECTION I

CLAUSE 1
Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

b) The Controller(s) and Processor(s) as mentioned above have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data as specified in Annex I.

d) Annexes I to III are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the Controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

CLAUSE 2
Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

CLAUSE 3
Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

CLAUSE 4
Hierarchy / Order of Precedence

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 5
Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a Controller or a Processor by completing the Annexes and co-signing to this DPA.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Controller or a Processor, in accordance with its co-signing.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II
OBLIGATIONS OF THE PARTIES

CLAUSE 6
Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Annex I.

CLAUSE 7
Obligations of the Parties

7.1. Instructions

a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the Controller.

7.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in Annex I.

7.4. Security of processing

a) The Processor shall at least implement the technical and organizational measures specified in Annex II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with these Clauses.

c) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

d) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of Sub-Processors

a) The Processor has the Controller's general authorization for the engagement of sub-Processors from an agreed list. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of sub-Processors at least 30 (thirty) days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-Processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object. If the Controller does not object within 30 days, his respective consent shall be deemed granted.

The Controller agrees herewith with the involvement of the Sub-Processors as listed in Annex III.

b) Where the Processor engages a sub-Processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the sub-Processor, in substance, the same data protection obligations as the ones imposed on the data Processor in accordance with these Clauses. The Processor shall ensure that the sub-Processor complies with the obligations to which the Processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the Controller's request, the Processor shall provide a copy of such a sub-Processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including personal data, the Processor may redact the text of the agreement prior to sharing the copy.

d) The Processor shall remain fully responsible to the Controller for the performance of the sub-Processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the sub-Processor to fulfil its contractual obligations.

7.8. International data transfers / international data processing

a) Any transfer of data to a third country or an international organization by the Processor shall be done - notwithstanding the provision in lit b below - only
   i. on the basis of documented instructions,
   ii. on the basis of a prior (general) consent by the Controller or
   iii. in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) Where the Processor engages a sub-Processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Controller agrees that such processing is allowed provided that

   i. the processing will be conducted in a country for which the EU-Commission has adopted a respective adequacy decision on the basis of Article 45 of Regulation (EU) 2016/679, or

   ii. the Processor and the Sub-Processor ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

c) The Controller agrees herewith with the transfer and processing of personal data within the meaning of Chapter V of Regulation (EU) 2016/679 by the Processor and/or Sub-Processors as listed in Annex III.

CLAUSE 8
Assistance to the Controller

a) The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the Controller.

b) The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the Processor shall comply with the Controller's instructions

c) In addition to the Processor's obligation to assist the Controller pursuant to Clause 8(b), the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

i. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a ‘data protection impact assessment’) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

ii. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

iii. the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

iv. the obligations in Article 32 Regulation (EU) 2016/679.

d) The Parties shall set out in Annex II the appropriate technical and organizational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

CLAUSE 9
Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the Processor.

9.1 Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant/ (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the Controller’s notification, and must at least include:

i. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

ii. the likely consequences of the personal data breach;

iii. the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex II all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III
FINAL PROVISIONS

CLAUSE 10
Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the Processor is in breach of its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with these Clauses, for whatever reason.

b) The Controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

   i. the processing of personal data by the Processor has been suspended by the Controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

   ii. the Processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

   iii. the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the Controller insists on compliance with the instructions.

d) Following termination of the contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

CLAUSE 11
List of Annexes

Annex I:	Details of Processing
Annex II:	Technical and organizational measures implemented by CONTINENTAL.
Annex III:	Sub-Processors, international data transfers / data processing

ANNEX I – DESCRIPTION OF THE PROCESSING

1. PURPOSE(S) FOR WHICH THE PERSONAL DATA IS PROCESSED ON BEHALF OF THE CONTROLLER

CONTINENTAL instructed to act as a data processor, in order to process on behalf of CUSTOMER (the Controller) the personal data which are necessary to render the services of the VDO FLEET SERVICES.

2. MANNER AND PURPOSE OF THE DATA PROCESSING IS:

2.1 CONTINENTAL is entitled to collect, process and use personal data only in accordance with the VDO FLEET SERVICES CONTRACT and the instructions of the CUSTOMER (see clause 7.1 above).

2.2 Details on the scope, nature and purpose of the collection, processing and / or use of personal data is subject of the General Terms and Conditions of the Contract, its Service Description as well as the products' functional overviews.

3. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS PROCESSED

☒ CUSTOMERs
☐ Event participants
☒ Communication participants
☐ Interested parties

☐ Visitors
☒ Service users
☒ Subscribers

☐ Supplier and/ or Service Provider (individual contacts at these vendors)

☒ Employees
☐ Former employees
☐ Employee's relatives
☒ Sales representatives
☒ Contact persons for business
☒ Business partners

☐ Applicants
☐ Apprentices/ interns
☐ Consultants
☐ Shareholders / bodies
☐ Suppliers and service providers

☒ Other please specify those employed by customers; i. e. drivers and users of VDO FLEET SERVICES

4. CATEGORIES OF PERSONAL DATA PROCESSED

General data/ private contact details

☒ Names Personal profiles
☒ Private address data

☐ Image
☒ Date of birth

☒ ID card data (e.g., Passport, Social Security, Driving License)
☐ Other please specify: ____

Contract data

☒ Settlement and payment data
☒ Financial Standing/ Creditworthiness

☒ Bank details/ credit card data
☒ Contract histories

☐ Other please specify: ____

Professional data

☒ Personal Details
☒ Performance Management
☒ Social Security Data

☐ Position and Employment Details
☐ Qualification and Education Details
☒ Absence from Work

☒ Other please specify:

- admission data of the customer and its operators / users
- driver data (e. g. name, address (company or private address as applicable), gender, birthday, license number, card number etc.)
- vehicle data and vehicle profiles
- communications data (e. g. telephone, email)
- movement data, GPS data

- activities of drivers and deployment profile, including driving times and rest times in accordance with Attachment 1B of the Regulation (EU) No. 561/2006, Regulation (EU) No. 2020/1054, Regulation (EC) No. 1360/2002, Regulation No. 165/2014 and Implementing Regulation (EU) No. 2016/799.
- data for use of the service by users download data for the driver card and tachograph

Service and IT usage data

☐ Device identifiers
☐ Image / video data
☐ Audio / voice data
☒ Access data
☐ Meta data
☐ Other please specify: ____

☒ Usage and connection data
☒ Telecommunication data/ message content
☐ Identification data
☐ Authorization

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.

Special categories of personal data

☐ Race or Ethnic Origin
☐ Physical or Mental Health
☐ Biometric Data
☐ Trade Union Membership
☐ Criminal Offences, Convictions or Judgments
☐ Other please specify: ____

☐ Religious or Philosophical Beliefs
☐ Political Opinions
☐ Genetic Data
☐ Sexual Life

5. DURATION OF THE PROCESSING

5.1 The duration of the data processing depends on the term of the Contract and/or any individual contracts or orders based on a framework agreement.

5.2 Until completion of the processing and subject to any other documented instructions of the Controller, the Processor shall return to the Controller or to a third party designated by the Controller, all documents, data carriers, processing results and data which have come into its possession, and which are connected with the contractual relationship or have been generated in the course of the execution of the Contract and/or this DPA.

This obligation extends to copies and/or reproductions of data carriers and/or data stocks. There is no right of retention with regard to the aforementioned data and data carriers. Unless otherwise provided for in the Contract, the Processor shall return all data and data carriers to the Controller free of charge. The Processor shall bear any costs and other expenses in connection with the return of data.

5.3 The Controller cannot demand the deletion of the data stored by the Processor, if and to the extent the Processor is subject to statutory retention obligations. Instead of deletion, the processing of the data can be restricted, as far as this is permissible due to local / country-specific implementation laws on data protection. This applies in particular if, due to the specific storage method, the deletion is not possible or only possible with disproportionately high expenditure.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Corporate Policy Continental Information Security Guideline (CISG) defines the **minimum requirements** for technical and organizational measures at CONTINENTAL in dealing with information. Depending on the classification of the information, measures are implemented that go beyond the minimum requirements.

The requirements of the CISG are implemented in the company on the basis of the Corporate Standard Information Security Framework and the corresponding Information Security Management System (ISMS).

Corporate Policy Continental Information Security Guideline (CISG)
Corporate Standard Information Security Framework
Annex 1 - Information Security Management System (ISMS)
Annex 2 - Roles & Responsibilities in Information Security - RACI Chart

1. PHYSICAL ACCESS CONTROL

Securing the physical access/access to processing systems with which the processing takes place against unauthorized persons (e.g. by physical object protection: fence, security personnel, door locks, turnstile, door with card reader, camera surveillance, organizational object protection, access authorization, access registration).

Corporate Standard Classification of Security Zones
Annex 1 - Layout and Security Requirements
Annex 2 - Audio/Visual Recording in Locations
Corporate Standard Continental ID Cards

Specifications for the measures:

☒	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 the use of automated processing systems by unauthorized persons by means of data transmission equipment (e.g., screensavers with passwords).

Corporate Manual Password Regulation (M60.02.01)
Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
Corporate Standard CUSTOMER Security Regulation (replaces M60.02.10)
Corporate Standard Mobile Environment Governance (replaces M60.05.01)

Specifications for the measures:

☒	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, modification or deletion of data carriers (data storage media control), prevention of unauthorized input of personal data as well as unauthorized knowledge, modification and deletion of stored personal data (data storage media control).

Guarantee that the persons authorized to use an automated processing system have access only to the personal data based on their access authorization (e.g. by means of authorization concepts, passwords, regulations governing the resignation and transfer of employees). (data usage control).

Corporate Manual Password Regulation (M60.02.01)
Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
Corporate Standard Classification and Control of Information
Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity

Specifications for the measures:

☒	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 32757)
☐	Logging of destruction
☐	Other:

4. TRANSFER CONTROL/TRANSPORTATION CONTROL

Ensuring the confidentiality and integrity of data during the transmission of personal information and the transport of data carriers (e.g., through powerful encryption of data transmissions, closed envelopes for mailings, encrypted storage on data carriers).

Corporate Standard Classification and Control of Information

Specifications for the measures:

☒	Establishment of dedicated lines or VPN tunnels
☒	Encrypted data transmission on the Internet (such as HTTPS, SFTP, etc.)
☒	E-mail encryption (transport 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

Ensure subsequent logging and verification of changes (which personal data were entered or modified, when and by whom) within automated processing systems (entry control). Ensure the sufficiently secured and documented transfer (including the secure and adequate transfer methods used) of personal data according to the geographical, physical or electronic transfer to other locations (transfer control).

Continental Information Security Guideline (CISG) – 3.5.10.1 Audit Logging
Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
Corporate Standard Classification and Control of Information
Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity

Specifications for the measures:

☒	Logging of the entry, change and erasure of data
☒	Traceability of the entry, change and erasure of data through unique usernames (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

Guarantee that systems used can be restored in the event of a malfunction (recoverability). Ensure that all functions of the system are available and that any malfunctions that occur are reported (reliability). Guarantee that stored personal data cannot be damaged by system malfunctions (data integrity). Guarantee that personal data is protected against accidental destruction or loss (availability control), e.g., by implementing suitable backup and disaster recovery concepts.

Corporate Manual Backup and Recovery Security Regulation (M60.02.08)

Specifications for the measures:

☒	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 zones: server rooms above the high-water 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 collected for different purposes can be processed separately. (e.g. by logical separation of customer data, special access controls (authorization concept), separation of test and production data.)

Continental Information Security Guideline (CISG) – 3.5.1.4 Separation of development, test and operational facilities

Specifications for the measures:

☒	Physically separated storing on separate systems or data storage media
☐	Including purpose attributions/data fields in data sets
☒	Establishing database rights
☐	Logical CUSTOMER 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 - SUB-PROCESSORS / INTERNATIONAL TRANSFERS

CONTINENTAL ensures an appropriate level of technical and organizational security measures at the Sub-Processors involved in order to process personal data within an appropriate and secure framework (Adequacy of the Sub-Processor).

If Sub-Processors are involved in the processing of personal data (e.g., hosting, provision of data center space, cloud services, operating software etc.), the implementation of technical and organizational measures by the respective Sub-Processor will be ensured by corresponding data processing agreements. Sub-Processors must - with sufficient warranty - ensure at least the same technical and organizational measures as agreed between the Customer and CONTINENTAL.

The following Sub-Processors / Subcontractors are engaged by CONTINENTAL:

	APPLICABLE ONLY IN CASE CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH IS NOT THE DIRECT CONTRACTING PARTY TO THE CUSTOMER AND IS ACTING AS SUB-PROCESSORS OF <RSOS/NATIONAL DEALERS/PARTNERS> **(APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):**
☐	**Continental Automotive Technologies GmbH**, Vahrenwalder Straße 9, 30165 Hannover, Germany (Development and Support)

	SUB-PROCESSORS OF CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH **(APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):**
☒	**Com-a-tec GmbH**, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Support Level 2)
☒	**Continental AG,** Hauptverwaltung, Vahrenwalder Straße 9, D-30165 Hannover Continental AG is the contract holder regarding the provision of services by the Sub-Processor of Continental AG towards Continental Automotive Technologies GmbH as listed below separately.
☒	**Continental Automotive Components (India) Private Limited** Technical Center India, South Gate Tech Park, Plot No. 1, Veerasandra Industrial Area, Hosur Main Road, Bangalore - 560 100, India. Continental Automotive Components India is a Continental Group Company which provides **Development, Monitoring and support on the services.** **Please note:** Any access by Continental Automotive Components India to (personal) data of TIS-Web-Customer within the EEA is subject to the Binding Corporate Rules of the Continental Group which ensures an adequate level of data protection in the meaning of Art 45 et seq. GDPR.
☒	**Continental Digital Services France SAS**, 1 avenue Paul Ourliac B.P.13704 31037 Toulouse, France Continental Digital Services France is a Continental Group Company which provides **Development, Monitoring and support on the services.**
☒	**Eviden Germany GmbH** , Otto-Hahn Ring 6, 81739 München (Support and Maintenance)
☒	**Google Ireland Limited,** Gordon House, Barrow Street, Dublin 4, Ireland (Provider of Cloud Services, e.g. Google Cloud Platform) **Please note:** Google will be used as "Sub-Processor" for the provision of cloud services. In this respect, CONTINENTAL has ensured that the data originated within the European Economic Area (EEA) will only be processed within the EEA, exempt as otherwise agreed with the CUSTOMER. In addition and as fallback, the Standard-Contractual-Clauses of the EU-Commission are in place (as provided by the Commissions' Implementing Decision (EU) 2021/914 of 04.06.2021) as also the new adequacy decision

	of the EU Commission for data processing in the USA of 10.07.2023 apply to Google LLC. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.
☒	**kernel concepts GmbH**, Hauptstraße 16, 57074 Siegen (Provider of kernel services, improvement, maintenance etc., data will be processed within the EEA only)
☒	**Zonar Systems, Inc.**, 18200 Cascade Ave S, Seattle, WA 98188, USA, a Continental Group Company. Zonar Systems provides support, maintenance, and development services for the TIS-Web-Services of CONTINENTAL. **Please note:** Any access by Zonar Systems to (personal) data of TIS-Web-Customer within the EEA is subject to the Binding Corporate Rules of the Continental Group which ensures an adequate level of data protection in the meaning of Art 45 et seq. GDPR. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA. As far as Zonar Systems is engaging further Sub-Processor for the provision of its services, such Sub-Processor are listed below.

	SUBPROCESSOR OF CONTINENTAL AUTOMOTIVE TRADING FRANCE SAS (ONLY APPLICABLE FOR FRANCE / FRENCH CUSTOMERS):
☒	**IMA TECHNOLOGIES**, 31 Route de Gachet 44300 Nantes, France (Support Hotline)

	SUBPROCESSOR OF CONTINENTAL AG (APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):
☒	**SYZYGY Deutschland GmbH**, Im Atzelnest 3, 61352 Bad Homburg, Germany (Hosting-Services)
☒	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Provider of Cloud Services; the cloud services are restricted to the EEA.)

	SUB-PROCESSORS OF ZONAR SYSTEMS, INC. (APPLICABLE FOR ALL COUNTRIES / CUSTOMERS):
☒	**Clearblade Inc.**, 1701 Directors BLVD STE 250, Austin, TX 78744, USA (Solution for managing telematic device connections, Support / Maintenance) **Please note:** Continental has ensured that the services and data originated within the EEA will only be processed on servers within the EEA. In addition, and as a fallback, the standard contractual clauses of the EU Commission (see Commission Implementing Decision (EU) 2021/914 of 04.06.2021) have been agreed with Clearblade. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.
☒	**DataDog Inc.,** New York Times Bldg, 620 8th Ave 45th Floor, New York, MA, USA (Support & Availability Services) **Please note:** Data Dog only processes pseudonymized, aggregated data; in addition and as fallback the Standard-Contractual-Clauses of the EU-Commission are in place (as provided by the Commissions' Implementing Decision (EU) 2021/914 of 04.06.2021). In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.
☒	**OKTA Inc.**, 100 First Street, 6th Floor, San Francisco, CA 94105, USA (Service Provider Customer Identity & Access Management (CIAM))

	Please note: Continental has ensured that the services and data originated within the EEA will only be processed on servers within the EEA. In addition, and as a fallback, the standard contractual clauses of the EU Commission (see Commission Implementing Decision (EU) 2021/914 of 04.06.2021) have been agreed with Okta as also the new adequacy decision of the EU Commission for data processing in the USA of 10.07.2023 apply. In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.
☒	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Provider of Cloud Services; the cloud services are restricted to the EEA.)
☒	**pendo.io Inc.,** 150 Fayetteville St., Raleigh, NC 27601, USA; European Representative (Art. 27 GDPR): DP-Dock GmbH, Ballindamm 39, 20095 Hamburg (Support & Development Services) **Please note:** pendo.io only processes pseudonymized, aggregated data. The data will only be processed and stored within the EEA. In addition, and as fallback, the Standard-Contractual-Clauses of the EU-Commission are in place (as provided by the Commissions’ Implementing Decision (EU) 2021/914 of 04.06.2021). In addition, Continental has implemented specific technical security measures as described above to prevent unauthorized access to data, especially from outside the EEA.

General information: Your rights as part of the European General Data Protection Regulation remain unchanged. CONTINENTAL furthermore confirms that your data will be stored in data centers in the European Union. CONTINENTAL uses highest security standards (e.g. ISO/DIN/https/encryption) and protects personal data during transmission and storage.

* * *