Data Processing Agreement (DPA)
related to the TIS-WEB SERVICES contract dated 24.06.2019

between

Example Customer

- Controller hereinafter referred to as "**Client"** -

and

Continental Automotive GmbH
- Muttergesellschaft der Continental Trading GmbH -
Heinrich-Hertz-Straße 45,
78052 Villingen-Schwenningen

- Processor hereinafter referred to as "**Contractor"** -

- jointly referred to as **"Parties"** -

This DPA stipulates the legal obligations of the Parties regarding data protection resulting from the processing of personal data related to the contract dated 24.06.2019 (hereinafter also referred to as "**Main Contract**"). The DPA applies to all activities associated with the Main Contract during which employees of the Contractor and/or third parties subcontracted by the Contractor have access to personal data provided by the Client.

1. OBJECT AND DURATION OF DATA PROCESSING

The Contractor processes personal data exclusively on behalf of and in accordance with the instructions of the Client. The Contractor is responsible for compliance with all applicable data protection provisions and regulations.

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

2. SCOPE OF DATA PROCESSING

The Contractor only, processes personal data within the scope of the main contract and this data processing agreement and according to Client's instructions (see clause 0).

2.1 Scope, type and purpose of data processing:

The subject matter of data processing, purpose and the details of the processing, type of personal data as well as categories of data subjects emerge from either the main contract concluded between the parties or from the processing activities described in **Attachment 1** (Details of Processing).

3. TECHNICAL/ORGANIZATIONAL MEASURES

If not stated in the basic service description under the Main Contract, technical and organizational measures taken by the Contractor are described in Attachment 2 to this DPA. The technical and organizational measures are subject to technological process and further development. Therefore, the Contractor is entitled to implement adequate alternative measures. The level of security for the implemented measures must not be compromised.

4. RIGHTS OF DATA SUBJECT – RECTIFICATION, RESTRICTION OF PROCESSING AND ERASURE OF DATA

4.1 The Contractor has to consult with the Client where this is necessary in order to safeguard the rights of the data subject and to fulfil the resulting legal obligations of the Client, in particular when notifying the data subject, providing information to data subjects and correcting, erasing personal data or restricting its processing.

4.2 The Contractor may only rectify, erase personal data or restrict the processing of personal data in accordance with Client's instructions. If a data subject contacts the Contractor directly in order to have their data rectified or erased, the Contractor shall promptly inform the Client about such request.

4.3 If the Client is legally obligated to provide information regarding processing of personal data to INDIVIDUALS (data subjects), the Contractor shall support the Client in providing this information, if

a) the Client requests the Contractor to do so in text form and insofar as

b) the Client shall bear the costs incurred by the Contractor as a result of the assistance.

5. INSPECTIONS AND OTHER RESPONSIBILITIES OF THE CONTRACTOR

The Contractor is also responsible for compliance with the following obligations:

5.1 Protecting data secrecy: All persons who can access personal data as part of their contracted work must be bound to observe secrecy of data.

5.2 Implementation of and compliance with all for this assignment necessary technical and organizational measures (see also clause 3).

5.3 Verifiability of the existing technical and organizational measures to the Client. The Contractor can also submit current certificates, reports or report excerpts from independent bodies (such as auditors, inspectors, data protection officers, IT security departments, data protection auditors and quality auditors) or a suitable certification from an IT security or data protection audit (e.g. in accordance with BSI Basic Protection).

5.4 Checks by means of regular reviews conducted by the Contractor with regard to the execution or fulfillment of the data processing, in particular compliance with and if any necessary amendments to regulations and measures of data processing. Notification of the Client of deficiencies and/or irregularities that are discovered during the review.

5.5 Appointment – if required by law – of a data protection officer. The Client will be provided with contact data for the purpose of direct contact.

5.6 Upon request provision of documentation regarding the, processing of personal data, on the basis of which the Client might prove the lawfulness of data processing.

5.7 Provision of the information and data necessary for the Client's records of processing activities; such information must be provided only upon Client's request and only in relation to data processing performed by the Contractor within the scope of this DPA.

5.8 The processing of data shall take place exclusively in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another state party to the Agreement on the European Economic Area. In the case of processing in a third country, the contractor shall ensure an adequate level of data protection at the data recipient within the meaning of Articles 45 - 47 EU GDPR.

6. SUB-CONTRACTOR(S) AND/OR SUB-PROCESSOR(S)

6.1 If Sub-Contractor(s) and/or Sub-Processor(s) are involved in the processing of personal data provided by the Client, the Client consents herewith with such involvement under the following conditions:

- The Contractor must select the Sub-Contractor(s) and/or Sub-Processor(s) carefully and ensure before contracting that such Sub-Contractor(s) and/or Sub-Processor(s) are able to comply with the arrangements made between the Client and the Contractor.
- The Contractor shall design contractual agreements with Sub-Contractor(s) and/or Sub-Processor(s) in such manner that they comply with the data protection provisions stipulated within the contractual relationship between the Client and the Contractor; sufficient guarantees must be provided to ensure that the appropriate technical and organizational measures are implemented in a way that the Processing takes place in accordance with the requirements of the GDPR.

6.2 The involvement of Sub-Contractors including the involvement of further processors by Sub-Contractor(s) and/or Sub-Processor(s) is permitted provided that the conditions set out in section 6.1 are met. The Contractor currently uses the Sub-Contractors/Sub-Processors listed in **Attachement 2**. The Client shall be informed in text form (§ 126b BGB) about (new) Subcontractors; he may only object to the use of a subcontractor for good cause, in particular due to a breach of contractual or statutory duties and regulations by the respective subcontractor.

6.3 Services obtained by the Contractor as ancillary services to support the Contractor in executing the contract data processing shall not be considered as subcontracting in the meaning of this section 6. These include, for instance, telecommunications services, maintenance and user service, cleaning services, auditors or the disposal of data storage media. The Contractor is, however, obligated to conclude appropriate contractual agreements and to implement controlling measures to ensure the protection and security of Client data, including with regard to ancillary services purchased from third parties.

7. CONTROL RIGHTS OF THE CLIENT

7.1 The Contractor agrees that the Client is entitled, after a written advance notice, to check compliance with the provisions on data protection and the contractual agreements to the necessary extent during regular business hours, in particular by obtaining information and inspecting the stored data and the data processing programs.

7.2 The Contractor is obligated, upon request, to provide the Client with information necessary to comply with its obligations related to contract data processing and to make relevant certifications available.

7.3 The costs and expenses of the inspection, in particular costs for employees of the Client, inspection service providers, travel costs, etc. shall be borne by the Client himself. As far as the expenditure or costs for the support by the Contractor exceed the duty to cooperate (Art. 28 (3) h) EU-GDPR), the Contractor can claim an appropriate compensation.

8. NOTIFICATION OF PERSONAL DATA BREACH

8.1 The Contractor shall notify every case of a personal data breach, for which the Contractor, its employees or subcontractors are responsible or breach of stipulation of the assignment to the Client.

8.2 This also applies to severe disruptions of the operating process, suspicion of violation of data protection law, or other irregularities in handling the personal data provided by the Client.

8.3 If the Client is subject to obligations to notify cases of data breach to supervisory authorities, the Contractor must support the Client.

9. CLIENT'S AUTHORITY TO GIVE INSTRUCTIONS

9.1 Personal data shall be processed exclusively within the scope of this DPA and in accordance with the instructions of the Client. Changes to the subject of processing and procedures must be jointly agreed and documented. The Contractor may provide information to third parties or data subjects only with the prior written consent of the Client.

9.2 The Client will confirm oral instruction in text form (e.g. e-mail) without undue delay. The Contractor shall not use the data for any other purpose, and is in particular not entitled to transfer it to third parties. No copies and duplicates shall be made without Client's knowledge thereof. This does not include back-up copies, if they are necessary to ensure proper data processing, and data necessary for compliance with legal archiving obligations.

9.3 The Contractor shall inform the Client promptly if it believes that Client's instructions violate data protection regulations. The Contractor is entitled to suspend carrying out the instruction in question until it is confirmed or changed by the person responsible at the Client.

10. DISCLOSURE, ERASURE OF DATA/RETURN OF DATA STORAGE MEDIA

10.1 The Contractor is obliged to hand over to the Client or to a third party designated by the Client all documents, data carriers, processing and usage results created and databases, upon Client's request or after completion of the contractual work - at the latest, however, upon termination of the contractual relationship. This obligation extends to copies and/or reproductions of data storage media and/or archived data. The Contractor has no right of retention. Such handovers must be free of charge and are not subject to any right of objection; any transfer costs or any other expenses related to the handover shall be borne by the Client.

10.2 After the handover the data in accordance with clause 10.1, or if the Client waives such handover, any data still in Contractor's possession must be destroyed or erased in accordance with data protection laws; the Client's consent must be obtained before any irrevocable erasure of data. The Contractor proves the erasure upon Client's request through appropriate documentation and/or confirmations. The Client may not demand the erasure of data if the Contractor is legally obligated to archive such data; the processing of such data shall be restricted by the Contractor. Instead of erasure, the processing of data shall be restricted if this is legally permissible (for instance based on local/country-specific implementation acts regarding data protection).

10.3 Documentation serving to prove proper data processing in accordance with this DPA and the law must be archived by the Contractor after the end of the DPA in accordance with applicable retention periods. As a relief documentation can be handed over to the Client at the end of this DPA.

10.4 The regulations of clauses 10.1 and 10.2 apply accordingly to testing and scrap material.

11. CLIENT'S DUTIES

11.1 The Client is responsible for compliance with data protection law, in particular for the legality of data transfer to the Contractor.

11.2 The Client shall provide the Contractor prompt and complete information if it detects any deficiencies or irregularities in relation to data protection law while reviewing processing results.

11.3 The Client shall maintain records of processing activities.

12. LIABILITY

12.1 The data protection obligations stated in this DPA represent significant contractual obligations for the Contractor (cardinal obligations) of the Main Contract concluded with the Client. In this respect, this DPA is to be seen as supplement to the Main Contract.

13. RELATIONSHIP TO THE MAIN CONTRACT, OTHER OBLIGATIONS AND PROVISIONS

13.1 The provisions of this DPA, including its attachments, shall take priority over the Main Contract and serve as a supplement to it, if not otherwise regulated in this DPA.

13.2 Should personal data provided by the Client to the Contractor be endangered by seizure or confiscation, by insolvency or composition proceedings or other events or by measures of third parties, the Contractor shall immediately inform the Client. The Contractor shall further

immediately inform all clients, their vicarious agents and all other relevant parties that the ownership of the data, data carriers, documents, etc. is exclusively with the Client.

13.3 Changes and/or amendments to this DPA must be made in writing to be effective. This shall also apply to a waiver of the written form requirement. With regard to the applicable law and the place of jurisdiction, the respective provisions of the Main Contract shall apply.

LIST OF ATTACHMENTS

ATTACHMENT 1:	Details of Processing
ATTACHMENT 2:	Technical and organizational measures for contract data processing implemented by the contractor

ATTACHMENT 1:

DETAILS OF PROCESSING

Editing note: Please select and complete the appropriate variant. The unsuitable clause that do not apply can be removed

1. Subject-matter of the assignment is:

1.1 Contractor is instructed to act as a data processor, in order to process on behalf of client, the data controller, the personal data which are necessary to render the services of TIS-Web application.

2. Manner and purpose of the data processing is:

2.1 Continental Trading GmbH is entitled to collect, process and use personal data only in accord-ance with the TIS WEB Services contract and the instructions of the client (see Section 9).

2.2 Details on the scope, nature and purpose of the collection, processing and / or use of per-sonal data can be found in the General Terms and Conditions of the Main Contract and the products functional overviews.

3. Categories of Data Subjects:

X Clients	☐ Visitors
☐ Event participants	X Service users
☐ Communication participants	X Subscribers
☐ Interested parties	
☐ Supplier and/ or Service Provider (individual contacts at these vendors)	
☐ Employees	☐ Applicants
☐ Former employees	☐ Apprentices/ interns
☐ Employees relatives	☐ Consultants
☐ Sales representatives	☐ Shareholders / bodies
X Contact persons for business	☐ Suppliers and service providers
X Business partners	

X other please specify: those employed by customers, i.e. drivers and users of TIS-Web services

4. Type of Personal Data:

General data/ private contact details:

X Names Personal profiles ☐ Image

☐ Private address data X Date of birth

X ID card data (e.g. Passport, Social Security, Driving Licence)

☐ other please specify: _____

Contract data:

X Settlement and payment data X Bank details/ credit card data

X Financial Standing/ Creditworthiness X Contract histories

☐ other please specify:_____

Professional data:

X Personal Details ☐ Position and Employment Details

☐ Performance Management ☐ Qualification and Education Details

☐ Salary or Social Security Data ☐ Absence from Work

X other please specify:

- admission data of the Customer and its operators / users
- driver data
- 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 regulation EU 561/2006
- data for use of the service by users
- download data for the driver card and tachograph

Service and IT usage data:

☐ Device identifiers ☐ Usage and connection data

☐ Image / video data ☐ Telecommunication data/ message content

☐ Audio / voice data ☐ Identification data

X Access data ☐ Authorisations

☐ Meta data

☐ other please specify: _____

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 ☐ Sexual Life

☐ Criminal Offences, Convictions or Judgments

☐ other please specify: _____

ATTACHMENT 2

Technical and organizational measures Continental (acc. Article 32 EU GDPR)

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
Annex 1 - Information Security Management System (ISMS)
Annex 2 - Roles & Responsibilities in Information Security - RACI Chart

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

Note: The implemented security measures are to be inserted by the service and / or business process responsible in the following table, or entered under "Other".

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:

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
Corporate Standard Client Security Regulation
Corporate Standard Mobile Environment Governance

Note: The implemented security measures are to be inserted by the service and / or business process responsible in the following table, or entered under "Other".

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:

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

Note: The implemented security measures are to be inserted by the service and / or business process responsible in the following table, or entered under "Other".

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:

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

Note: The implemented security measures are to be inserted by the service and / or business process responsible in the following table, or entered under "Other".

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
☒	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:

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

Note: The implemented security measures are to be inserted by the service and / or business process responsible in the following table, or entered under "Other".

Specifications for the measures:

☒	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:

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)

Note: The implemented security measures are to be inserted by the service and / or business process responsible in the following table, or entered under "Other".

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:

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

Note: The implemented security measures are to be inserted by the service and / or business process responsible in the following table, or entered under "Other".

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 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:

Subcontractors

Ensuring an appropriate level of technical and organizational security measures at the supporting parties commissioned by the Contractor in order to be able to process the relevant personal data within an appropriate and secure framework (suitability of the Contractor).

If subcontractors are commissioned (e.g. for hosting, provision of data center space, operating software for processing personal data, etc.) for the processing of personal data, the implementation of technical and organizational measures by the respective subcontractor shall be regulated by corresponding data processing agreements. The subcontractor must - with sufficient warranty - ensure at least the technical and organizational measures agreed with the contractor.

Note: *Continental usually employs subcontractors e.g. for hosting or for maintenance / troubleshooting support.* ***It is imperative to check which subcontractors are involved****.*

The following subcontractors are commissioned:

☒	**Continental Automotive GmbH**, Vahrenwalder Straße 9, 30165 Hannover, Germany (Support)
☒	**SYZYGY Deutschland GmbH**, Im Atzelnest 3, 61352 Bad Homburg, Germany (Hosting-Services)
☒	**Astrata Europe B.V.,** High Tech Campus 32, 5656 AE Eindhoven, Netherland (Cloud-/Hosting-Services)
☒	**Atos Information Technology GmbH,** Otto-Hahn-Ring 6, 81739 Munich, Germany (Support Level 3 and Maintenance)
☒	**MiX Telematics Europe Ltd.,** 6180 Knights Court, Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YB, United Kingdom (RTM service)
☒	**Com-a-tec GmbH**, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Support Level 2)
☒	**Global Logic SA,** Strzegomska 46b, 53-611,Wroclaw, Poland (Support Level 3 and Maintenance)