# Commissioned Data Processing Agreement

in accordance with Art. 28 of the EU General Data Protection Regulation (GDPR)

between

**Name**

**and**

**address**

(hereinafter referred to as "**Controller"**)

and

**Name**

**and**

**address**

(hereinafter referred to as "**Processor"**)

(Together as the **“Parties”**)

**§ 1 - Subject matter**

1. **Principal Agreement.** This Commissioned Data Processing Agreement **(“Agreement”)** governs the obligations of the contracting parties in connection with the processing of the Controller’s personal data by the Processor under the agreement mentioned in Attachment 1 (“**Principal Agreement**”).

2. **Scope.** The subject, scope and purpose of the processing of personal data by the Processor can be found in Attachment 1 and in the Principal Agreement’s specification of services.

3. **Priority regulation**. The provisions of this Agreement including its Attachments shall take precedence over the provisions of the Principal Agreement.

Should the EU Standard Contractual Clauses become part of the Agreement, they will take precedence over the provisions of this Agreement and its Attachments.

**§ 2 - Controller rights and duties**

1. **Role of the Controller.** The Controller is the responsible party within the meaning of Art. 4 (7) of the GDPR or (sub-)processor within the meaning of Art. 4 (8) of the GDPR of one/more controller(s) or of one/more other processor(s) whose data he processes on a (sub-)contract basis. He is in particular responsible for the lawfulness of the processing of personal data, as well as for the protection of the data subjects’ rights.

2. **Instructions.** The Controller has the right to issue instructions regarding the nature, scope and methods of the processing of personal data. The Controller shall generally issue instructions in writing or by e-mail. In case of urgency or due to other special circumstances, instructions may also be given orally or by telephone and shall always be confirmed afterwards by the Controller in writing or by e-mail without undue delay.

The persons authorized to issue instructions on behalf of the Controller and the entitled Processor’s recipients of instructions are listed in Attachment 1. The Parties shall notify each other in writing or by email without undue delay of any changes to the persons entitled to give or receive instructions.

**§ 3 - Processor rights and duties**

1. **Role of the Processor.** The term (Sub-) **“Processor”** shall have the same meaning as in Art. 4 (8) of the GDPR.

The Processor and any person acting under his authority with access to the data shall process the data exclusively for the purposes specified in Attachment 1 and within the framework of the Principle Agreement in accordance with the Controller's instructions – including with regard to transfers of personal data to a third country or an international organization-, unless the Processor is obliged by Union or Member State law to process the data in a certain way. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such notification on important grounds of public interest (Art. 28 (3) (2nd sentence) (a) of the GDPR).

The Processor shall document the instructions given to him in a suitable, clear form and shall make this documentation available to the Controller on request.

Any specific instructions at the commencement of the Agreement are stipulated in Attachment 1. Copies or duplicates of personal data will not be made without the knowledge of the Controller. Exceptions to this are back-up copies, insofar as they are necessary to guarantee proper data processing, as well as data required to comply with mandatory retention periods defined by law.

2. **Deletion, return.** Upon request by the Controller or without undue delay after completion of the contractual work the Processor shall, according to the Controller’s specification, return or destroy resp. delete in accordance with data protection legislations all personal data from the contractual relationship (this also applies to any existing copies), unless Union or Member State law requires storage of the personal data. The Processor shall inform the Controller of such a legal obligation, unless this is prohibited by law. The obligation to delete or return also applies to test and reject material. The deletion, destruction or complete return must be confirmed to the Controller in writing, stating the date. The plea of rights of retention, for example within the meaning of § 273 BGB, is excluded with regard to the processed data and the associated data carriers.

3. **Data Protection Officer or Data Protection Contact Person.** The Processor shall ensure the appointment of a Data Protection Officer if legally required or, if the appointment of a Data Protection Officer is not required by law, the Processor shall ensure the appointment of a Data Protection Contact Person.

The contact details of the Data Protection Officer or the Data Protection Contact Person are listed in Attachment 1. Any changes shall be reported without undue delay to the Controller in writing or by email.

4. **Data secrecy.** The Processor is obliged to treat the data confidentially. The Processor shall comply with the provisions of the GDPR on the preservation of confidentiality in accordance with Art. 28 (3) (2nd sentence) (b), Art. 29 and Art. 32 (4) of the GDPR. Accordingly, the Processor shall only engage employees who are bound to confidentiality and have previously been made familiar with the data protection laws applicable. The confidentiality obligation of the Processor's employees shall also apply after termination of their employment contracts. These obligations of the Processor shall continue to apply after the termination of this Agreement.

5. **Legal compliance, monitoring.** The Processor is obliged to comply with all applicable legal regulations concerning the processing of personal data. The Processor shall regularly monitor compliance with the applicable data protection provisions, contractual obligations and the instructions of the Controller during the term of the Agreement and shall provide the Controller with appropriate proof of this upon request. The duty of control applies in particular to the internal processes as well as the technical and organizational measures. A concept for monitoring measures must be documented and presented to the Controller upon request.

6. **Support to the Controller in the fulfilment of its obligations according to the GDPR.** Considering the nature of the processing, the Processor shall, if possible, support the Controller with suitable technical and organizational measures in order to comply with its obligation to respond to data subject’s requests as set out in Chapter III of the GDPR. If the data subjects assert their rights with the Processor, the Processor must immediately forward the requests to the Controller. The Processor may only provide information to the data subjects, correct or delete their data or restrict the processing of the data in accordance with documented instructions from the Controller.

The Processor will also support the Controller in complying with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available.

The Processor shall otherwise support the Controller to an appropriate extent in answering official or judicial enquiries and in dealing with other official or judicial measures (e.g. inspections) and shall provide the necessary information.

7. **Data breaches**. Personal data breaches at the Processor or at his Subprocessors must be reported to the Controller without undue delay after becoming aware of the breach and the information and documents required to comply with any reporting and notification obligations of the Controller pursuant to Art. 33 and Art. 34 GDPR shall be included. The Processor shall inform of all relevant circumstances, the measures taken and provide an assessment of the risks arising from the data breach to the data subjects concerned. The Processor shall answer any queries without undue delay and cooperate closely with the Controller in clarifying the circumstances. The notification of a data breach to the competent authority and the notification to the data subjects shall be made exclusively by the Controller.

The notification of the Processor must be sent simultaneously to the following e-mail addresses:

- E-mail address of the authorized representative referred to in Attachment 1 section 9

- Controller’s data protection functional mailbox, Attachment 1 section 13.

**§ 4 - Place of processing**

1. **Consent requirement for processing in a third country with poor data protection security.** The processing of the data by the Processor and the Subprocessors approved by the Controller (see § 7) shall in principle take place exclusively in the Federal Republic of Germany, in a Member State of the European Union, in a state which is a party to the Agreement on the European Economic Area or in a country where an adequacy decision has been issued by the European Commission in accordance with Art. 45 of the GDPR. Any relocation of processing to another country (**"third country with poor data protection security"**) requires the consent of the Controller and may only take place if the legal requirements for data transfers to third countries under the applicable data protection laws are met. The Processor shall complete section 7 of Attachment 1 and provide additional documents if necessary.

2. **Processing by Processor in a third country with poor data protection security.** If the processing of the data by the Processor takes place exclusively or also in a third country with poor data protection security, the EU standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (“EU standard contractual clauses 2021”) shall apply in respect of such processing. The selection of the module of these EU standard contractual clauses 2021 applicable to the processing shall be made in Attachment 1.   
  
Controller and Processor shall cooperate closely in documenting compliance with the obligations resulting from the EU standard contractual clauses 2021. In order to meet the criteria set out in Clause 14 of the EU standard contractual clauses 2021, the Processor shall provide the Controller with all information required in this respect. In particular, the Processor shall answer the Controller’s questions truthfully, comprehensively and within a reasonable period of time regarding the applicability of legal provisions and practices or their practical implementation in the relevant third countries with poor data protection security.

If, due to the legal provisions and practices in these third countries with poor data protection security and in view of the particular circumstances of the processing, there is no reasonable assurance that the processing will be carried out in compliance with the EU standard contractual clauses 2021, the Processor shall, in consultation with the Controller, (i) implement additional technical and organizational measures and/or (ii) provide additional contractual assurances, which, taking into account these legal provisions and practices and the particular circumstances of the processing, provide a sufficient guarantee for the processing of the data in compliance with the Processor’s obligations under the EU standard contractual clauses 2021 (“Additional Measures and Assurances”).

The processing of the data by the Processor may only start after the Controller’s questions mentioned in paragraph 2 have been answered by the Processor and after the Additional Measures and Assurances possibly required according to paragraph 3 have been taken or given.

3. **Processing by Subprocessors in a third country with poor data protection security (if Processor is established in the EU or in a country with an adequate level of data protection).** If Subprocessors within the meaning of § 7 (1) of a Processor established in the EU or in a country with an adequate level of data protection process data in a third country with poor data protection security, the Processor shall, in addition to the requirements set out in § 4 (1), ensure before the start of processing by these Subprocessors that the EU standard contractual clauses 2021 have been concluded with the Subprocessor or that Binding corporate rules within the meaning of Art. 47 of the GDPR apply to the Subprocessor. § 4 (2) paragraph 2 and 3 shall apply accordingly in the relationship between the Processor and Subprocessor. Upon request of the Controller, the Processor shall provide the Controller with a copy of the documents relevant insofar.

4. **Processing by Subprocessors in a third country with poor data protection security (if Processor is neither established in the EU nor in a country with an adequate level of data protection).** If Subprocessors within the meaning of § 7 (1) of a Processor neither based in the EU nor in a country with an adequate level of data protection process data in a third country with poor data protection security, the Processor shall, in addition to the requirements set out in § 4 (1), conclude contractual agreements with these Subprocessors before the start of the processing by these Subprocesors which ensure, with regard to the processing by the Subprocessors, that this processing takes place at a level of data protection which corresponds to the level guaranteed by the EU standard contractual clauses 2021 or by Binding corporate rules within the meaning of Art. 47 of the GDPR. § 4 (2) paragraph 2 and 3 shall apply accordingly in the relationship between the Processor and Subprocessor. Upon request of the Controller, the Processor shall provide the Controller with a copy of the documents relevant insofar.

**§ 5 - Liability**

The Processor shall be liable in accordance with the statutory provisions for damages of the Controller resulting from the Processor’s culpable breach of this Agreement or statutory data protection obligations affecting the Processor (Art. 82 GDPR). In this regard, any limitations of liability otherwise agreed between the parties (e.g. in the Principal Agreement) shall not apply.

**§ 6 Technical and organizational measures**

1. **General information.** The Processor shall take the appropriate technical and organizational measures within the meaning of Art. 28 paragraph 3 lit. c and Art. 32 of the GDPR, in particular in connection with Art. 5 paragraph 1, paragraph 2 of the GDPR to ensure a level of protection appropriate to the risk arising from the processing of the data.

In assessing the adequate level of protection, the contracting parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the risks to data subjects.

Against this background, the Processor shall implement at least the technical and organizational measures defined in Attachment 2.

Technical and organizational measures are subject to technical progress and continuous development. In this respect, the Processor is permitted, in consultation with the Controller, to implement alternative adequate measures, provided that the security level of the agreed technical and organizational measures is not fallen below. Changes must be documented and communicated to the controller immediately. Significant changes require the prior written consent of the controller.

2. **Certification.** In addition, the Processor must document and demonstrate the suitability for implementing adequate security measures by a corresponding TISAX or ISO/IEC 27001 certification.

The Processor is obliged to implement the safety measures required to achieve and maintain the certification, which he has specified in the certification procedure, as well as such measures contractually agreed in Attachment 2, throughout the term of the contract.

Deviations from certification according to TISAX or ISO/IEC 27001 are only permitted with the prior written consent of the responsible information security department of the Controller.

3.  **Audit rights.** With regard to the control obligations of the Controller before the start of data processing and during the term of the contract, the Processor shall ensure that the Controller can satisfy himself of compliance with the technical and organizational measures taken.

4. **Data processing in private homes.** The processing of the contractual personal data in private homes is only permitted if an appropriate level of security is also guaranteed there by the Processor within the meaning of the GDPR and this agreement.

**§ 7 - Subprocessors**

1. **Use of Subprocessors.** The Controller agrees that the Processor may involve third parties ("Subprocessors") for the performance of the contractually agreed services and the processing of data in connection therewith, provided that the requirements of the following paragraphs are guaranteed.
2. **Subprocessors permitted at the time of conclusion of this Agreement**. The Processor is permitted to use the Subprocessors listed in Attachment 1.
3. **Further Subprocessors**. The Controller shall be informed by the Processor in writing or by e-mail without undue delay, but no later than 45 calendar days prior to the assignment, of any intended assignment of additional Subprocessors or replacement of existing Subprocessors, so that the Controller has sufficient time to raise objections to such assignment before the assignment. The Processor shall provide the Controller with the necessary information to enable the Controller to exercise his right of objection. The processing of data by the Subprocessor is only permitted once all legal requirements and those resulting from this Agreement are met.
4. **Agreements with Subprocessors.** The Processor must ensure that the contractual agreements with the Subprocessors have the same contractual data protection obligations to which the Processor is subject under this Agreement. The Processor shall regularly check compliance with these data protection obligations by the Subprocessors, in particular the implementation of the necessary technical and organizational measures.
5. **Liability.** If the Subprocessor does not fulfill its data protection obligations, the Processor is liable to the Controller for compliance with the obligations of that Subprocessor.

**§ 8 – Audit rights of the Controller**

1. **Audit rights.** The Controller has the right to verify compliance with the provisions of this Agreement, the instructions issued and the applicable data protection laws, either by itself or through a suitable third party appointed by the Controller and obliged to maintain secrecy. In particular, the Processor shall provide the Controller with all necessary information to prove compliance with the obligations laid down in Art. 28 of the GDPR and enable on-site inspections and other checks to be carried out by the Controller or another auditor appointed by the Controller.

2. **Duty to provide assistance.** The Processor assures assistance in these checks to a reasonable extent, if necessary. In particular, the Processor shall grant access to data processing systems, provide the necessary information and make available the necessary documentation.

3. **Execution.** Inspections at the Processor's premises must be announced in due time and must not disproportionately affect its business operations.

**§ 9 – Notification duties**

1. **Unlawful instructions.** The Processor shall inform the Controller without undue delay if he assesses an instruction issued by the Controller to infringe the GDPR or other Union or Member State data protection provisions. The Processor is entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the Controller.

2. **Controls by the data protection authorities.** Any investigations or actions taken by the data protection authorities againstthe Processor must be notified to the Controller without undue delay, insofar as the data of the Controller is affected. The Processor shall put remedy to any objections raised by the data protection authorities without undue delay and notify the Controller accordingly.

3. **Errors and irregularities.** Insofar as the data of the Controller is affected, the Processor shall notify the Controller without undue delay of any malfunctions, detected or suspected infringements to the applicable data protection laws or this Agreement made by the Processor or the Processor’s employees, as well as any suspicion of data breaches or irregularities in the processing of the data. This applies in particular with regard to any reporting and notification obligations of the Controller in accordance with Art. 33 and 34 of the GDPR.

**§ 10 - Term**

1. **Term.** The term of this Agreement shall correspond to the term of the Principal Agreement.

2. **Continuity.** If the Processor effectively continues to process the Controller’s personal data beyond the term of the Principal Agreement (e.g. storage due to retention obligations defined by law), the provisions of this Agreement continue to apply.

**§ 11 - Miscellaneous**

1. **Changes.** Changes to this Agreement must always be made in writing, unless otherwise specified in this Agreement.
2. **Adjustments.** Insofar as adaptations of this Agreement are necessary for the parties to comply with the legal requirements, they shall make the corresponding adaptations without undue delay.
3. **Expenses.** The services by the Processor under this Agreement are compensated by the remuneration set out in the Principal Agreement.
4. **Third-party measures**. If the Controller’s personal data at the Processor is jeopardized as a result of third-party measures such as seizure, insolvency or settlement proceedings, or as a result of other comparable events, the Processor must inform the Controller without undue delay.
5. **Severability clause.** Should individual sections of this Agreement be or become ineffective, this does not affect the validity of the rest of the Agreement. The Controller and the Processor undertake to replace the invalid provision with a legally permissible provision that comes as close as possible to the purpose of the invalid provision and meets the requirements of Art. 28 of the GDPR.

4. **Applicable law, place of jurisdiction.** This agreement is governed by law of the Federal Republic of Germany excluding the United Nations Convention of April 11, 1980 on Contracts for the International Sale of Goods (CISG). The sole place of jurisdiction is that of the Controller.

5. **Attachments.** Attachments 1 and 2 form an integral part of the Agreement.

Attachment 1 Description of Data Processing

Attachment 2 Technical and Organizational Security Measures

\* \* \*

|  |  |
| --- | --- |
| **Controller** | |
| Name (printed):  Click or tap here to enter text.  Function / Title:  Click or tap here to enter text.  Place, Date:  Click or tap here to enter text.  Signature:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Name (printed):  Click or tap here to enter text.  Function / Title:  Click or tap here to enter text.  Place, Date:  Click or tap here to enter text.  Signature:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
| **Processor** | |
| Name (printed):  Click or tap here to enter text.  Function / Title:  Click or tap here to enter text.  Place, Date:  Click or tap here to enter text.  Signature:  \_\_\_\_\_\_\_\_ | Name (printed):  Click or tap here to enter text.  Function / Title:  Click or tap here to enter text.  Place, Date:  Click or tap here to enter text.  Signature:  \_\_\_ \_\_\_\_ |

**ATTACHMENT 1 - Description of the Commissioned Data Processing**

1. **Principal Agreement**

Principal Agreement within the meaning of § 1 section 1 of this Agreement:

Title: ……

Parties: ……

Date: ……

2. **Subject matter of the processing**

The subject matter of the processing is the performance of the following services by the Processor:

……

3. **Scope and purpose of data processing / data processing measures**

More detailed description of the processing in terms of scope and purpose:

……

4. **Categories of data subjects**

The following groups of persons are affected by the Commissioned Data Processing:

**Employees.** Employees of the own group company, with the meaning of employee of the Controller.

*e.g. Employees, trainees, applicants, former employees*

**Group employees.** Employees of another group company, with the meaning of employee of a VW Group company, but not of the Controller.

*e.g. Employees of other MAN companies, Scania employees, Audi employees*

**Partner company employees.** Employees of a supplier, service provider, joint venture, temporary employment agency

*e.g. Employees from partner companies (e.g. IT service providers, suppliers), employees from joint ventures, temporary employees*

**Customers.** Any person who has a customer business relationship with the Controller

*e.g. Vehicle buyers, bank customers, insurance policy holders, rental customers*

**Other business partners.** Any natural or legal person with whom the Controller has a business relationship, except customers

*e.g. Suppliers, importers or service partners themselves; intermediaries, shareholders, freelancers*

**Outsiders.** Any person who has no business relationship with the Controller

*e.g. Visitors, guests, interested parties*

**Children.** The assessment of whether the data subject is a child is governed by the respective national law.

*e.g. in Germany, persons under the age of 16 are referred to as children*

5. **Categories of personal data**

The Commissioned Data Processing includes the following types of personal data:

**Professional contact and (work) organization data**

*e.g. surname, first name, gender, address, e-mail address, telephone number, mobile phone number, company, area, department, cost center, personnel numbers, responsibilities, functions*

**Data regarding IT use**

*e.g. UserID, roles, authorizations, login times, computer name, IP address, GID, Legic No.*

**Motor vehicle usage data with vehicle identification number/license plate number, guarantee, warranty, product liability, safe vehicle operation.** Data generated during motor vehicle use that is linked to vehicle identification numbers/license plate numbers and is relevant in connection with workshop repairs, guarantees and warranties, or is important for product liability, or if its availability is necessary for safe vehicle operation.

**Private contact and identification data**

*e.g. surname, first name, gender, address, e-mail address, telephone number, mobile phone number, date and place of birth, identification numbers, nationality*

**Contract data**

*e.g. products purchased, (financial) services, date of purchase agreement, purchase price, extras, warranties*

**Motor vehicle data with vehicle identification number/license plate number: comfort settings, multimedia, navigation.** Data generated during motor vehicle usage that is linked to vehicle identification numbers/license plate numbers and that relates to comfort settings such as seat position, preferred radio stations, air conditioning settings, GPS data, e-mail/text contact information

**Motor vehicle usage data with vehicle identification numbers/license plate number: assist systems, vehicle handling characteristics**  
Data produced during motor vehicle usage linked to vehicle identification numbers/license plate numbers and that relates to vehicle handling characteristics or the use of assist systems and their specific operational data

**Position data**

*e.g. GPS, radio network location, movement profile, WLAN hotspot location*

**Data concerning personal/professional relationships and characteristics**

*e.g. data on spouse or children, marital status, portrait photo, honorary office, job title, professional career, length of service, tasks, activities, dates of entry and exit, qualifications, assessments / evaluations*

**Remuneration and time management data**

*e.g. pay scale group, payroll accounting, special payments, garnishment, daily attendance times, reasons for absence*

**Solvency and bank data**

*e.g. payment behavior, balance sheets, data from credit agencies, credit score values, financial circumstances, bank account details, credit card number*

**Special categories of personal data**: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (fingerprints, voice recognition, iris scan, etc.), data concerning health, data concerning sexual life or sexual orientation.  
  
Only in the event that special categories of personal data are being processed in third countries with poor data protection security:  
  
a) Please specifically indicate here the relevant special categories of personal data:   
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
b) Please indicate here the limitations and safeguards agreed in relation to the special categories of personal data referred to in a), which take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions, records of access to data, restrictions on onward transfers or additional security measures  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Personal data on criminal offences / administrative offences:** Data relating to criminal offences or suspected criminal offences.

**Special category: Employee photo.** Portrait photo published by the employee on a voluntary basis (e.g. intranet telephone book, internal social media platform)

6. **Further description of the data transfer**  
  
If the EU standard contractual clauses 2021 are part of the Agreement, please provide further information here:

a) Frequency of data transfer to third countries with poor data security (multiple answers possible):   
  
  one time  regularly  continuously

b) Duration for which the personal data will be stored or, if this is not possible, the criteria for determining this duration (multiple answers possible):   
  
  No or only volatile storage  
  
  Storage until the individual processing purpose has been achieved

Storage until termination of the Principal Agreement  
  
 If applicable, criteria for determining the duration:  
  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
c) Competent supervisory authority  
  
 Supervisory authority responsible for the Controller:   
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. **Special instructions at the start of the Agreement**

Anonymization of certain data: …

Prohibition of the transmission of data: …

Deletion of the data after every ... month

The following policies, manuals and company agreements must be observed: …

…

8. **Processing location** *Multiple answers possible!*

Germany

Member State of the European Union or part of the European Economic Area

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.  
Iceland, Norway, Liechtenstein

Countries with an adequate level of data protection, currently:

Andorra, Argentina, Australia (Restricted for passenger data only), Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, United Kingdom, United States of America (USA; only if certified according to the EU-U.S. Data Privacy Framework) and Uruguay.

Third country with poor data protection security: …..

If data processing takes place in a third country with poor data protection security, at least one of the additional admissibility requirements listed below must be met. Please tick all applicable alternatives.

Module 2 of the EU standard contractual clauses 2021 is completed between the Controller and every Processor in a third country with poor data protection security.

Module 3 of the EU standard contractual clauses 2021 is completed between the Processor and any Subprocessor in a third country with poor data protection security.

The data processing is covered by consent of the data subjects.

The Processor and every Subprocessor are subject to Binding corporate rules within the meaning of Art. 47 of the GDPR.

9. **Authorized person to issue instructions and carry out verification on behalf of the Controller**

Name: ……

Contact details (e-mail, telephone, address): ……

10. **Responsible recipient for receiving instructions on behalf of the Processor**

Name: ……

Contact details (e-mail, telephone, address): ……

11. **Processor’s Data Protection Officer or Data Protection Contact Person**

The Processor has appointed the following Data Protection Officer:

Name: ……

Contact details (e-mail, telephone, address): ……

The Processor has appointed the following Data Protection Contact Person:

Name: ……

Contact details (e-mail, telephone, address): ……

12. **Subprocessors**

The Processor shall not employ Subprocessors.

The Processor employs the following Subprocessors:

No. \_\_ Subprocessor (name, legal form, address, contact person):

...

Processed data categories:

...

Processing activity of the Subprocessor (brief description of the tasks):

...

Duration of processing:

...

Processing (also) takes place in the following third countries with poor data protection security:

...

13. **Notification of Data Breaches**

The notification of data breaches of the Processor shall be sent to the following selected functional   
e-mailboxes of the Controller:

[DSGVO-Zentralteam@man.eu](mailto:DSGVO-Zentralteam@man.eu)

mtb-iso@man.eu

mtb-cdc@man.eu

information-security@traton.com

...

14. **Data Processing in private homes (home office)**

Yes, data processing may take place in private homes.

No, there is no data processing in private homes.

**ATTACHMENT 2 - Technical and Organizational Security Measures**

1. The Processor has taken the following technical and organizational security measures:

... List of TOMs...

or.

Reference to a data security concept according to Art. 32 GDPR

1. The Processor has demonstrated his suitability by submitting the following certificate documents:

VDA ISA (TISAX Label - shared with the Controller in the ENX database)

ISO 27001 – certificate (including Statement of Applicability)

Other existing certifications: (in addition to the above basic requirements):

Cloud Vendor Assessment (DCSO)

BSI C5 (Federal Office for Information Security, Cloud)

CSA STAR (Cloud Security Alliance)

ISO 27017 (Extension of ISO 27001 with regard to Cloud Controls)

ISO 27018 (Extension of ISO 27001 with regard to personal data)