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 collection, processing and use of the Controller's personal data by the Processor under the agreement mentioned in Annex 1 ("**Principal Agreement**").

2. **Scope.** The subject, scope, nature, and purpose of the collection, processing, and use of personal data by the Processor can be found in Annex 1 and in the Principal Agreement's specification of services .

3. **Priority regulation**. The provisions of this Agreement including its Annexes 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 annexes.

§ 2 - Controller duties

1. **Role of the Controller.** The Controller is the responsible party within the meaning of Art. 4 (7) of the GDPR. He is in particular responsible for the legal admissibility 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 purposes and means 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 Annex 1. The Parties shall immediately notify each other in writing or by email of any changes to the persons entitled to give or receive instructions.

§ 3 - Processor duties

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

   The Processor and any person acting under its authority with access to the data shall process the data exclusively for the purposes specified in Annex 1 and within the framework of the Principle Agreement in accordance with the Controller's instructions, unless the Processor is obliged by mandatory law to process the data in another way. In such a case, the Processor shall inform the controller of that legal requirement before processing, unless that law prohibits such notification as stated on Art. 28 (3)(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 Annex 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 immediately after completion of the contractual work – but at the latest upon termination of the Principal Agreement - the Processor shall, according to the Controller's specification, return and/or destroy or delete in accordance with data protection legislations all documents that are in the Processor's possession, results of processing, as well as datasets that contain personal data in the Controller's responsibility, unless there is a legal obligation to store 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 the right of retention in terms 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 Annex 1. Any changes shall be reported immediately to the Controller.

4. **Data secrecy.** The Processor is obliged to treat the data confidentially. The Processor shall not disclose any information to third parties or to data subjects without the Controller's prior written consent. The Processor shall comply with the provisions of the GDPR on the preservation of confidentiality in accordance with Art. 28 (3)(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. The monitoring measures must be described and presented to the Controller upon request.

6. **Compliance with operational regulations of the client**. The Processor commits to carry out the data processing in compliance with the guidelines, instructions and work agreements that apply to the Controller, insofar as the Processor has been informed of their content.

7. **Support to the Controller in the fulfilment of his 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 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 type of processing and the information available.

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

8. **Data breaches**. Personal data breaches or incidents that could lead to a personal data breach must be reported to the Controller without undue delay , at the latest however within 24 hours of becoming aware of the breach. The Processor shall inform of all 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. No later than 48 hours after becoming aware of it, the Processor must notify the Controller of the information required by Art. 33 (3) of the GDPR in such detail that the Controller is able to fulfil its obligation to notify the competent authority.

   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 Annex 1 section 8
- Controller's Data Protection Department (functional mailbox), Annex 1 section 12.

§ 4 - Place of processing

1. **Consent requirement for processing in a third country.** 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 prior written 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. Additional documents may be required as stated in Annex 1 section 7.

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 partly in a third country with poor data protection security, the relevant EU Standard Contractual Clauses will apply in relation to such processing. References to Directive 95/46/EC in the EU Standard Contractual Clauses shall be understood as references to the relevant and corresponding articles in the GDPR.

3. **Processing by subprocessors in a third country with poor data protection security.** If subprocessors within the meaning of § 7 (1) of this Agreement process data in a third country with poor data protection security, the Processor shall, in addition to the requirements set out in § 4 (1) of this Agreement, ensure the conclusion of the relevant EU Standard contractual Clauses between the Controller as data exporter and the subprocessors concerned as data importers before the start of the processing by these subprocessors. By signing this Commissioned Data Processing Agreement, the Controller authorizes the Processor to conclude the EU Standard Contractual Clauses with the subprocessors in the name and on behalf of the Controller. Upon request of the Controller, the Processor shall provide the Controller with a copy of the concluded EU Standard Contractual Clauses.

§ 5 - Liability

The Processor shall be liable to the Controller in the event of violations of data protection laws applicable to the Processor, in the event of other violations of the law and in the event of a breach of obligations arising from this Agreement (**"Breaches and Violations of Obligations"**) in accordance with the statutory provisions. The parties agree that fines imposed on the Controller as a result of violations and breaches of duty by the Processor are also included as compensable damages.

§ 6 - Technical and organizational measures for data security

1. **General information.** The Processor shall take the appropriate technical and organizational measures within the meaning of Art. 32 of the GDPR to ensure a level of protection appropriate to the risk arising from the processing of the data. The Processor is obliged to appropriately

document the collection, processing and use of data, on the basis of which the Controller can provide evidence of the proper use of data.

2. **TISAX certification**. The appropriate technical and organizational measures are to be documented and proven by a corresponding TISAX certification.

   The scope of the assessment and the necessary labels are determined based on the necessary degree of protection for fulfilling the contractually agreed services. The Processor shall carry out all the necessary technical and organisational measures for receiving the TISAX certification that it had stated in the process of certification, and, if applicable, further contractually agreed measures in Annex 2, , for the entire term of the contract, including after a possible loss of the TISAX certification. Furthermore and to the extent necessary, the Processor shall carry out further measures if this is necessary to ensure an adequate level of protection. The Processor shall document such further measures and provide the documentation upon the Controller's request.

3. **Special cases.** Exceptions from the obligation to present and implement a corresponding TISAX certification in accordance with section 2 are only permitted with the prior written consent of the Controller (here: Information security).

4. **Audit rights**. With regard to the Controller's audit obligations before the start of data processing and during the term of the agreement, the Processor shall ensure that the Controller is able to verify that the technical and organizational measures taken have been observed.

5. **Data processing in private homes**. The processing of the Controller's personal by the Processor or its contractual partners in private homes is only permitted if the Controller has been notified in advance and the Processor has ensured that all necessary technical and organizational measures are also taken in this working environment.

§ 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.

   For the purposes of this provision, subprocessing relationships are to be understood as those services that directly relate to the performing of the main service. This does not include auxiliary services that the Processor uses, e.g. telecommunications services, postal or transport services, maintenance and user services or the disposal of data carriers or other measures for ensuring the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Processor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Controller's personal data, even in the case of auxiliary services being outsourced.

2. **Subprocessors permitted at the time of conclusion of this Agreement**. The Processor is permitted to use the subprocessors listed in Annex 1.

3. **Other subprocessors**. The Controller must be informed immediately in writing or by e-mail of any intended assignment of further subprocessors or replacement of previous subprocessors. Subcontracting is only permitted with the prior consent of the Controller, which must be given in writing or by e-mail.The processing of data by the subprocessor is only permitted if all legal

requirements and those resulting from this Commissioned Data Processing 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 Commissioned Data Processing Agreement and the Principal Agreement.

5. **Controls by the Processor.** If the Processor carries out inspections at a subprocessor's premises, these must be documented and the documentation must be made available to the Controller upon request.

6. **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 checks - including inspections - 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 good 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 an instruction issued by the Controller could conflict with the applicable data protection laws. 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 authority.** Any investigations or actions taken by the data protection authority against the 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 personal data of the Controller is affected, the Processor shall notify the Controller immediately of any malfunctions, detected or suspected infringements to the applicable data protection laws 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 Commissioned Data Processing 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 Commissioned Data Processing Agreement continue to apply.

§ 11 - Miscellaneous

1. **Changes.** Changes to this Commissioned Data Processing Agreement must always be made in writing, unless otherwise specified in this Agreement.

2. **Adjustments.** Insofar as adaptations of this Commissioned Data Processing 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 Commissioned Data Processing 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. **Annexes.** Annexes 1 and 2 form an integral part of the agreement.

Annex 1	Description of Data Processing
Annex 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: _____

ANNEX 1 - Description of Data Processing

1. **Principal Agreement**

Principal Agreement within the meaning of § 1 section 1 of the Commissioned Data Processing Agreement:

Title: ……

Parties: ……

Date: ……

2. **Subject matter of the commission**

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

……

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

More detailed description of the subject matter of the commission in terms of scope, nature and purpose:

……

4. **Categories of data subjects concerned**

The following groups of data subjects are affected by the Commissioned Data Processing Agreement:

☐ **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 another 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

☐ **External parties.** 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 Agreement 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

☐ **IT usage data**

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, etc.

☐ **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, etc.

☐ **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 , etc.

☐ **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

☐ **Creditworthiness and other financial data, bank details**

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.

☐ **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. **Special instructions at the start of the agreement**

☐ Anonymization of certain data: …

☐ Prohibition of the disclosure of data: …

☐ Deletion of the data after every ... month

☐ …..

7. **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 a recognized 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, Switzerland and Uruguay

☐ Third country with poor data protection security: …..

If data processing takes place in a third country with poor data protection security, the following additional documentation is required:

☐ EU Standard Contractual Clauses for the transfer of personal data to processors or sub-processors in third countries, possibly supplemented by additional measures and obligations in accordance with the ECJ ruling of 16 July 2020 (C-311/18, "Schrems II")

☐ between the Controller and the Processor (if Processor in third country)

☐ between the Controller and the subprocessor (if subprocessor in third country)

or

☐ Consent of the data subjects

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

Name: ……

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

9. Responsible recipient of instructions for receiving instructions on behalf of the Processor

Name: ……

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

10. 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): ……

11. **Subprocessors**

☐ The Processor shall not employ subprocessors.

☐ The Processor employs the following subprocessors:

No.	Subprocessor (company, address, contact person)	Categories of data processed	Processing activity of the subprocessor	Processing in a third country with poor data protection security
---	---	----	---	---

12. **Notification of Data Breaches**

Functional mailbox of the Controller for reporting Data Breaches by the Processor:
……

13. **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.

ANNEX 2 - Technical and Organizational Security Measures

The technical and organizational security measures to be taken by the Processor are described in:

…

Additional technical and organizational security measures to be taken by the Processor:

☐ Especially protected transport of documents: …

☐ Special stipulations for using encryption techniques: …

☐ Special limitations for the group of persons with access authority: …

☐ ……