Agreement
Data Processing under Commission GDPR

between

1. **Data Controller**

Purchaser according to individual order of maintenance services

- hereinafter referred to as “Data Controller”-

and

2. **Data Processor**

ETAS GmbH

Borsigstrasse 24

70469 Stuttgart

- hereinafter referred to as “Data Processor”-

Preamble

The present Agreement specifies the obligations of the parties on data protection according to the order detailed in the individual order for maintenance services (referred to hereinafter as "Contract"). It is applicable to all activities connected to the Contract and in which employees of the Data Processor or Subprocessors of the Data Processor may process personal data ("data") of the Data Controller.

1. Subject matter, duration, and specification of contract data processing

1.1. The subject matter of contract data processing under commission is described in the Contract. Substantially, the Data Processor's tasks comprise the following:

- Support maintenance within the scope of service contract or warranty

1.2. The type and purpose of contract data processing under commission are described in the Contract and specifically comprise:

- Purpose of the data processing is the support of bug analysis and bug fixing

1.3. The processing comprises the categories of data specified below:

- Measurement files, protocol and other kind of files that are transferred to the Data Processor might contain personal data.
- The type of data is described in the handbooks of the product which is covered by this service contract and might include e.g.: IP addresses, user-ID, vehicle identification number, GPS- or video data.

1.4. The following categories of individuals are affected by the processing:

- Staff or agents of the Data Controller

1.5. The term of the present Agreement and the duration of the processing are determined by the term of the Contract unless obligations going beyond that date result from the provisions of the present Agreement.

1.6. Any services in connection with data processing under commission under this Agreement shall be rendered exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the Data Controller's prior agreement and is permitted only if the special requirements of Art. 44 et seqq. GDPR have been satisfied. An adequate level of protection in the third country:

☒ has been established by an adequacy decision by the Commission (Art. 45 (3) GDPR);

☒ is ensured by binding corporate rules (Art. 46 (2) lit. b) in conjunction with Art. 47 GDPR);

☒ is ensured by standard data protection clauses (Art. 46 (2) lit. c) and d) GDPR)

2. Scope of application and responsibility

2.1. The Data Processor processes personal data at the instruction of the Data Controller. This comprises activities as described in detail in the Contract and in the performance specification. Regarding to data processing under commission, the Data Controller is responsible for compliance with the statutory regulations on data protection and especially for the legitimacy of data processing.

2.2. At first, the instructions will be set forth in a contract and may subsequently be amended, supplemented, or replaced by the Data Controller in writing or in text form (single instruction) to the indicated persons of the Data Processor. Single instructions going beyond the services agreed in the contract, will be treated as a change request, and the Data Processor is entitled to request adequate financial compensation.

2.3. Any oral instructions shall be confirmed by the Data Controller without delay, at least in text form.

2.4. The Data Processor shall inform the Data Controller without delay if it is of the opinion that an instruction violates data protection rules. The Data Processor is entitled to suspend compliance with the instruction in question until it is either confirmed or changed by the Data Controller.

3. Obligations of the Data Processor

3.1. The Data Processor may process personal data of data subjects only within the scope of the assignment and the documented instructions of the Data Controller. If the Data Processor is obliged to process data differently because of national or European law, it shall point out the circumstance to the Data Controller before processing begins unless that law prohibits such information on important grounds of public interest.

3.2. The Data Processor shall set up the internal organisation of his area of responsibility in such a manner that it meets the specific requirements of data protection. The Data Processor shall take the technical and organizational measures described in **Appendix 1** to ensure an adequate protection of the Data Controller's personal data. The purpose of these measures is to ensure long-term confidentiality, integrity, availability and resilience of the systems and services in connection with the processing of personal data under commission. The Data Controller is informed of these technical and organizational measures. It is the Data Controller's responsibility to ensure that these measures provide an adequate level of protection regarding the risks of personal data processing.

3.3. The Data Processor reserves the right to change the technical and organizational measures taken but must guarantee that the level of protection agreed in the contract is not reduced.

3.4. To the best of his ability and within the scope of the services or under the contract, the Data Processor shall assist the Data Controller in dealing with requests and claims of data subjects according to chapter III of the GDPR and in respecting its obligations specified in Articles 32 to 36 GDPR. For these services, the Data Processor is entitled to adequate financial compensation.

3.5. The Data Processor warrants that its employees involved in the processing of the Data Controller's personal data and other individuals working for the Data Processor are prohibited from processing such personal data outside the scope of the Data Controller's instructions. The Data Processor further ensures that the individuals authorized to process personal data have signed an agreement of confidentiality or are subject to an adequate confidentiality clause. This obligation of confidentiality and secrecy shall remain in effect even beyond completion of an assignment.

3.6. The Data Processor shall inform the Data Controller without delay as soon as it becomes aware of any violation of the protection of the Data Controller's personal data. The Data Processor shall take the necessary measures to safeguard personal data and to alleviate possible disadvantageous consequences for the data subject and shall consult with the Data Controller in that respect without delay.

3.7. The Data Processor is obliged to appoint a competent and reliable Data Protection Officer according to Art. 37 GDPR to the extent and if the statutory prerequisites for such an obligatory appointment are in force. The Data Controller shall be informed of the contact data of this individual for the purpose of making direct contact. Any change of Data Protection Officer shall be communicated to the Data Controller without delay.

If the Data Processor is not obliged to appoint a Data Protection Officer, it shall give the Data Controller the name of the contact for any questions in relation to data protection that may arise in connection with the Agreement.

First contact for data protection issues:
Name: ETAS GmbH
Data Security Officer
ETAS/DSO
Address: Borsigstrasse 24, 70469 Stuttgart
E-Mail: office.etasisp@etas.com

And the contact data of the Data Protection Officer of the Data Processor:
Name: Robert Bosch GmbH
Data Protection Officer
Information Security and Privacy (C/ISP)
Anschrift: Post Office Box 30 02 20, 70442 Stuttgart
E-Mail: DPO@bosch.com

3.8. The Data Processor shall ensure that its obligations according to Art. 32 (1) lit. d) GDPR are complied with and put in place a process for regular examination of the effectiveness of the technical and organizational measures to ensure the safety of processing.

3.9. The Data Processor shall correct or erase personal data if instructed accordingly by the Data Controller and if this is a part of the scope of instructions. If appropriate erasure or a restriction of data processing is not possible, the Data Processor shall destroy any data carriers and other materials in accordance with the regulations of data protection based on a single instruction by the Data Controller unless this has already been agreed in the contract.

3.10. Personal data is an integrated part of measurements files or protocol data and transferred for bug analysis and bug fixing. Measurement files and protocol data can support the bug analysis in other support requests of the data Controller. The measurement files and protocol data are therefore deleted not before 5 years after closure of the dedicated support call. It is up to the Data Controller to make backup copies of its personal data. The Data Processor is not obliged to hand over personal data to which the Data Controller has direct access.

3.11. The Data Processor undertakes to maintain a record of data processing activities according to Art. 30 (2) GDPR.

4. Obligation of the Data Controller

4.1. It is the Data Controller's responsibility to provide the Data Processor with the personal data in due time to enable the latter to provide the services according to the Contract. The Data Controller is responsible for the quality of the personal data. The Data Controller shall inform the Data Processor immediately and completely in the event that it should identify any errors or irregularities with regard to data protection rules or in the performance of the Data Processor when checking the work results.

4.2. If claims should be made by a data subject in connection with Art. 82 GDPR, the Data Controller and the Data Processor undertake to assist each other in the defense against such claims.

4.3. The Data Controller’s contact for data protection issues regarding this processing as well as the data protection officer should be named when placing the order. In case of not naming someone, the Data Processor will use the contact person of the support call instead.

5. Enquiries from Data Subjects

If a data subject contacts the Data Processor demanding correction, erasure, restriction of processing or information about the personal data, the Data Processor shall refer the data subject to the Data Controller if allocation to the Data Controller is possible based on the information provided by the data.

6. Ways of verification

6.1. If requested, the Data Processor shall submit suitable proof to the Data Controller that the obligations set forth in Art. 28 GDPR and in the present Agreement are complied with. To proving compliance with the agreed obligations, the Data Processor may provide the Data Controller with certificates and third-party test results (e.g., according to Art. 42 GDPR or ISO 27001) or with test reports from the internal Data Protection Officer or any individual to whom this task has been assigned by the Data Protection Officer.

6.2. If spot checks by the Data Controller, or an auditor appointed by the Data Controller should turn out to be necessary in individual cases, these shall be conducted during regular business hours from Monday to Friday between 8 a.m. and 5 p.m. without disruption of operations and after an adequate notification period of at least 4 days. The Data Processor is entitled to make approval of such checks dependent on signing an adequate declaration of secrecy by the Data Controller or the auditor assigned by the Data Controller. If the auditor appointed by the Data Controller should be a competitor of the Data Processor, the Data Processor is entitled to object. Such objection shall be declared to the Data Controller in text form.

6.3. If an audit should be carried out by the data protection supervisory agency or another state authority, chapter 6.2 shall apply accordingly. Signing a confidentiality obligation is not required if the supervisory authority is subject to professional or statutory confidentiality any breach of which shall be penalized in accordance with the German Criminal Code.

6.4. The Data Processor is entitled to request adequate compensation for carrying out such an audit as per chapter 6.2 or 6.3, unless the reason for such an audit is the strong suspicion that a data protection breach has taken place within the scope of responsibility of the Data Processor. In such a case, details of the suspicion must be submitted by the Data Controller together with the notification of the examination.

7. Sub-Processors (additional contract data Processors)

7.1. The Data Controller agrees to the Data Processor involving Subprocessors. Before involving or replacing Subprocessors, the Data Processor shall inform the Data Controller directly either in written text or by the internet page of the data Processor (www.etas.com/AGB-ETASGmbH) within a four-week period in advance. The Data Controller may object to such a change only for important reason. Any objection must be lodged in writing within 14 days, and all reasons must be specified explicitly. If no objection is lodged within this time limit, consent to the involvement or replacement is deemed to have been given. If there is an important reason which cannot be eliminated by the Data Processor by adjusting the assignment, the Data Controller is granted an extraordinary right of termination. No separate information will be provided regarding the Subprocessors and their partial services than given in **Appendix 2** “Subprocessors Agreement Data Processing under Commission Maintenance” upon signature of the Agreement. If the Data Processor assigns any Subprocessors, it is up to the Data Processor to convey its obligations regarding data protection under the present Agreement to the Subprocessors.

7.2. Upon written request of the Data Controller, the Data Processor shall provide information regarding the data protection obligations of its Subprocessors at any time.

7.3. The provisions of this chapter 7 shall also apply if a Subprocessors in a third country is involved - observing the principles of Chapter 5 of the GDPR. The Data Processor agrees to cooperate to the required extend in meeting the prerequisites as set in Chapter 5 of the GDPR.

8. Liability

8.1. The limitations of liability under statutory law and the Contract are applicable.

8.2. The Data Controller shall indemnify the Data Processor against any claims lodged by third parties against the Data Processor because of the processing of personal data according to the instructions of the Data Controller unless the claim of such third party is based on processing the personal data by the Data Processor in violation of instructions.

9. Obligations of information, written form clause, choice of law

9.1. If the Data Controller's personal data processed by the Data Processor should be placed at risk because of seizure or confiscation, insolvency, or settlement proceedings or by other events or measures of a third party, the Data Processor shall inform the Data Controller without delay. In this connection, the Data Processor shall inform all third parties without delay that the control and ownership of the personal data exclusively lies with the Data Controller as "Controller", as defined in the GDPR.

9.2. Any amendments and additions to the present Agreement and its constituent elements – including any assurances granted by the Data Processor – shall be made in the form of a written agreement which may also be in electronic form and include an explicit reference that it is an amendment or addition to this Agreement. This shall also apply to the waiver of the requirements of this format.

9.3. In the event of contradictions, the regulations in this data protection Agreement shall take precedence over the regulations of the Contract. If individual regulations of the present Agreement should become invalid, the validity of the agreement as such shall not be affected.

9.4. This Agreement shall be governed by German law.

Appendix 1: Technical and organizational measures / security concept

The following TOMS are agreed between the Data Controller and the Data Processor

1. Measures to ensure confidentiality (Art. 32 para. 1 lit. b of the GDPR)

- Physical access control
  No unauthorized access to data processing systems, by using magnetic or chip smart cards, keys, electric doors opener, plant security or gatekeepers, alarm systems and partly video systems for securing the fence.
- Logical access control
  No unauthorized system usage due to binding regulations for secure passwords with implemented verification of minimum standards, binding regulations as well as implemented, automatic mechanisms for screen lock, encryption of data carriers and storage devices
- Data access control
  No unauthorized reading, copying, modification or removal within the system, due to defined authorization concepts and access rights, including regular checks.
- Separation control
  Data for the software maintenance services is managed separately from all other data of the data Processor and separately for each data Controller.

2. Measures to ensure integrity (Art. 32 para. 1 lit. b of the GDPR)

- Transfer control
  No unauthorized reading, copying, modification or removal during electronic transmission or transport, due to encrypted network and Virtual Private Networks (VPN)
- Input control
  Solely the data transferred by the data Controller for the respective support call within the scope of the software maintenance services is stored unchanged.

3. Measures to ensure availability and resilience (Art. 32 para. 1 lit. b of the GDPR), e.g.

- Availability Control
  Our IT systems and networks are protected against accidental or deliberate destruction or loss by various backup strategies, firewalls, virus protection and emergency scenarios.

- Order Control
  We use the data transferred by the Data Controller solely to support bug analyze and fixing of our software.
- Resilience
  Systems and services (e.g., storage, access, line capacities, etc.) are designed in such a way that even occasional high loads or high continuous loads of processing are ensured.

4. Measures for the pseudonymization of personal data:

- As far as possible, the Data Controller transfers anonymized or pseudonymized data. Further information how to anonymize or pseudonymize can be found at the manuals of our products
- The data transferred by the Data Controller will not be modified (see 2. Input control) and therefore could not be pseudonymized by the data Processor.

5. Measures for the encryption of personal data:

- Implemented only during the generation of configuration, measurement, or log files. Further information how to encrypt can be found at the manuals of our products.

6. Measures to quickly restore the availability of personal data to them a physical or technical incident:

- Our IT systems and networks are designed for rapid recovery using different backup strategies and IT infrastructure at different locations.

7. Procedures for periodical review, assessment, and evaluation (Art. 32 para. 1 lit. d of the GDPR; Art. 25 para. 1 of the GDPR):

- In addition to internal data protection management, we also have an internal incident response management.
- A data protection officer has been appointed and a worldwide data protection organisation has been set up.
- The processes are regularly checked by the internal data protection organization and the internal auditing.

Appendix 2: Subprocessors Agreement Data Processing under Commission Maintenance

See separate document