DRIVING EMBEDDED EXCELLENCE

Agreement
Data Processing under Commission GDPR

between

Data controller

Purchaser according to individual order of "Model Simulator"

- hereinafter referred to as "Data controller"-

and

Data processor

ETAS GmbH
Borsigstrasse 24
70439 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 *"Model Simulator"* (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:

- *Operation of Model Simulator including backend services in order to be able to process vehicle information like measurement data for simulation.*
- *Additionally to that over-the-air updates can be performed.*
- *Collected data can be exported on customer request.*

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

- *Identity and access management for users.*
- *Operations of the Model Simulator*

1.3 The processing comprises the categories of data specified below:

☒ Personal details: email-address, name, telephone

☒ Logging data/minutes: IP-address, User-ID, meta-data

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

☒ Staff including volunteers, agents, temporary and casual workers

☒ Customer and clients

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 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. With regard 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. In the event that the Data processor is obliged to process data differently as a result 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 organisational measures described in **Appendix 1** so as 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 organisational 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 organisational 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 authorised 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 as long as 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: Beate Winter
Address: Borsigstrasse 24, 70439 Stuttgart
E-Mail: Beate.Winter@etas.com
Telephone number: +49 (711) 3423-2679

And the contact data of the Data Protection Officer of the Data processor:

Name: Thoralf Knuth, Data Protection Officer, department for information security and privacy at Bosch group (C/ISP)
Address: Robert Bosch GmbH, P.O. 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 organisational 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 on the basis of a single instruction by the Data controller unless this has already been agreed in the contract.

3.10 The personal data shall be erased at the date of completion of the respective Contract. It is up to the Data controller to prepare backup copies of its personal data and to move such personal data before the end of the contract. 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. Obligations 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 so as 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 In the event that 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 defence against such claims.

4.3 The Data controllers 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 “Customer’s Cloud Administrator” 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 that request without delay to the Data controller if allocation to the Data controller is possible on the basis of the information provided by the data subject.

6. Ways of verification

6.1 If so 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. For the purpose of 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 In the event that 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 In the event that 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 penalised 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 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 subprocessor.

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 subprocessor 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 as a result 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 In the event that the Data controller's personal data processed by the Data processor should be placed at risk as a result 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

Data at rest

To protect the data at rest we have defined the data management and protection at rest requirements, such as encryption and data retention, to meet the organizational, legal, and compliance requirements. Encryption at rest protects our data from a system compromise or data ex-filtration by encrypting data while stored.

The following measures are implemented to secure the data at rest:

- Implement secure key management - Encryption keys are stored securely, and rotated with strict access control
- The AWS Key Management Service (KMS) is being used to use keys and policies to leverage encryption capabilities in AWS.
- Customer Master Keys (CMK) with defined key policies and permissions

Data in-transit

- Transfer control
  No unauthorized reading, copying, changing or removing during electronic transmission or transport, e.g.: encryption

- Input control
  Determination of whether and by whom personal data was entered, changed or removed in data processing systems, e.g.: logging, document management

TLS encryption for data in transit is enabled for all external communication outside of the AWS environment and also enabled internally as a defense in depth measure. This includes all Rest API and Messaging Queue communications.

The following measures are implemented to secure the data in transit:

- Encryption standards based on data classification to meet the organizational, legal, and compliance requirements.
- Implement secure key and certificate management: An extensive certificate management is imperative to encrypt and authenticate all the traffic from and to the system.
- encryption is enabled to/from message broker, database instances, permanent storage
- encryption is enabled between all the services and the load-balancer
- mTLS is enabled on the applicable endpints
- encryption is enabled in transit for all the logs

User Management and Access

- Logical access control
  No unauthorized system use, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, data encryption
- Data access control
  No unauthorized reading, copying, changing or removing within the system, e.g.: authorization concepts and user-specific access rights, logging of access

Enforced access control

- Enforcing the access control with least privileges and mechanisms, including backups, isolation and versioning to help protect the data at rest.
- Provide mechanisms to keep people away from data - It is made sure that we always keep maximum or all users away from directly accessing sensitive data.
- IAM: Identity and Access Management is the foundation of rights and role management. Through which we the concept of least privilege into the roles for users and services is achieved.
- MFA(Multi-factor Authentication) is configured for all users

Infrastructure Security

- For all publicly available services the use of a Web Application Firewall is enabled
- Systems and services (e.g. storage, access, line capacities, etc.) are designed in a way that even intermittent high stresses or high constant loads of processing can be ensured
- Anti-malware software is enabled on all nodes
- Inbound and outbound traffic to and from the solution network is restricted only to the required ports

Security Testing and Audits

- The platform is submitted to regular Pentesting.
- Security controls, limitations, network connections, and restrictions are regularly tested to assure conformance with applicable standards.
- Internal and external vulnerability scans are implemented
- Privacy management
- Incident response management
- Assessment by data protection department
- There is active monitoring on all elements that are part of the solution.

Appendix 2: Subprocessor of the Data processor

	Company name, direction of the subprocessor and nomination of possible data protection officer/contract partner for data protection questions	Content of assignment (Scope of the commission by the Data processor)	Place of data processing
1.	ESCRYPT GmbH	Organization of the 1st and 2nd level customer support as well as operation of IT-Service for the whole Cloud solution.	Wittener Straße 45, 44789 Bochum, Germany
2.	Robert Bosch Engineering and Business Solutions Private Limited	Organization of the 3rd level customer support.	123, Industrial Layout Hosur Road, Koramangala Bengaluru 560 095
3.	Amazon Web Services, Inc. & Amazon Web Services EMEA SARL	Organization of the cloud services. AWS is an external processor outside EU/EEA but data processing is within the EU (Region Frankfurt).	Frankfurt am Main