DRIVING EMBEDDED EXCELLENCE

Agreement
Data Processing under Commission GDPR

between

Data controller

Purchaser according to individual order of "Vehicle Management Solution"

- 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 *"Vehicle Management Solution"* (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 telematic services including an on-board-unit located in vehicles of the customer and backend services in order to be able to collect vehicle information like measurement data and diagnostic data.*
- *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:

- *Appropriation of vehicle measurement and diagnostic data.*
- *Storage of vehicle measurement and diagnostic data for a defined time range.*
- *Identity and access management for users.*

1.3 The processing comprises the categories of data specified below:

☒ Personal details: *email-address, name*

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

☒ Miscellaneous:

Meta-data: Description of vehicle configuration like on-board-unit id, vehicle ID (VIN) and software versions of the on-board-unit and ECUs.

Technical measurement data of the vehicle: Technical signals available in the vehicle network like e.g. velocity, pressure and odometer

Technical data of the on-board-unit: Operational data of the on-board-unit like log-files, mobile network connection information

Technical diagnostic data of the vehicle: Vehicle diagnostic data like diagnostic trouble codes

Geo-Positions of the vehicle

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

☒ Staff including volunteers, agents, temporary and casual workers

☒ Relatives, guardians, dependents, referees, trustees and other persons associated with the data subject

☒ 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

Confidentiality (Article 32 Paragraph 1 lit b GDPR)

Physical access control
Prevention of unauthorized persons from gaining access to personal data processing systems.

- Definition of individuals with access authorization
- Documented regulations for access control
- Need-based rights of access
- Access control facilities using a personalized and encoded ID card with photograph
- Obligation to carry an ID at all times
- Magnetic or chip cards
- Logging of access to server rooms (automatically by access control system or by designed lists)
- Biometric access control (for example to server rooms)
- Restrictive rules regarding keys
- Conventional locking system (ward keys)
- Different security zones
- Logging of system access events
- Visitors on the premises allowed only if accompanied by employees of the contract data processor
- Entrance security staff
- Door status monitoring for server room
- Construction measures (e. g. burglar resistant windows
- Documentation of the assignment or withdrawal of access authorizations
- Rights authorization concept
- Established control mechanisms (e. g. spot check documented regulations for access control of key management)
- Regulations for access of external individuals
- Compulsory wearing of authorization cards
- Identity check at the gatekeeper / reception
- Additional access control measures and monitoring the status of doors leading to server facilities
- Security locks
- Video surveillance in server room
- Video surveillance of entrances
- Video surveillance of datacenter
- Facility security services
- Monitoring emergency exits
- Automatic door pull-in device for entrance and exit in server rooms
- Alarm System / Intrusion Detection System
- Intrusion detection systems with direct alert to a permanently manned security control center or a police station

Logical access control
Prevention of personal data processing systems from being used without authorization.

- Password Policy (secure/complex passwords)
- Password regulations (e.g., regulations regarding the use of special characters, minimum length, regular change of the password)
- Defaults of the password management applications to use
- Authentication with user name / password
- Prohibition to pass on passwords
- Lockout in case of incorrect access attempts
- Periodic password changes
- Regular checks of access authorizations
- Segregation of duties regarding the assignment of user rights
- Blocking of workstation and/or user accounts after multiple incorrect log-ins
- Regular access authorizations check for user access to the network of Employees and Externals
- Automatic locking the screen in case of inactivity by time
- Isolation of internal networks by setting up firewall systems
- Regular conditional access checks for administrators of networks, network services, servers and risk identified applications
- Segmentation of networks
- Usage of on Virtual Private Networks (VPN) with user/password as authentication criteria and/or token as authentication criteria
- Encrypting smartphones
- Sealing off internal networks by installing firewall systems
- Intrusion-Detection-System
- Encryption of mobile devices (e. g. notebook)
- Anti-virus software (Client / Server)
- Hardware firewall
- Software firewall

Data access control
Ensuring that persons entitled to use a personal data processing system gain access only to such personal data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and subsequent storage, personal data cannot be read, copied, modified or deleted without authorization.

- Use of individualized and user related authorization information
- Number of administrations limited to the most necessary
- Defined authorization concepts
- Periodic control of user rights
- Logging of granted authorizations
- Logging of access to confidential data
- Documentation of the allocation of authorization
- Deletion of data before reuse of data carriers
- Privacy compliant disposal of data, data carriers and print outs
- Blocking of external interfaces

based on the security concept

Separation control
Ensuring that personal data collected for different purposes can be processed separately.

- Logical/technical data separation or internal multi-client capability
- Logical client data separation
- Access authorizations
- Separation of development,testing and production systems

Pseudonymization
Separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately by the customer.

- Pseydonomized identities for platform operator
- Data pseudonymised by customer can be stored in Systems; Bosch is unable to associate the data with a specific data subject without the assistance of additional data kept by the customer

Encryption
Measures to protect data against being processed by unauthorized persons

- Encryption of confidential data during transport and over data networks
- Training internal and external employees in handling encrypted personal data
- Encryption guidelines take into account the different protection categories of personal data
- Use of data encryption during data transfer to data center (if implemented by customer)
- Instructions for using coordinated and approved cryptographic techniques, algorithms, applications, and standards
- Secure data transmission (SFTP, VPN, TLS)
- Secrecy of the private keys of a certificate
- Deletion or destruction of keys no longer needed in a secure way
- Regular testing of the encryption processes (especially for safety gaps) and adjustment of such processes to the current technological developments (especially updating of the software used)

Integrity (Article 32 Paragraph 1 lit b GDPR)

Data transfer control
No unauthorized reading, copying, changes or deletions of data during electronic transfer or transport

- Use of virtual private networks (VPN)
- Secure data transmission (SFTP, VPN, TLS)

- Privacy compliant disposal of data, data carries and print outs based on the security concept
- Use of data encryption during data transfer to data center
- Documentation of the allocation of authorizations and roles
- Restriction of the authorized person group for transmission
- Documentation of the hardware and software in inventories and keeping an inventory register
- Controlled destruction of data carriers by certified disposal companies
- Electronic signature

Input control
Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted

- Legal form of contracts for the data processing of personal data with sub processors, including appropriate regulations for control mechanisms
- Procuring self-disclosures from service providers with regard to their implementing the data protection law

Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

Availability
Measures ensuring that personal data are protected against incidental destruction or loss.

- Central purchasing of software and hardware
- Regular backup-process or mirror hard disks, e.g. RAID-procedure
- Central procurement of hardware and software
- Data security concept with regular backups
- Backup strategy (online/offline; on-site/off-site)
- Redundant storage of personal data
- Regular data backup or use of redundancies
- Operating and regular testing of Uninterruptible Power Supply (UPS), emergency power, surge protection
- Uninterrupted electricity supply in server rooms
- IT supervision by qualified employees who are trained continuously
- Fire doors
- Early alert system for fire, water and high temperature in server rooms
- Early fire / smoke detection systems
- Storage of data media in different fire areas
- Alarm system in server rooms
- Fire extinguishers in server rooms
- Business Continuity planning
- Air conditioning system in server rooms
- Disaster recovery plan
- Two independent ways of access to the external network (Internet access through at least two different providers)
- Multilayer antivirus and firewall architecture
- Availability of backup computers and software solutions for emergency situations
- Virus protection
- Firewall

- Reporting procedure

Resilience
Measures to ensure permanent stress resistance of the systems and services

- Load-Balancing
- Regular training of the staff deployed (both management and other internal or external employees) to act in accordance with the requirements of integrity and confidentiality of data processing (at least once a year)
- Penetration tests

Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

Data protection management
Ensuring lawfulness, adequacy and effectiveness of data protection

- Internal audits by the relevant authorities (e.g. auditors, data protection officers, information security officers, process controls through quality management
- External audits by auditors, certification authorities with regard to ISO 27001
- Establishment of a data protection organization and data protection management
- Data protection concepts
- Data protection trainings for employees
- Communication channel for security incidents
- Internal and external test reports and evaluations
- Designation of data protection officer
- Internal data protection audits / checks

Control of observance of instructions
Ensuring that personal data are processed solely in accordance with the Instructions.

- Contractual agreement on supervisory and audit rights of controller
- Detailed written regulations (contract/agreement) of the assignment relationship and formalization of the entire sequence of the assignment including the use of sub-processors, clear regulations regarding competencies and responsibilities
- Contractual agreement with sub-processors to commit both internal and external staff to data secrecy
- Due diligence for supplier selection
- Contractor has appointed data protection officer
- Obligation of the contractor's employees to data secrecy

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.	Robert Bosch GmbH Connected Mobility Solutions	Organization of the whole customer support as well as provision of IT-Service for the whole Cloud solution via Corporate Sector Information Systems & Services	Hoferstraße 30, 71636 Ludwigsburg, Germany
2.	Bosch (South East Asia) Pte. Ltd	Provision of IT-Services in the field of ,,BICS-Services" (Bosch Internet of Things Cloud-Services) including but not limited to services in the field of Software as a Service, Platform as a Service und Infrastructure as a Service including hosting, monitoring, change management and support/trouble shooting, also including documentation of all operational proceedings for all services, applications or IT infrastructure provided to and/or used by Data Controller within the BICS-Services, whereas the possibility of access on personal data can, at least, not be excluded.	11 Bishan Street 21 (Opposite Raffles Institution), Singapore 573943
3.	Robert Bosch Engineering and Business Solutions Private Limited	Provision of IT-Services in the field of ,,BICS-Services" (Bosch Internet of Things Cloud- Services) including but not limited to services in the field of Software as a Service, Platform as a Service und Infrastructure as a Service including hosting, monitoring, change management and support/trouble shooting, also including documentation of all operational proceedings for all services, applications or IT infrastructure provided to and/or used by Data Controller within the BICS-Services. whereas the possibility of access on personal data can, at least, not be excluded.	No. 123 Industrial Lay- out Hosur Road, 560095 Bengaluru, India
4.	Bosch (China) Investment Ltd.	Provision of IT-Services in the field of ,,BICS-Services" (Bosch Internet of Things Cloud- Services) including but not limited to services in the field of Software as a Service, Platform as a Service und Infrastructure as a Service including hosting, monitoring, change man-	333 Fuquan Road North, Changning District, China

		agement and support/trouble shooting, also including documentation of all operational pro- ceedings for all services, applications or IT infrastructure provided to and/or used by Data Controller within the BICS-Services, whereas the possibility of access on personal data can, at least, not be excluded.	
5.	Robert Bosch Ltda.	Provision of IT-Services in the field of ,,BICS-Services" (Bosch Internet of Things Cloud- Services) including but not limited to services in the field of Software as a Service, Platform as a Service und Infrastructure as a Service including hosting, monitoring, change man- agement and support/trouble shooting, also including documentation of all operational pro- ceedings for all services, applications or IT infrastructure provided to and/or used by Data Controller within the BICS-Services, whereas the possibility of access on personal data can, at least, not be excluded.	Via Anhanguera Km 98- Bairro Boa Vista - Cl, Campinas - SP - CEP : 13065-900, Sao Paulo, Brazil
6.	Robert Bosch North America LLC	Provision of IT-Services in the field of ,,BICS-Services" (Bosch Internet of Things Cloud- Services) including but not limited to services in the field of Software as a Service, Platform as a Service und Infrastructure as a Service including hosting, monitoring, change man- agement and support/trouble shooting, also including documentation of all operational pro- ceedings for all services, applications or IT infrastructure provided to and/or used by Data Controller within the BICS-Services, whereas the possibility of access on personal data can, at least, not be excluded.	38000 Hills Tech Drive, Farmington Hills, Ml 48331, USA
7.	Robert Bosch Tool Corporation	Provision of IT-Services in the field of ,,BICS-Services" (Bosch Internet of Things Cloud- Services) including but not limited to services in the field of Software as a Service, Platform as a Service und Infrastructure as a Service including hosting, monitoring, change man- agement and support/trouble shooting, also including documentation of all operational pro- ceedings for all services, applications or IT infrastructure provided to and/or used by Data Controller within the BICS-Services, whereas the possibility of access on personal data can, at least, not be excluded.	1800 West Central Road, IL60056 Mount Prospect, USA
8.	EMC Deutschland GmbH	Services on an infrastructural level (operative system and near operative system ser-vices);Services, that use VMware products. This includes the virtualizing platform on sys- tem and network level, supervising and documentation systems and automation systems; automated processes, that have been implemented within the automation system. These processes enable BICS (Bosch Internet of Things Cloud-Services) customers to provide automated virtual Windows and Linux systems	Am Kronberger Hang 2A, 65824 Schwalbach am Taunus, Germany

		and Services on platform level. This in- cludes the runtime environment (Cloud Foundry) and the basic services, which are provided to BICS's customers in the market place.Operation of the services /processes includes: Supervision, change management and troubleshooting as well as, if necessary, documentation of the operation processes and instructions of procedure in operation manuals (runbooks}, whereas the possibility of access on personal data of the Data Controller can, at least, not be excluded.	
9.	Microsoft Deutschland GmbH	Technical support of Microsoft software related to Active Directory which is used for setting up and operating the BICS services whereas the possibility of access on personal data of the Data Controller can, at least, not be excluded	Konrad-Zuse-Strasse 1, 85716 Unterschleissheim, Germany
10.	retarus GmbH	Technical support of retarus software related to mailing services which is used for set- ting up and operating the BICS services whereas the possibility of access on personal data of the Data Controller can, at least, not be excluded.	Aschauer Strasse 30, 81549 München, Germany
11.	Bosch.IO GmbH (former Bosch Software Innovations GmbH)	Services in the field of the operation of BICS-Services (Bosch Internet of Things Cloud- Services), particularly Software as a Service, Platform as a Service and Infrastructure as a Service Services incl. supervision, change management and troubleshooting and documentation of operating processes for all provided or, if applicable, used services or applications and IT-infrastructure by the Data Controller, whereas the possibility of access on personal data can, at least, not be excluded	Ullsteinstraße 128, 12109 Berlin, Germany