DAIMLER

Agreement on Data Processing on behalf

between

(Please insert Controller)

- as Controller -

and

(Please insert Processor)

- as Processor -

Contact details	
Controller	
Name	
Zip code, town/city	
No., street, P.O. box no.	
Contact name	
- Tel.	
- Email	
Data Protection Officer / Coordinator	
- Tel.	
- Email	
Information Security Officer	
- Tel.	
- Email	
Processor	
Name	
Zip code, town/city	
No., street, P.O. box no.	
Contact name	
- Tel.	
- Email	
Data Protection Officer	
- Tel.	
- Email	
Information Security Officer	
- Tel.	
- Email	
Name of representative in the European Union[1]	
- Tel.	
- Email	

[1] Necessary, as far as the processor is not established in the European Union

Contents

Part 1: Contract ensuring Data Protection and Information Security

1.1 DESCRIPTION OF THE CONTRACT

1.1.1. The **subject matter of the Contract** is the processing of personal data by Processor on behalf of Controller and in accordance with Controller's instructions as part of the service described in the Main Agreement.

This Contract also applies *mutatis mutandis* to (remote) testing and maintenance of automated procedures or data processing systems if processing of personal data is part of the testing and maintenance task.

(Please describe the subject matter of the contract and the type of service that the Processor renders. You might refer to the Main Agreement, if existing, if it does include regulations regarding data processing)

1.1.2. The **term of this Contract** is the same as the term specified for the provision of the service agreed in the Main Agreement.

(Please specify contract term. In case a Main Agreement exists, and contract terms are identical, reference to the Main Agreement is possible)

1.1.3. **Types of personal data used**

Processor will have access to the following personal data:

(Please list relevant data types, e.g. name, address, user-ID etc.)

1.1.4. **Locations of data processing**

(Please list all the locations where personal data is being processed - for example data centers or offices - AND all locations from where (remote) access to personal data for testing and maintenance purposes takes place. Please specify the city and the country of the location)

1.1.5. **Scope, nature and purpose of processing** of personal data:

Processor shall provide the following services for Controller in relation to the data specified in subclause 3:

Please describe in further detail which data processing operations the Processor performs. Processing of personal data means almost any kind of handling of personal data, such as collection, adaption, retrieval, use or disclosure by transmission. Should this already be described in the Main Agreement, a reference to the Main Agreement may be used: e.g. "The persons concerned by the services are described under section ... of the Main Agreement")

1.1.6. The **group** of people (data subjects) **affected** by the handling of their personal data in the context of this Contract is as follows:

(Please describe in concrete terms whose data are affected by the service, e.g. employees of company XY , customer of service A, users of application B, drivers, suppliers, etc. Should this already be described in the Main Agreement, a reference to the Main Agreement may be used: e.g. "The persons concerned by the services are described under section ... of the Main Agreement")

1.2 NON-DISCLOSURE

1.2.1. Processor undertakes to treat as confidential all information – including, but not limited to, technical and commercial information, plans, findings, intelligence, designs, and documents – that becomes known to it or that it receives from Controller under this Agreement, not to disclose this information to third parties, to protect it from third-party access, to use it only for purposes in connection with this Agreement, and to disclose it only to employees who are themselves under an obligation to observe confidentiality, unless otherwise agreed in writing between the Parties.

1.2.2. This confidentiality undertaking shall not apply in respect of information

- that can be proven to have been known to Processor before this Agreement came into effect,
- that can be proven to have been lawfully obtained by Processor from a third party without being subject to a confidentiality obligation,
- that is already in the public domain or that enters into the public domain without any infringement of the obligations under this Agreement,
- that can be proven to have been developed by Processor during the course of its own independent work.

1.2.3. As far as the Controller is a financial services company and is obliged to observe requirements of banking secrecy, the same requirements shall apply to the Processor.

1.2.4. Processor agrees to impose upon its employees to whom this information is disclosed the same duty of confidentiality as Processor has entered into above unless these employees are already subject to an equivalent non-disclosure obligation by virtue of their contracts of employment.

1.2.5. If notified of any development results that are capable of being protected by intellectual property rights, the Parties reserve all rights in respect of any such property rights subsequently applied for or granted.

1.2.6. The non-disclosure obligations in respect of information that has been made available during the term of this Agreement shall continue to apply for a period of five years after the Agreement has ended.

1.3 PROCESSING UNDER THE AUTHORITY OF THE CONTROLLER

1.3.1 Processor processes personal data on behalf of Controller. Controller is responsible for complying with the provisions of applicable data protection law.

1.3.2. Processor shall follow solely the instructions issued by Controller when processing personal data. Such instructions must be given in writing or by electronic mail. Other than as instructed by Controller, Processor may not use, either for its own purposes or the purposes of third parties, the data to which it has been given

access for processing or use, or the data it has collected under this Agreement. In accordance with the instructions issued by Controller, Processor must amend, delete, or block the data it is processing on behalf of Controller. The Processor shall inform the Controller if, in its opinion, an instruction infringes applicable data protection provisions.

1.4 OBLIGATIONS OF THE PROCESSOR

1.4.1. Processor shall assist Controller in satisfying the rights of the persons whose personal data is processed (data subjects), which may include rights of access, rectification, restriction of processing, objection, erasure, and data portability regarding their data. If a data subject contacts Processor directly to ask for information or request to have his/her personal data being corrected, deleted, or blocked, Processor shall forward this request to Controller without delay.

1.4.2. Processor undertakes to provide data protection training for its employees entrusted with the processing of the data provided by Controller and to impose on such employees an obligation to observe data secrecy (obligation not to disclose personal data).

1.4.3. Processor must provide Controller with the details of contacts for data protection and information security. If Processor is subject to a statutory obligation to appoint a data protection officer, Processor shall appoint such an officer in writing and shall send Controller the name(s) of the person(s) concerned.

1.4.4. Upon request, Processor shall provide Controller with the information necessary to enable Controller to satisfy notification obligations, maintaining records of processing activities, or performing a data protection impact assessment.

1.4.5. Processor remains, to an unlimited amount, fully liable to the Controller for culpable infringements of regulations of this Agreement and of applicable data protection provisions.

1.4.6. Controller may at any time instruct the immediate erasure of the data processed under this Agreement. Upon request, and regardless to the afore-mentioned provision, the Processor is under the obligation to surrender the data in a generally readable format. If the data is deleted, action must be taken to ensure that the data cannot be reconstructed. Processor shall prove to Controller and confirm in writing, including in electronic form, that all the data, copies and storage media have been returned and deleted. As far as binding legal requirements do not allow the erasure of contractual data or data categories the Processor must inform the Controller about such requirements.

1.4.7. Processor must store Controller's data for a period of six months, even after the relevant service agreement has ended. Within this six-month period, the data must be returned in a generally readable format or, if instructed, deleted.

1.4.8. In case Processor's company or major parts of the company are purchased by a third party or if a third party purchases the majority of the shares or voting rights, Controller has the right to terminate this agreement extraordinarily.

1.5 SUBCONTRACTORS

1.5.1. If Processor involves subcontractors or freelancers it must first obtain the prior consent of Controller in writing, including electronic form. The contractual arrangements between Processor and the subcontractor or freelancer must be drafted in such a way that they correspond with the arrangements contained in the contractual relationship between Controller and Processor. In particular, Processor must ensure that Controller can also carry out the checks specified in clause 1.7 of this Contract in respect of the subcontractors or freelancers. Controller is entitled to receive information from Processor concerning the essential contractual provisions and the implementation of the obligations in this Contract – if necessary by means of inspecting the relevant contract documents.

1.5.2. Controller is deemed to have consented to the involvement of the subcontractors and functions listed in Part 3 when Controller signs this Agreement. Processor must ensure that these subcontractors comply with the technical and organizational requirements specified in Part 2 in the same way as Processor itself. If subcontractors are replaced or added during the course of the contractual relationship, Processor must first obtain the consent of Controller in writing, including electronic from.

1.6 INFORMATION SECURITY

1.6.1. Processor undertakes, as part of an information security concept, to use state of the art technology to safeguard all Controller's information and data immediately and effectively against unauthorized access, modification, destruction or loss, unauthorized transfer, other unauthorized processing, and other misuse. The security concept must be described in detail by completing the fields in Part 2. Processor shall agree its information security concept with Controller's relevant information security officer. For the purpose of completing part 2, the adherence of the Processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate sufficient technical and organizational measures. The demonstration of such code of conduct or certification does not replace a case-by-case assessment. Is one of those elements used to demonstrate sufficient technical and organizational measures, the element shall be attached to this Agreement.

1.6.2. Processor may only authorize access to Controller's data for its own employees in accordance with the authorization rules and only to the extent necessary to allow the employee concerned to carry out the relevant task in connection with fulfillment of contractual requirements. If it is necessary to issue access authorizations to employees of subcontractors or to freelancers to facilitate fulfillment of this Agreement, this can only be done with the prior consent of Controller in writing or by electronic mail and only to the extent necessary for the task concerned. Upon request, Processor must supply Controller with the names of persons or groups of persons to whom access authorization has been granted. Processor undertakes not to disclose to any unauthorized person the access authorizations granted to enable Processor to use the system.

1.6.3. If Processor is granted access to the IT systems of Controller, its representatives, or subcontractors, Processor undertakes only to access the data and information necessary to enable it to satisfy its obligations under this Agreement

1.6.4. The Processor must ensure that the technical and organizational described in Part 2 are implemented before data processing begins and that the associated activities are regularly reviewed and adjusted.

1.6.5. Processor must inform the Controller's information security officer in writing, including electronic form, if there are any material changes to data processing. In the event of any foreseeable reduction in the effectiveness of the data protection, the consent of Controller must be obtained in writing, including electronic form, before the related change is carried out.

1.7 CHECKS

1.7.1. Controller or its representatives have the right to carry out checks on compliance with the requirements of this Agreement. Processor shall provide the desired information and, upon request of Controller and within a reasonable period, submit documentary evidence that it has met its obligations by completing a questionnaire supplied by Controller.

1.7.2 Subject to advance notice, Controller or its representative shall be granted access to the offices and IT systems in/on which Controller's data is used or processed so that the implementation of the contractual agreements and the appropriateness of the technical and organizational data security measures can be verified.

1.7.3. Processor must inform Controller without delay should any suspicion arise that there has been a personal data breach or a breach of banking secrecy, in order to enable the Controller to make a notification of the breach within 72 hours to the supervisory authority. In consultation with Controller, Processor must initiate all necessary steps to rectify the problem and prevent further personal data breaches.

1.7.4. Processor informs Controller without delay about checks of supervisory authorities which take place in Processor's company or within used IT infrastructure and where Controller's personal data is being processed. In case Controller's data held by Processor is placed at risk as a result of seizure, distraint, judicial inquiries, or other enforcement actions by authorities, as a result of insolvency or composition proceedings, or as a result of other events or action taken by third parties, Processor must inform Controller without delay. Processor shall inform all parties involved in any such action without delay that the power of control over the data subject to this Agreement lies with Controller and shall not transfer any data to third parties or allow access to the data by third parties without the consent of Controller. If Processor is sworn to secrecy as a result of a control, access or other measures taken by a party authorized to access data, he has the duty to take any action to stop those controls and to nullify the secrecy obligation.

1.8 DATA PROCESSING IN A NON-EEA COUNTRY

1.8.1 Additionally to this Agreement, Processor or its subcontractor who processes personal data emanating from the European Union (EU), outside the European Economic Area (EU member states together with Iceland, Liechtenstein, Norway) or outside a country recognized by the European Commission as having an appropriate level of data protection, or if Processor or its subcontractor accesses EU-sourced personal data from outside the countries specified above

- Controller must sign a written agreement with Processor or its subcontractor to include the EU's standard contractual clauses governing Data Processing on Behalf in non-EEA countries, or
- the data processing must be subject to binding rules and regulations that have been put in place by Processor and are recognized by a relevant regulatory authority as providing a sufficient basis for creating an appropriate level of data protection within the meaning of EU law.

1.8.2. In the case of personal data that emanates from countries other than those specified in subclause 1 and that also gives rise to requirements under data protection law in respect of data processing abroad, appropriate measures must be implemented in accordance with provisions under national law.

Part 2: Data Protection and Information Security Measures

This part must be used to document the technical and organizational measures implemented in order to safeguard the security of data processing activities. It must be clearly stated whether the action concerned is taken by Controller (Co) or by Processor (Pr). There is no requirement to implement all the action points listed below; the parties need to ensure that the overall level of protection is appropriate in each case.

The adherence of an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate sufficient technical and organizational measures. The demonstration of such code of conduct or certification does not replace a case-by-case assessment. If one of those elements is used to demonstrate sufficient technical and organizational measures, the element shall be attached to this Agreement.

2.1 Access control (physical)

Definition: Physical access control means the action taken to deny unauthorized persons physical access to locations and areas in which personal data is being processed.

2.1.2 Who holds overall responsibility for implementing and ensuring compliance with physical access control?

◯ *Controller* ◯ *Processor*

2.1.2 What action is taken to implement physical access control and who carries out this action? (Please select appropriate answers and mark with a cross, as applicable)

	Co	Pr
• *Specification of authorized persons, including scope of authority*	☐	☐
• *Admittance authorization IDs issued*	☐	☐
• *Rules and regulations for visitors in place*	☐	☐
• *Rules and regulations governing keys implemented*	☐	☐
• *All individuals recorded in and out*	☐	☐
• *Physical protection measures in place and regularly checked:*		
o *Secure entrance (e.g. locking system, ID readers)*	☐	☐
o *Burglar-resistant windows*	☐	☐
o *Equipment secured against theft, manipulation, damage*	☐	☐
o *Surveillance installation (e.g. alarm system, CCTV)*	☐	☐
o *Separation system (e.g. turnstiles, double-door system)*	☐	☐

- *Security guards* ☐ ☐
- *Areas divided into different security zones* ☐ ☐

2.1.3 Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.1.4. If physical access control is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.2 ACCESS CONTROL (SYSTEMS)

Definition: Systems access control means the action taken to prevent unauthorized persons from using data processing systems.

2.2.1. Who holds overall responsibility for implementing and ensuring compliance with systems access control?

◯ *Controller* ◯ *Processor*

2.2.2. What action is taken to implement systems access control (user identification and authentication) and who carries out this action? *(Please select appropriate answers and mark with a cross, as applicable)*

	Co	Pr
• *Authorization concept designed and implemented*		
o *Authorization concept for terminal devices (computers)*	☐	☐
o *Authorization concept for systems*	☐	☐
• *User identified and authorization verified*	☐	☐
• *User identity management system implemented*	☐	☐
• *Access attempts monitored, including response to security issues*	☐	☐

- *Access authority specified and checked* ☐ ☐
- *Authentication procedure based on required level of protection for the information (classification)* ☐ ☐
- *Appropriate password protection (binding requirements, encrypted storage)* ☐ ☐
- *Special security software (e.g. anti-malware, VPN, firewall)* ☐ ☐
- *Rules and regulations for visitors in place* ☐ ☐
- *Access function using tokens* ☐ ☐

2.2.3. Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.2.4. If systems access control is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.3 ACCESS CONTROL (USER RIGHTS)

Definition: Access control (user rights) comprises the action taken to ensure that the persons authorized to use a data processing system can only access the data corresponding to their access authorization and that personal data cannot be read, copied, amended, or removed without authorization during processing or use, or after the data has been saved.

2.3.1. Who holds overall responsibility for implementing and ensuring compliance with access control (user rights)?

◯ *Controller* ◯ *Processor*

2.3.2. What action is taken to implement access control (user rights) and who carries out this action? *(Please select appropriate answers and mark with a cross, as applicable)*

	Co	Pr
• *Authorization and roles concept implemented for applications*	☐	☐
• *Rules and regulations for authorizing users and data access implemented*	☐	☐
• *Regular review of authorizations*	☐	☐
• *Functions restricted (in terms of function and time)*	☐	☐
• *Access restrictions imposed (based on principles of need-to-know and least privilege)*	☐	☐
• *Encrypted storage of personal data*	☐	☐
• *Logging*		
o *Read-access logged*	☐	☐
o *Write-access logged*	☐	☐
o *Unauthorized access attempts logged*	☐	☐
o *Regular analyses carried out*	☐	☐
o *Ad hoc analyses carried out*	☐	☐
• *Implementation of retention periods for data*	☐	☐
• *Rules and regulations on handling digital storage media implemented*	☐	☐
• *Rules and regulations on disposing of storage media implemented*	☐	☐
• *Integrity checks carried out*	☐	☐
• *Separation of test and productive environment*	☐	☐

2.3.3 Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.3.4. If access control (user rights) is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.4 DISCLOSURE CONTROL

Definition: Disclosure control refers to the action taken to ensure that personal data cannot be read, copied, amended, or removed without authorization during electronic transmission, during storage on data media, or during transit on such media, and to ensure that it is possible to establish and review the points at which it is envisaged it will be necessary to transfer personal data using data transfer facilities.

2.4.1. Who holds overall responsibility for implementing and ensuring compliance with disclosure control?

◯ *Controller* ◯ *Processor*

2.4.2. What action is taken to implement disclosure control and who carries out this action?
(Please select appropriate answers and mark with a cross, as applicable)

	Co	Pr
• *Forms of data forwarding fully documented (e.g. printout, data media, automated transfer)*	☐	☐
• *Data recipients listed (enter under c))*	☐	☐
• *Interfaces, retrieval and transmission programs documented*	☐	☐
• *For printouts and data media:*		
o *Regular inventory checks carried out*	☐	☐
o *Transit security measures implemented (e.g. containers, encrypted storage media, handover records)*	☐	☐
• *For electronic forwarding:*		
o *Data transfer encrypted*	☐	☐
o *Data forwarding or transfer logged*	☐	☐

- *Plausibility, completeness, and accuracy checks carried out*..... ☐ ☐

- *Action taken to prevent uncontrolled information outflow:*
  - o *USB interface deactivation* ☐ ☐
  - o *Restriction of rights for data transfer* ☐ ☐
  - o *Regular checks on permitted recipients* ☐ ☐
  - o *Forwarding restricted to permitted recipients by technical measures* ☐ ☐

2.4.3. Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.4.4. If disclosure control is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.5 INPUT CONTROL

Definition: Input control refers to the action taken to ensure that retrospective checks can be carried out to establish whether personal data in data processing systems has been entered, modified, or removed and, if so, by whom.

2.5.1. Who holds overall responsibility for implementing and ensuring compliance with input control?

◯ *Controller* ◯ *Processor*

2.5.2. What action is taken to implement input control and who carries out this action?
(Please select appropriate answers and mark with a cross, as applicable)

	Co	Pr
• *Inputs/Changes logged*	☐	☐
• *Regular review of logs*	☐	☐
• *Inputting responsibilities specified in organizational structure*	☐	☐

2.5.3. Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.5.4. If input control is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.6. JOB CONTROL

Definition: Job control means the action taken to ensure that personal data being processed on behalf of Controller can only be processed in accordance with the instructions issued by Controller.

2.6.1. Who holds overall responsibility for implementing and ensuring compliance with job control?

◯ *Controller* ◯ *Processor*

2.6.2. What action is taken to implement job control and who carries out this action?
(Please select appropriate answers and mark with a cross, as applicable)

	Co	Pr
• *System implemented for regularly checking the commissioning process*		
o *Submission of self-assessments*	☐	☐
o *Submission of agreements with subcontractors*	☐	☐
o *Checks on subcontractors by Processor*	☐	☐

2.6.3. Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.6.4. If job control is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.7. AVAILABILITY CONTROL

Definition: Availability control means the action taken to ensure that personal data is protected against accidental destruction or loss.

2.7.1. Who holds overall responsibility for implementing and ensuring compliance with availability control?

○ *Controller* ○ *Processor*

2.7.2. What action is taken to implement availability control and who carries out this action?
(Please select appropriate answers and mark with a cross, as applicable)

	Co	Pr
• *System condition regularly checked (monitoring)*	☐	☐
• *Backup and recovery plan in place (regular data backups)*	☐	☐
• *Data archiving strategy implemented*	☐	☐
• *Documented contingency plans (business continuity, disaster recovery)*	☐	☐
• *Contingency plans regularly tested*	☐	☐
• *Presence of redundant IT systems assessed (servers, storage, etc.)*	☐	☐
• *Fully operational physical protection systems in place (fire protection, energy, A/C)*	☐	☐

2.7.3. Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.7.4. If availability control is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.8. SEGREGATION PRINCIPLE

Definition: The segregation principle requires the implementation of measures to ensure that data collected for different purposes can be processed separately.

2.8.1. Who holds overall responsibility for implementing and ensuring compliance with the segregation principle?

◯ *Controller* ◯ *Processor*

2.8.2. What action is taken to implement the segregation principle and who carries out this action? (Please select appropriate answers and mark with a cross, as applicable)

	Co	Pr
• *Segregation of functions documented*	☐	☐
• *Policies and procedural instructions in place*	☐	☐
• *Procedure documentation in place*	☐	☐
• *Multi-client capability:*		
o *Physical separation*	☐	☐
o *Separation at system level*	☐	☐
o *Separation at data level*	☐	☐
• *Regular checks carried out to ensure fully compliant use of information and IT systems*	☐	☐

2.8.3. Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.8.4. If the segregation principle is not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

2.9. ORGANIZATIONAL SECURITY CRITERIA

Definition: The organizational security criteria are the rules and processes used to protect personal data.

2.9.1. Who holds overall responsibility for implementing and ensuring compliance with the organizational security criteria?

☐ *Controller* ☐ *Processor*

2.9.2. What action is taken to implement the organizational security criteria and who carries out this action? (Please select appropriate answers and mark with a cross, as applicable)

	Co	Pr
• *Data protection responsibilities fixed in writing*	☐	☐
• *Information security responsibilities fixed in writing*	☐	☐
• *Appropriate information security management system in place*	☐	☐
• *Appropriate incident management system in place*	☐	☐
• *Information classification system implemented*	☐	☐

- *Clarification and awareness sessions regularly carried out for employees and managers*..... ☐ ☐

2.9.3. Please use the following field (free text) for details of additional or other measures you have implemented or if you would like to provide more specific information on the above items:

(Please use additional sheet if necessary.)

2.9.4. If organizational security criteria are not relevant to the services subject to this Agreement, please briefly state the reasons below:

(Please use additional sheet if necessary.)

Part 3: Approved subcontractors

Subcontractor name, address (1)	
Name	
Zip code, town/city	
No., street, P.O. box no.	
Country	
Data protection contact	
Information security contact	

Brief description of the function carried out by this subcontractor:

Subcontractor name, address (2)	
Name	
Zip code, town/city	
No., street, P.O. box no.	
Country	
Data protection contact	
Information security contact	

Brief description of the function carried out by this subcontractor:

(Provide details for any further subcontractors)

Processor shall ensure that the subcontractors listed above are contractually bound by the obligations specified in Part 1 and have implemented the technical and organizational measures in accordance with the specifications in Part 2 or can furnish proof that they have been awarded suitable certification (for example, ISO 2700x).

Part 4: Signatures

Note: This part is only to be filled out, if applicable legislation or internal regulations demand hand-written signatures of the parties. Otherwise this document is valid without a hand-written signature. The written form, including the electronic form, is sufficient.

Name Controller	**Name Controller**
Place, date	**Place, date**
Controller signature(s)	**Controller signature(s)**

Name Processor	**Name Processor**
Place, date	**Place, date**
Processor signature(s)	**Processor signature(s)**

Daimler AG
Mercedesstr. 137
70327 Stuttgart
Germany
www.daimler.com