DAIMLER

AGREEMENT ON DATA PROCESSING ON BEHALF

between

Controller

- as Controller -

and

Processor

- as Processor -

Contact details	
Controller	
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	
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	

Contents

PART 1: CONTRACT ENSURING DATA PROTECTION AND INFORMATION SECURITY

1 DESCRIPTION OF THE CONTRACT

(1) The **subject matter of the Contract** is the collection, processing, and use 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 [1]) testing and maintenance of automated procedures or data processing systems if it is not possible to rule out access to personal data when such work is carried out.

(reference Main Agreement; describe the subject matter of the contract, if there is no Main Agreement or if the Main Agreement does not include regulations regading data processing)

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

name the duration of the contract if there is no Main Agreement or should it not contain any such information

(3) **Type of personal data used**

Processor will have access to the following personal data:

Please list relevant data eg name address etc

(4) **Scope, nature, and purpose involved in collecting, processing, and/or using** personal data:

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

(Please describe in concrete terms which services the Processor shall provide in connection with the Data Processing on Behalf. If these services are already described in the Main Agreement, a reference to the Main Agreement may be used: e.g. "Procesor provides the services as described under section ... of the Main Agreement")

[1] Remote access

(5) 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. employee data, customer data, supplier data, 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")

2 Non-Disclosure

(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 only to disclose it to employees who are themselves under an obligation to observe confidentiality, unless otherwise agreed in writing between the Parties.

(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.

(3) 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.

(4) 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.

(5) 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.

3 Data Protection

(1) Processor collects, processes, and uses personal data on behalf of Controller. Controller is responsible for complying with the provisions of data protection law.

(2) Processor shall follow solely the instructions issued by Controller when collecting, processing, and using 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. In accordance with the

instructions issued by Controller, Processor must amend, delete, or block the data it is processing on behalf of Controller.

(3) Processor shall assist Controller in satisfying the rights of the persons whose personal data is stored (data subjects), which may include correcting, deleting, blocking, or providing information about such data. If a data subject contacts Processor directly to ask for information or request that his/her personal data be corrected, deleted, or blocked, Processor shall forward this request to Controller without delay.

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

(5) 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.

(6) Upon request, Processor shall provide Controller with the information necessary to enable Controller to satisfy reporting obligations and maintain a systems and procedures overview.

(7) Processor shall inform Controller without delay of any checks or action taken by the relevant regulatory authorities in its organization or in connection with the IT infrastructure it uses.

4 INFORMATION SECURITY

(1) Processor undertakes, as part of an information security strategy, 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 strategy must be described in detail by completing the fields in Part 2. Processor shall agree its information security strategy with Controller's relevant information security officer. Part 2 need not be completed if Processor has suitable certification (for example, in accordance with ISO 2700x) covering the services that form the subject matter of this Contract. In this case, a reference to the certification must be inserted and the certification attached as an annex to this Agreement. If this certification becomes invalid and re-certification is not obtained within a reasonable period, this Agreement and the Main Agreement may be terminated by Controller.

(2) 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. 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 or by electronic mail that all the data, copies, and storage media have been returned and deleted. Controller may at any time specify an earlier date for data deletion. Regardless of this provision, Processor shall be under an obligation to surrender the data in a generally readable format at any time upon request by Controller.

(3) Processor must ensure that the technical and organizational measures described in Part 2 are implemented before data processing begins and that the associated activities are regularly reviewed and adjusted. Processor must inform Controller in writing or by electronic mail 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 or by electronic mail before the related change is carried out.

5 Subcontractors and Access Control

(1) If Processor involves subcontractors or freelancers it must first obtain the prior consent of Controller in writing or by electronic mail. 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 6 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.

(2) Controller is deemed to have consented to 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 or by electronic mail.

(3) 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 contractual requirements, 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.

(4) 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.

6 Checks

(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, at the request of Controller and within a reasonable period, submit documentary evidence that it has met its obligations by completing a questionnaire supplied by Controller.

(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.

(3) Processor must inform Controller without delay should any suspicion arise that there has been a violation of data protection requirements (in particular, unlawful forwarding of Controller's data to third parties or

unlawful access by third parties to Controller's data), a breach of security, or other manipulation during data processing. In consultation with Controller, Processor must initiate all necessary steps to rectify the problem and prevent further data protection and/or security violations.

(4) If Controller's data held by Processor is placed at risk as a result of seizure, distraint, judicial inquiries, or other enforcement of legal control by relevant 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.

7 Data Processing in a Non-EEA Country

(1) If Processor or its subcontractor 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 come to 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
- Processor must participate in a certification system recognized by the EU and satisfy the requirements of this system, 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.

(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 STRATEGY

This section 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 or by Processor. There is no requirement to implement all the action points listed below; the parties need to ensure that there is an appropriate level of protection from an overall perspective in each case.

Completion of this section may be replaced by documentary evidence of suitable certification (for example, in accordance with ISO 2700x) provided that the certification covers the services involved. In this case, a copy of the certification must be attached to the Agreement documents.

1. Access control (physical)

Definition: Physical control means the action taken to deny unauthorized persons physical access to data processing systems in which personal data is processed or used.

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

○ *Controller* ○ *Processor*

b) 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. lockable doors, 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)*	☐	☐
o *Security guards*	☐	☐

- *Areas divided into different security zones*..... ☐ ☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

2. Access control (systems)

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

a) Who holds overall responsibility for implementing and ensuring compliance with user systems access control?

◯ *Controller* ◯ *Processor*

b) 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)* ☐ ☐
- *Encryption implemented* ☐ ☐
- *Appropriate password protection (code of conduct, encrypted archives)* ☐ ☐
- *Special security software (e.g. anti-malware, VPN, firewall)* ☐ ☐
- *Rules and regulations for visitors in place* ☐ ☐
- *Access function using tokens* ☐ ☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

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.

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

○ *Controller* ○ *Processor*

b) 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*	☐	☐
• *Authorizations reviewed*	☐	☐
• *Functions restricted (in terms of function and time)*	☐	☐
• *Access restrictions imposed (based on principles of need-to-know and least privilege)*	☐	☐
• *Data stored with encryption*	☐	☐
• *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*	☐	☐
• *Rules and regulations on data deletion implemented*	☐	☐
• *Rules and regulations on handling digital storage media implemented*	☐	☐
• *Rules and regulations on disposing of storage media implemented*	☐	☐
• *Integrity checks carried out*	☐	☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

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.

a) Who holds overall responsibility for implementing and ensuring compliance with disclosure control?

○ *Controller* ○ *Processor*

b) 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 disclosure 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 disclosure:*		
o *Data transfer encrypted*	☐	☐
o *Data disclosure or transfer logged*	☐	☐
• *Plausibility, completeness, and accuracy checks carried out*	☐	☐

- *Action taken to prevent uncontrolled information outflow*

  (e.g. USB interface deactivation, regular checks on permitted

  recipients, forwarding restricted to permitted recipients by technical measures)..... ☐ ☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

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.

a) Who holds overall responsibility for implementing and ensuring compliance with input control?

○ *Controller* ○ *Processor*

b) 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 logged and logs reviewed*	☐	☐
• *Inputting responsibilities specified in organizational structure*	☐	☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

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.

a) Who holds overall responsibility for implementing and ensuring compliance with job control?

◯ *Controller* ◯ *Processor*

b) 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 service process (e.g. submission of self-assessments, submission of agreements with subcontractors, implementation of checks on subcontractors by Processor)*	☐	☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

7. Availability control

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

a) Who holds overall responsibility for implementing and ensuring compliance with availability control?

○ *Controller* ○ *Processor*

b) 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*	☐	☐
• *Contingency plans in place (business continuity, disaster recovery plans)*	☐	☐
• *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)* ..	☐	☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

8. Segregation principle

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

a) Who holds overall responsibility for implementing and ensuring compliance with the segregation principle?

○ *Controller* ○ *Processor*

b) 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*	☐	☐
• *Live and test systems separated*	☐	☐
• *Regular checks carried out to ensure fully compliant use of information and IT systems*	☐	☐

c) 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 an additional sheet if necessary)

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

(Please use an additional sheet if necessary)

9. Organizational security criteria

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

a) Who holds overall responsibility for implementing and ensuring compliance with the organizational security criteria?

○ *Controller* ○ *Processor*

b) 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*	☐	☐

c) 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 an additional sheet if necessary)

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

(Please use an 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

Place, date	Place, date
Controller signature(s)	Controller signature(s)
Place, date	Place, date
Processor signature(s)	Processor signature(s)