DAIMLER

Version 05/2021

Agreement on Processing on Behalf

between

(please insert Controller)

- as Controller -

and

(please insert Processor)

- as Processor -

concluded on

(please insert date)

☐ Controller is rendering the services, which are subject matter to this agreement, as a processor to another party which is the original controller according to data protection laws. Thus, in relation to that original controller, the Processor is acting as a subprocessor.

Contact Details	
Controller	
Name	
No., street, P.O. box no.	
ZIP code, town/city	
Contact name	
Tel.	
Email	
Name of Data Protection Officer/Contact	
Tel.	
E-mail	
Information Security Officer	
Tel.	
E-mail	
Contact in the event of data protection security breaches	cyber.security@daimler.com; +49 711 1776758
Processor	
Name	
No., street, P.O. box no.	
ZIP code, town/city	
Contact name	
Tel.	
E-mail	
Name of Data Protection Officer/Contact	
Tel.	
Email	
Name of Information Security Officer	
Tel.	
E-mail	
Name of representative in the European Union[1]	
No., street, P.O. box no.	
ZIP code/town/city/country	
Tel.	
Email	

[1] Required if the Processor is not based in the EU and processes personal data relating to data subjects in the EU for the purpose of offering goods or services in the EU or monitoring the behavior of data subjects in the EU.

1 Agreement on Processing on Behalf and Ensuring the Security of Processing

1.1 Description of the Contract

1.1.1 Subject Matter of the Agreement

(Please describe if a Main (Service) Agreement exists, to which this agreement on processing on behalf relates, which kind of service the Processors renders, and what its general task in relation to Controller's personal data is)

1.1.2 Term of this 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 processed

(Please list relevant data types, e.g. name, address, user-ID, vehicle data, credit card information, customer profiles, 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 note: If you want to confirm the implementation of appropriate technical and organizational measures witch a TISAX certification (section 1.6.5.), please also list the exact address of all locations of data processing. Otherwise, a confirmation based on a TISAX certification is not possible.)

1.1.5 **Scope, Nature and Purpose of Processing** of Personal Data

The Processor shall provide the following services for the Controller in relation to the data specified in section 1.1.3:

(Please describe in detail which data processing operations the Processor performs with regard to Controller's personal data. 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 processor renders - with regard to the data described in clause 1.1.3 - the services described in section … of the Main Agreement”)

1.1.6 The **groups** of people **affected** by the handling of their personal data in the context of the present agreement:

(Please describe in detail whose data are affected by the service, e.g. employees of company XY , customer of service A, users of application B, drivers, suppliers, etc. In case this is already 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 The 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 the Controller in connection with the present agreement. That includes, not to disclose this information to third parties, to protect it from third-party access, to use it only for the purposes of the present 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 obligation shall not apply in respect of information

- That can be proven to have been known to the Processor before the present agreement came into effect
- That can be proven to have been lawfully obtained by the 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 contained in the present agreement
- That can proven to have been developed by the Processor during the course of its own independent work.

1.2.3 If the Controller is a financial services company that is subject to bank/client confidentiality requirements, the Processor undertakes to comply with the same requirements.

1.2.4 The Processor undertakes to impose on its employees to whom this information is disclosed the same obligations that it entered into above unless said employees are already subject to an equivalent confidentiality obligation by virtue of their employment contracts.

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

1.2.6 The confidentiality obligations in respect of information that has been made available during the term of the present agreement shall continue to apply for a period of five years after the present agreement has ended.

1.3 Instruction Authority of the Controller

1.3.1 The Processor processes personal data on behalf of the Controller. The Controller is responsible for maintaining compliance with data protection regulations.

1.3.2 During the processing of personal data, the Processor is obligated to follow only the instructions of the Controller. Such instructions must be given in writing or by electronic mail. Outside the scope of these instructions, the Processor may not use the data provided to it for processing either for its own purposes or for the purposes of third parties. The Processor shall adjust, delete or block the data processed in the order in

accordance with the Controller's instructions. If the Processor is of the opinion that instructions of the Controller are in breach of the applicable data protection regulations, it must notify the Controller accordingly without delay.

1.4 Obligations of the Processor

1.4.1 The Processor shall assist the Controller in satisfying the data subjects' rights to access, rectification, restriction of processing, objection, erasure, and data portability regarding their personal data. If a data subject contacts the Processor directly regarding the rights listed above, the Processor shall forward this request to the Controller without delay.

1.4.2 The Processor undertakes to provide data protection training for its employees entrusted with the processing of the data provided by the Controller, and to impose on such employees an obligation to observe data secrecy (compliance with the confidentiality of personal data).

1.4.3 The Processor shall provide the Controller with the contact details of the contact partners for data protection and information security. If the Processor is subject to a statutory obligation to appoint a data protection officer, it shall appoint such an officer in writing and shall send the Controller their name(s) and contact details.

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

1.4.5 Each party to the present agreement shall be liable towards the other party for damage or losses incurred as a result of culpable violations of the present agreement or applicable data protection regulations. If both parties are at fault, they shall be liable according to their respective share of culpability.

1.4.6 The Controller may at any time instruct the immediate erasure of the data processed under the present agreement. Irrespective of this, the Processor is under obligation to surrender the data in a generally readable format at any time, at the request of the Controller. Once the term of the present agreement has ended, the Processor shall be obliged to surrender the data processed under the present agreement in a generally readable format or to delete it, at the Controller's discretion. In case of erasure, it must be ensured that the data cannot be reconstructed. The Processor shall prove to the Controller and confirm in writing, including in electronic form, that all of the data, copies and storage media have been returned and deleted. If binding legal requirements do not allow the erasure of certain data or categories of data, the Processor must inform the Controller about such requirements.

1.4.7 In the event that the Processor or significant parts of the Processor's company are acquired by a third party, or if a third party acquires a majority of the Processor's shares or voting rights, the Controller shall have the right to effect the extraordinary termination of the present agreement.

1.4.8 Upon request, the Processor shall provide the Controller an overview of all recipients of data that are not Subprocessors within the meaning of section 1.5 and shall provide information on the scope and purpose of the respective data transfer upon request.

1.5 Use of Subprocessors

1.5.1 If the Processor engages subprocessors or freelancers, it must first obtain the prior consent of the Controller in writing, including in electronic form. The contractual arrangements between the Processor and the subprocessor or freelancer must be structured in such a way that they correspond with the agreements concluded here between the Controller and the Processor. In particular, the Processor must ensure that the Controller can also perform checks relating to the subprocessors or freelancers in accordance with section 1.7 of the present agreement. The Controller is entitled to receive information from the Processor concerning the essential contractual provisions and the implementation of the obligations arising from the present agreement – if necessary also by inspecting the relevant contractual documents.

1.5.2 The Controller is deemed to have consented to the involvement of the subprocessors and functions listed in Part 3 of the present agreement by signing the present agreement. The Processor must ensure that the subprocessors comply with the technical and organizational requirements specified in Part 2 of the present agreement in the same way as the Processor itself.

1.5.3 If subprocessors are replaced or added during the term of the present agreement, the Processor must first obtain the consent of the Controller in writing, including in electronic form. If the Processor intends to involve subprocessors other than those agreed on in Part 3, it shall notify the Controller's contract management function of this fact via any prescribed channels of communication. Alternatively, it may notify the Controller's contact person as listed on page 2. If the Controller gives its consent, the Processor shall update the overview in Part 3 and provide the updated version of Part 3 to the Controller. The present agreement shall then apply with the updated Part 3.

1.6 Security of Processing

1.6.1 The Processor undertakes to use state-of-the-art technology to safeguard all of the Controller's information and data at all times by implementing technical and organizational measures that are appropriate to the risk associated with the processing. This includes protection against unauthorized access, unauthorized or accidental modification, destruction or loss, unauthorized transfer, other unauthorized processing or any other form of misuse. The measures must be described in detail in Part 2 of the present agreement. Section 1.1.2 notwithstanding, the obligation to protect the information and data shall apply for as long as the Processor stores said data and information, or otherwise processes it or has it processed by subprocessors.

1.6.2 The Processor must establish an Information Security Management System. Considering the risks, the Processor must determine what measures it needs to implement, regularly review them, and amend them. The Processor must document and substantiate both the risks and the measures implemented.

1.6.3 At the Controller's request, the Processor shall coordinate the technical and organizational measures to be implemented with the Controller's competent Information Security Officer.

1.6.4 Compliance with approved codes of conduct or an approved certification procedure and certifications of the information security management system (e.g. in accordance with ISO 27.001) may be included as factors for the assessment of appropriate technical and organizational measures. However, such certifications do not replace examination of appropriateness in individual cases. If such certification is used as a factor it must be appended to the present agreement.

1.6.5 Depending on the risk of processing, a TISAX certification (at least Assessment Level 2 with the Assessment objective “Information with high protection needs (Info high)” and “Data protection (Data)”) can be used to confirm appropriate technical and organizational measures without further verification. The TISAX certification must be available for all locations listed in section 1.1.4. The technical and organizational measures required and implemented to achieve the TISAX certification must be implemented during the entire term of this agreement, even after a possible expiration of the TISAX certification.

1.6.6 The Processor may only grant authorization to access the Controller's data to its own employees in accordance with the authorization concept, and to the extent required for the task in question in connection with the execution of the present agreement. Upon request, the Processor must supply the Controller with the names of persons or groups of persons to whom access authorization has been granted. The Processor undertakes not to disclose the access authorizations assigned to it for the use of the system to any unauthorized persons.

1.6.7 If the Processor is granted access to the IT systems of the Controller or its subprocessors, the Processor undertakes to only access the data and information required to execute the present agreement.

1.6.8 The Processor must notify the Controller's contract management function (or alternatively the Controller's relevant Information Security Officer) in writing, including in electronic form, about significant changes to the technical and organizational measures described in Part 2 via any prescribed communication channels. In the event of any foreseeable reduction in the effectiveness of the security, the consent of the controller must be obtained in writing before the change is carried out.

1.7 Checks

1.7.1 The Controller or its representative have the right to carry out checks on compliance with the requirements of the present agreement. The Processor shall provide the desired information and, at the request of the Controller and within a reasonable period, submit documentary evidence that it has met its obligations by completing a questionnaire supplied by the Controller or by confirming in writing that the measures agreed on in Part 2 are appropriate and up-to-date.

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

1.7.3 The Processor must inform the Controller without delay of any control procedures by supervisory authorities, which take place in its company or the IT infrastructure used by it, and which involve the processing of the Controller's personal data. In the event of impending access to data of the Controller in the context of seizure, confiscation, judicial inquiries or other official measures, which are carried out at the Processor, or in the context of insolvency proceedings or other measures of third parties, the Processor shall inform the Controller accordingly without delay.

1.7.4 In the context of Section 1.7.3, the Processor shall inform all parties involved in any such action without delay that the power of disposal over the data subject to the present agreement lies with the Controller, and shall not transfer any data to third parties or allow third parties to access the data without the Controller's consent. If the Processor is sworn to secrecy in the event of a check, access or other measure in relation to the Controller's

data by a party authorized to access the data, it must exercise due diligence on behalf of the Controller and will take any opportunity to take action against the measures and the confidentiality obligations.

1.8 Reporting of Data Protection Security Breaches

1.8.1 The Processor must report any data protection security breaches (unintentional or unauthorized destruction, loss, amendment, disclosure or access involving personal data processed under the present agreement) or violation of bank/client confidentiality to the Controller without delay in order to give the Controller the opportunity to report the incident to the relevant authorities within 72 hours. The report is to be addressed to the contact address for data protection security breaches as specified on page 2.

1.8.2 In consultation with the Controller, the Processor shall initiate all steps necessary to clarify the matter and remedy the security incident without delay, and provide the Controller all information necessary to document the event and potentially submit a report to the relevant supervisory authority.

1.9 Data Processing in a Third Country

1.9.1. Does the Processor or its subprocessors process personal data emanating from the EU outside the European Economic Area (EU member states plus Iceland, Liechtenstein and Norway) or outside a country recognized by the European Commission as having an adequate level of data protection, or does the Processor or its subprocessors access EU-sourced personal data from outside the countries specified above?

Yes ◉ No ○

If yes, how is the adequate level of data protection ensured with respect to processing in said state(s)?

☐ The application of the EU's standard contractual clauses governing data processing on behalf in third countries has been agreed in writing with the Processor or its subprocessor.

☐ The data processing is subject to binding rules and regulations that have been put in place by the Processor and are recognized by the relevant regulatory authority as providing an adequate basis for providing an appropriate level of data protection within the meaning of EU law.

1.9.2. Does the personal data processed under the present agreement emanate from countries other than those specified in Section 1.9.1. that also specify requirements under data protection law in respect of data processing abroad, and is this data processed abroad from the perspective of those countries?

If yes, how is the legal basis ensured with respect to processing outside this/these country/countries?

2 Measures to ensure the Security of Processing

In the following, the technical and organizational measures implemented by the Processor in order to safeguard the security of data processing activities must be documented. The assessment of the adequacy of the measures is carried out by Daimler, depending on the risk of processing.

There is no requirement to implement all of the action points listed below; the Processor needs to ensure that the overall level of protection is appropriate according to the state of the art. The state of the art comprises established and effective measures that are currently available on the market; recognized national or international standards offer greater specification (e.g. BSI, ENISA, NIST, TeleTrust).

In order to confirm the implementation of appropriate technical and organizational measures, depending on the risk of processing, an approved certification procedure can be used as a factor or replacement of this Section 2 (see Section 1.6.4. and 1.6.5.).

2.1. Confidentiality of Systems and Services

2.1.1 Physical protection of confidentiality

- Definition and documentation of people with access authorization, including scope of authority
- Access / entrance rules for external visitors (e.g. accompaniment, access bans, ID cards) in place
- Access protection in the form of an external enclosure/fence
- Rules governing key usage (incl. secure locking systems) are implemented
- All individuals recorded in and out
- Outdoor security measures (e.g. access barriers, lightning, video surveillance and detection sensors)
- Access authorization IDs are distributed
- ID requirement or open carry of employee ID on company premises and buildings
- Gate and reception personnel during work hours
- Security service for properties outside of working hours
- Entrance secured by ID readers
- Burglar-resistant windows on the ground floor / basement
- Equipment secured against theft, physical manipulation and damage
- Creation of different security zones (e.g. visitor meeting rooms, workstations, server rooms, development)
- At higher security level: Surveillance device (e.g. alarm system, video surveillance)
- Separation plants (e.g. hub, person lock)
- Work computers kept in locked rooms
- Rooms containing servers are alarm-monitored
- Measures to prevent simple eavesdropping or illegitimate disclosure (esp. at customer reception, shared spaces or mobile work)
- Printing confined to defined zones of the building, or in person (e.g. print-to-me, follow-me print, with PIN)

- Destruction of documents exclusively within defined zones (e. g. by shredding)
- For server rooms used jointly with other companies, hardware (interfaces) are secured using locked racks, cabinets, cages or other means
- Movement sensors, glass breakage sensors or video surveillance
- Prompt handling of alarms in accordance with the alarm plan

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:

If physical protection measures are not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.1.2 System access control

- Mandatory use of strong passwords according to state-of-the-art recommendations (e.g. from BSI, NIST, ENISA)
- Passwords are not stored in plain text
- Passwords are stored hashed in accordance with the state of the art
- Publication of password rules for employees (e.g. prohibition of disclosure, storage in the browser of multiple use)
- Passwords are blocked after a security incident, even in case of suspicion, and must be reassigned by the user
- Secure delivery of user credentials (e.g. encrypted mail, separate letters for username and password)
- Automatic blocking of access in case of many failed attempts (temporary or complete)
- Delay between multiple login attempts (especially when logging in via the internet)
- Authorization concept and device management for IT devices
- Authorization concept for IT applications / IT systems
- Further interaction with the IT system is only possible after successful authentication
- The user authentication procedure was chosen on the basis of a risk assessment and potential attack scenarios are taken into consideration (e.g. possibility of direct access from the internet)
- Use of two-or multi-factor authentication for system access to critical content and admin accounts
- Only strong passwords are used for admin accounts of IT systems (e.g. at least 15 characters, complex and without common word components)
- Implementation of a central IT-system to administer user identities (Identity and Access Management System)
- A segmentation of the networks used has been defined
- Network segmentation rules and procedures have been defined and implemented

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:

If access control is not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.1.3 Authorization management (rights and roles)

- Use of distinct and personal user accounts
- The authorization and role concepts for IT applications and systems are documented and implemented
- Access authorizations only according to necessity (“need-to-know”) and with least possible rights (“least privilege”)
- Regular review of authorizations (at least once a year)
- Authorizations are reviewed and access rights are checked for all users within an IT system (e.g. module, table, data set)
- Audit-proof documentation of user authorizations
- User accounts are set up in accordance with an approval process that follows the principle of dual control
- The use of "shared accounts" is regulated (e.g. restricted, only when proof of activity is not required)
- A basic user account with minimal access rights and functionalities is available and is used (e.g for external workers)
- Changes in the responsibility or employment relationship of employees are immediately reflected in access authorizations
- Read-access logged
- Write-access logged (including deletion / overwriting)
- Unauthorized access attempts are logged
- Regular evaluation of logging
- Occasion-related evaluation of logging
- A management process (approval / change / deletion) for privileged user IDs is documented and established
- User accounts with privileged rights are documented and regularly reviewed

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:

If access control is not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.1.4 Encryption and Pseudonymization

- The electric transmission of data is encrypted
- The storage of personal data is encrypted
- All personal data on mobile devices and mobile storage media is encrypted
- All encryption technologies used correspond to the state of the art
- The administration of the key material has been defined and documented for the relevant IT systems
- Transport layer encryption is exclusively implemented on an end-to-end basis
- A set of rules with requirements for encryption strength, algorithm and key management is implemented
- Pseudonymization of personal data by means of disposable functions
- Pseudonymization by assignment tables, these are separated from the rest of the data processing

If you have implemented other or additional measures, or would like to provide more details of the measures mentioned above, **particularly if transmission using state-of-the-art encryption cannot be guaranteed**, please provide details below:

If encryption is not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.2. Integrity of Systems and Services

2.2.1 Protection of data transmission

- Definition and documentation of the recipients of personal data in the context of the processing on behalf agreed in this agreement

- Secure physical transportation (e.g. secure vehicle, container, encryption of storage media, handover protocols)
- Documentation of all interfaces for the electronic transmission of personal data
- Use of digital signature methods to ensure the authenticity of data transmissions
- USB interface deactivation
- Own virtual lines for data transmission
- Restriction of employees' powers to transfer data
- Use of a web proxie that all HTTP(S) connections must go through
- Connection of branches or home office only via VPN connections
- Regular checks of permitted recipients
- Technical restriction of forwarding to only permitted recipients
- In cases of mass e-mail distribution, the disclosure of all recipients is prevented by technical or organizational means
- Documentation of the transmission routes of personal data under this agreement of processing on behalf (e.g. printout, media, automated delivery)
- Logging of electronic data transfer or transmission
- Plausibility, completeness and accuracy checks are carried out

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:

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

2.2.2. Input control

- Inputs/changes of personal data are logged
- Regular (indiscriminate) evaluation of log files to detect unusual inputs
- Inputting responsibilities specified in organizational structure

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:

If input control is not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.2.3 Other measures to ensure the integrity of systems and services

- System hardening measures are implemented (e.g. limitation / deactivation of unnecessary permissions, ports, protocols, servers) ☐
- Multi-tenant capability implemented by dedicated physical servers ☐
- Multi-tenant capability implemented by separation at the system level ☐
- Multi-tenant capability: Segregation at the data level ☐
- Description of the implementation of tenant separation ☐
- Use of a mobile device management solution for smartphones ☐
- The inputting of data is validated on the basis of semantic criteria (semantic input validation) ☐
- System hardening regarding shared virtual machines and/or application instances ☐
- The separation of data, applications, the operating system, storage and network is implemented ☐
- Received data and programs that are automatically checked for malware before being opened (on-access scan) ☐
- All data held in all systems is regularly checked for malware ☐
- Data loss prevention solutions are used ☐
- Purpose attributes have been defined for data fields and sets ☐

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:

If the above measures are not relevant to the processing on behalf subject to the present agreement, please briefly state the reasons below:

2.3. Availability of Systems and Services

2.3.1 Ensuring the Availability of Personal Data

- Redundant IT systems are in place (end devices, servers, storage etc.) ☐
- Uninterrupted power supply (UPS) ☐
- Technical protection systems for fire protection, power supply, air conditioning ☐

- Server rooms and data processing centers have fire and smoke alarms
- Server rooms and data processing centers have fire extinguishers or fire extinguishing systems
- Server rooms and data processing centers have systems for monitoring temperature and humidity
- System status is regularly checked (monitoring)
- Differently designed IT systems are in place (same functionality from different manufacturers)
- Regular stock checks carried out for print-outs and storage media

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:

If ensuring availability is not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.3.2 Deletion

- Feasibility of implementation of deletion periods for controller's personal data according to the specifications by the controller
- Definition and documentation of procedures to dispose of and destroy data storage media
- Documentation of a deletion concept for processing on behalf
- Implementation of regulations for the disposal of storage media
- Integrity control for deletions or deletion routines
- Deletion implemented for development, test and production environments
- Shredder (min. Level 3, cross cutting) for paper documents
- External shreddenor (DIN 32757)

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

If deletion measures are not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.4 Resilience of Systems and Services

2.4.1 Safeguard against disruptions (continuity assurance)

- Load balancer
- Virus scanner with up-to-date search patterns on all end-user devices
- Patch management process (among others update plan for the software used)
- Redundant IT systems
- Execution of penetration tests (in other applications for web applications)
- Use of firewall systems (e.g. at the central transition to the internet, securing databases on web servers)
- Regulated process for proper configuration of firewall systems, including shares / exceptions
- Data storage in a RAID system
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Measures to improve the error tolerance of systems and services
- For websites and web applications: A Content Security Policy (CSP) has been defined and implemented

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

If safeguarding the continuity of systems and services is not relevant to the processing on behalf subject to the present agreement, please briefly state the reasons below:

2.4.2 Restarting and restoring of availability

- Back-up and restarting concept (data backed up regularly)
- Appropriate physical storage of backup media (e.g. safe, fire protection, spatial separation)
- Appropriate protection of backups against encryption by ransomware
- Restart concept (measures to restore availability immediately in the event of system failure)
- Documented and tested emergency operational concept (IT service continuity)
- Documented and established Business Continuity Management

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

If restarting and restoring of the availability of the above measures are not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.5 Organizational and process-related protection measures

2.5.1 Organizational Security Measures

- The roles and responsibilities in the field of data security are described, staffed and known internally
- Implementation of an appropriate information security management system
- Security guidelines for the handling of information are defined, adopted by the management and communicated to the employees
- Existence of adequate incident management (response to security breaches)
- An attack identification and reporting is in place (incident response)
- A documented Change Management process for IT systems that process personal data in the context of the present agreement
- Information about technical vulnerabilities about the systems and software (assets) used is collected and assessed in terms of impact
- Adequate response to identified technical vulnerabilities (e.g. shutdown / separation of services and systems, monitoring, adapting firewalls)
- Awareness measures for all users regarding data protection and data security
- Training measures or appropriate in-house education in data protection
- Classification of all information according to its protection needs (e.g. confidentiality, availability, integrity)
- Separation of production systems and development / test systems
- Only synthetic data, i.e. no genuine or personal data, is processed in the test and development environment
- Prohibition of the storage of personal data in source code (repositories)
- Regulations on the mobile / private use of terminal devices (e.g. smartphones, notebooks) by employees have been made
- Regular verification of the intended use of information and IT systems (e.g. audits by IT security or data protection officers)
- Process for regular review of the effectiveness of all protective measures and, where appropriate, their adaption (PDCA cycle)

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:

If organizational security measures are not relevant to the services subject to the present agreement, please briefly state the reasons below:

2.5.2 Monitoring of Assignment

- Documentation of all subprocessors used to process the personal data for the purpose of the present agreement
- There are historicalized and versioned service level agreements (SLAs) with relevant subprocessors
- There is a quality management system at the relevant subprocessors that fully covers processing on behalf
- There is an information security management system (ISMS) among the relevant subprocessors that fully covers processing on behalf
- All relevant subprocessors have established certification in the field of information security (e.g ISO 27001, TISAX, SOC 2, BSI IT-Grundschutz)
- Regular monitoring of relevant subprocessors by submitting self-assessments
- Regular third-party checks of relevant subprocessors (e.g auditors, data protection auditors)
- Regular inspection of the relevant subprocessors by examining contracts with (further) subprocessors
- The implementation of checks at subprocessors
- The existence of internal policies and work instructions for processing on behalf

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:

If measures with regard to the monitoring of the assignment are not relevant to the services subject to the present agreement, please briefly state the reasons below:

3 Approved Subprocessors

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

Brief description of the function carried out by this subprocessor:

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

Brief description of the function carried out by this subprocessor:

(Provide details for any further subprocessors, if relevant)

The Processor offers assurance that the subprocessors listed here are bound by contract to fulfill the obligations of Part 1 and have implemented technical and organizational measures in accordance with the specifications of Part 2.

4 Signatures

Note: The conclusion of the present agreement must be documented. For this purpose, an electronic documentation of the conclusion is sufficient. Alternatively, for example if required for the purpose of internal signature regulations, hard copies of the agreement may be signed.

Processor	**Controller**
Place, date:	Place, date:
Name of representative (1): (Signature)	Name of representative (1): (Signature)
Name of representative (2): (Signature)	Name of representative (2): (Signature)