Personal Information Processing on Behalf Agreement

Between

Click here to insert

as

Entrusting Party

and

Click here to insert

as

Entrusted Party

Version: 2023

Contact Details	
Entrusting Party	
Company name	Click here to insert
Address	Click here to insert
Contact name	Click here to insert
Tel.	Click here to insert
Email	Click here to insert
Entrusted Party	
Company name	Click here to insert
Address	Click here to insert
Contact name	Click here to insert
Tel.	Click here to insert
Email	Click here to insert

1. Applicability

1.1. This Personal Information Processing on Behalf Agreement (the "**Agreement**") shall apply to any activity in which the Entrusted Party, as a supplier or partner of the Entrusting Party, process personal information on behalf of the Entrusting Party when providing goods or services to the Entrusting Party as entrusted by the Entrusting Party.

1.2. Part A of Annex 1 - Data Processing Questionnaire of the Agreement ("**Annex 1**") shall be filled in by the Entrusting Party, the Entrusted Party shall provide all necessary support and assistance. Unless agreed by the Entrusting Party, the activities carried out by the Entrusted Party during the performance of the Agreement shall not exceed the scope specified in Part A. Part B of Annex 1 shall be filled in by the Entrusted Party, which constitutes the Entrusted Party's representation and warranty under the Agreement. If the Entrusted Party needs to update or modify the information in Part B of Annex 1 during the performance of the Agreement, it shall promptly notify the Entrusting Party.

2. Definitions

Under the Agreement:

2.1. **"Data protection laws and regulations**" means all laws, regulations and national standards regarding personal information security, data security and cyber security that apply to the Entrusting Party or the Entrusted Party, including but not limited to *Personal Information Protection Law of the People's Republic of China*, *Data Security Law of the People's Republic of China*, *Cybersecurity Law of the People's Republic of China*, etc.

2.2. "**Data protection and information security measures**" means the measures listed in Annex 1: Part B of the Agreement and other measures agreed or required to perform the Agreement.

2.3. "**China**" means the People's Republic of China, for the purpose of the Agreement, excluding Hong Kong, Macao and Taiwan.

2.4. "**Processing**" means the collection, storage, use, processing, transmission, provision, disclosure, deletion and other activities of personal information.

2.5. "**Personal information**" means all kinds of information recorded electronically or by other means relating to identified or identifiable natural persons, and shall not include information after anonymization.

2.6. "**Personal information security incident**" means unauthorized use, unauthorized or accidental modification, damage, disclosure, tampering, loss, unauthorized transmission, unauthorized processing, and other forms of abuse of personal information.

2.7. "**Writing**" or "**Written**" means contract, letter, data message (including telegram, telex, facsimile, electronic data interchange and e-mail) and others that can tangibly represent the contents it carries.

3. Authorization granted to the Entrusted Party

3.1. The Entrusted Party shall comply with applicable data protection laws and regulations when processing the personal information provided by the Entrusting Party.

3.2. During the processing of personal information provided by the Entrusting Party, the Entrusted

Party shall strictly follow the instructions provided by the Entrusting Party. Apart from the arrangement as agreed by both parties in Part A of Annex 1, all instructions shall be given by the Entrusting Party in writing.

3.3. The Entrusted Party shall not, for its own or third party's purposes, process the personal information provided to it by the Entrusting Party beyond the above instructions. If the Entrusted Party is of the opinion that instructions of the Entrusting Party are in breach of the applicable data protection laws and regulations or is unable to process personal information by following instructions of the Entrusting Party due to any special reasons, both parties shall actively communicate with each other to reach agreement on relevant details at that time..

3.4. Without the prior written consent of the Entrusting Party or unless otherwise agreed herein, the Entrusted Party shall not transmit to any third party or allow any third party to access any personal information provided by the Entrusting Party.

3.5. Unless otherwise agreed in writing by both parties, the Entrusted Party shall not have the right to, at its sole discretion, determine the processing activities regarding the personal information provided by the Entrusting Party, and shall not acquire, by virtue of the Agreement, corresponding rights to copy or reproduce such information under applicable laws and regulations.

4. Obligations of the Entrusted Party

4.1. The Entrusted Party shall, in accordance with data protection laws and regulations, take necessary measures to ensure the security of the personal information it processes, and assist the Entrusting Party in fulfilling relevant obligations of data protection laws and regulations.

4.2. Entrusted Party shall assist the Entrusting Party in responding the request of personal information subjects exercising their rights, including but not limited to rights to be informed, decide, access, copy, rectify, supplement and delete their personal information, etc. If a personal information subject contacts the Entrusted Party directly regarding the foresaid rights, the Entrusted Party shall forward this request to the Entrusting Party in writing without delay, and observe the instructions provided by the Entrusting Party: (1) without authorization from the Entrusting Party, the Entrusted Party shall not directly respond to the exercise request of the personal information subjects; (2) if authorized by the Entrusting Party to respond directly, the Entrusted Party shall respond to the exercise request of the personal information subjects within the scope authorized by the Entrusting Party.

4.3. The Entrusted Party shall provide data protection training for its personnel involved in the processing of the personal information provided by the Entrusting Party.

4.4. The Entrusted Party shall establish the mechanism, system and procedure for data protection and personal information protection in accordance with applicable laws and regulations.

4.5. Upon request by the Entrusting Party, the Entrusted Party shall provide the Entrusting Party with the reasonable and necessary information and materials to assist the Entrusting Party to perform its obligations under applicable data protection laws and regulations, such as notification obligations, maintaining records of processing activities, performing data protection impact assessments, and applying for cybersecurity examinations (if applicable), etc., as required by applicable laws and regulations.

4.6. Unless otherwise agreed in writing by both parties, the Entrusted Party shall bear all relevant

costs, fees and expenses incurred by it in performing its duties and obligations under the Agreement.

4.7. The Entrusting Party may, within a reasonable time, request the Entrusted Party in advance to return the entrusted processed personal information and its copies and/or permanently and securely delete or destroy the personal information and its copies processed under the Agreement. If the personal information has been deleted, the Entrusted Party shall ensure that the personal information cannot be reconstructed. The Entrusting Party has right to reasonably request the Entrusted Party to provide relevant materials to prove its fulfillment of the aforementioned requirements.

4.8. The processing of personal information hereunder shall be limited to the territory of China. Without the prior written consent or authorization of the Entrusting Party, the Entrusted Party shall not provide any relevant personal information overseas under this Agreement, including but not limited to: (1) shall not access or provide opportunities for others to access the personal information outside China; (2) shall not transfer any personal information to other countries or regions outside China; and (3) shall not have any other acts of cross-border data transfer as specified in data protection laws and regulations. Upon the request of the Entrusting Party, the Entrusted Party shall cooperate with the Entrusting Party to the maximum reasonable extent to comply with the compliance requirements of cross-border data transfer (including but not limited to completing personal information protection impact assessment, cross-border data transfer security assessment, filing of standard contracts for cross-border transfer of personal information, personal information protection certification, etc.) in China. If the Entrusted Party breaches any provision of this clause 4.8, the Entrusting Party shall have the right to terminate the Agreement with an immediate effect and hold the Entrusted Party liable for breach of the Agreement in accordance with clause 9 under the Agreement.

4.9. In the event that a third party acquires a majority of the Entrusted Party's shares or voting rights or all or substantially all of the assets or business of the Entrusted Party, or if the major business of the Entrusted Party have material changes, the Entrusting Party shall have the right to terminate the Agreement. At that time, both parties shall communicate the relevant details.

4.10. The Entrusted Party shall procure its affiliates, subsidiaries and their respective subcontractors (if any), employees, directors, supervisors, agents or managing officers who have access to any entrusted processed personal information to comply with the obligations of the Entrusted Party under the Agreement. The Entrusted Party shall ensure that such personnel are aware of and comply with the obligations at least as strict as those under the Agreement.

5. Subcontractors

5.1. If the Entrusted Party engages subcontractors, it shall first obtain the prior consent of the Entrusting Party in writing. The contractual arrangements between the Entrusted Party and the subcontractor shall conform with the provisions and requirements of the Agreement. In particular, the Entrusted Party shall ensure that the Entrusting Party can also perform checks relating to the subcontractors in accordance with clause 7 of the Agreement. The Entrusted Party shall provide the Entrusting Party with all information regarding the engagement of subcontractors, including but not limited to relevant contractual documents for the Entrusting Party for review.

5.2. The Entrusted Party shall fill in the subcontractor information in Part C of Annex 1. The Entrusted Party shall ensure that the subcontractors comply with the data protection and information security measures specified in Part B of Annex 1 in the same way as the Entrusted

Party.

5.3. If the Entrusted Party intends to replace or add subcontractors during the term of the Agreement and subject to the consent of the Entrusting Party, the Entrusted Party shall provide an updated version of Part C of Annex 1 to the Entrusting Party.

5.4. During the performance of the Agreement, the Entrusted Party shall assume corresponding liabilities to the Entrusting Party regarding subcontractor's duties and obligations under the Agreement.

6. Information Security

6.1. The Entrusted Party undertakes to process all of the personal information provided by the Entrusting Party by implementing data protection and information security measures that are appropriate to the risk associated with the processing (including but not limited to data protection and information security measures involved in Part B of Annex 1) in order to prevent the occurrence of personal information security incidents. The Entrusted Party shall completely fill in the data protection and information security measures in Part B of Annex 1 under the Agreement. Regardless of the expiration or termination of the Agreement, the foresaid measures shall be applicable as long as the Entrusted Party processes, or engages subcontractors to process, personal information provided by the Entrusting Party. If the Entrusting Party considers it necessary for the Entrusted Party to take additional security measures as required by applicable data protection laws and regulations, it may require the Entrusted Party to implement such additional measures.

6.2. The Entrusted Party shall establish an information security management system, implementing measures and risk responding measures. The Entrusted Party shall regularly update and amend such system and measures and record accordingly.

6.3. At the Entrusting Party's request, the Entrusted Party shall inform the Entrusting Party of the implementation status on the data protection and information security measures.

6.4. If the Entrusted Party has obtained the certifications of the information security management system, such as ISO27001, it shall provide corresponding documents to the Entrusting Party.

6.5. During the performance of the Agreement, the Entrusted Party may grant corresponding authorization to its personnel and subcontractors only when it is for the purpose of performing tasks according to this Agreement, and may only permit such personnel to perform tasks in connection with the implementation and performance of the Agreement.

6.6. The Entrusted Party shall notify the Entrusting Party in writing of any significant changes to the data protection and information security measures described in Part B of Annex 1.

7. Checks

7.1. The Entrusting Party or its representative have the right to carry out checks on Entrusted Party’s compliance with the requirements of the Agreement. The Entrusted Party shall provide the desired information. When the Entrusting Party is aware of or identifies that the Entrusted Party: (1) fails to follow the Entrusting Party’s instructions or the Agreement to process the personal information; or (2) fails to perform the duties of personal information security protection, the Entrusted Party shall cease the relevant activities and make remediation

measures (such as changing password, revoking permissions, disconnecting from network) or eliminate the security risk to personal information, in line with the instructions of the Entrusting Party. Additionally, at the request of the Entrusting Party and within a reasonable period, the Entrusted Party shall complete a questionnaire provided by the Entrusting Party and submit documentary evidence that it has met its obligations or confirm in writing that the measures agreed on in Part B of Annex 1 are appropriate and up-to-date.

7.2. Subject to advance notice, the Entrusting Party or its representative may be granted access to the Entrusted Party's offices and IT systems in/on which the Entrusted Party could process the personal information provided by the Entrusting Party so that the implementation of the Agreement and the appropriateness of the data protection and information security measures can be verified.

7.3. The Entrusted Party shall inform the Entrusting Party in writing without delay of any control procedures or other enforcement measures by supervisory authorities, which take place in its company or the IT infrastructure used by it, and which are in connection with the Agreement or may affect the performance of the Agreement. In the context of seizure, confiscation, judicial inquiries or other official measures by relevant authorities, or in the context of insolvency proceedings, reorganization proceedings or other measures of third parties, which prevents the performance of the Agreement, the Entrusted Party shall inform the Entrusting Party in writing accordingly without delay.

7.4. In the context of clause 7.3, if the Entrusted Party accepts a check, access or other authorized access in relation to the personal information provided by the Entrusting Party, it shall take adequate measures to ensure security of the personal information.

7.5. The Entrusted Party agrees that the Entrusting Party may engage an independent third party to carry out the inspection activities specified in this clause 7.

8. Personal Information Security Incident

8.1. In the event of any occurrence of personal information security incident, the Entrusted Party shall notify the Entrusting Party as soon as possible (and in any case not more than 48 hours after it becomes aware of such situation), so that the Entrusting Party can evaluate its next step in accordance with applicable data protection laws and regulations.

8.2. At the request of the Entrusting Party, the Entrusted Party shall take measures, including but not limited to the following: (1) all steps necessary to clarify the matter and remedy the personal information security incident without delay, including but not limited to stopping illegal processing, recovering lost or damaged personal information (if feasible), eliminating all impact caused by illegal processing methods or measures, upgrading optimization technology and organizational security measures, etc.; (2) providing the Entrusting Party with necessary information and assistance to record the event and, as the case may be, report to the relevant supervisory authority or notify the personal information subject.

9. Liabilities for Breach of the Agreement

9.1. Any failure to perform or incomplete performance of any provision under this Agreement (including but not limited to failure to perform or incomplete performance of the obligations under the Agreement) or data protection laws and regulations by the Entrusted Party

constitutes a default (the "**Default**").

9.2. In the case of any Default by the Entrusted Party, the Entrusting Party has the right to:

(1) take effective remedial measures (such as suspending transmission of personal information, changing password, revoking permissions, disconnecting from network, etc.) to control or eliminate the security risks to the personal information provided by the Entrusting Party as a result of the Entrusted Party's Default;

(2) take action against the Entrusted Party's Default in accordance with applicable laws and regulations, including but not limited to requiring the Entrusted Party to indemnify the Entrusting Party, its affiliates, subsidiaries and their respective subcontractors (if any), employees, directors, supervisors, agents or managing officers (collectively, the "**Indemnified Party**") for the losses, expenses and penalties (collectively, the "**Claims**", including litigation fees, foreseeable and reasonable loss of profits or revenue, and/or the claim or allegation brought by personal information subjects or government authorities regarding the processing of personal information);

(3) request the Entrusted Party to continue to perform the relevant obligations in accordance with the provisions of the Agreement; and

(4) terminate the Agreement in accordance with clause 10.1 under this Agreement.

9.3. In the case of any Default by the Entrusted Party, without prejudice to any other rights or remedies of the Indemnified Party under the laws of China or in connection with this Agreement, the Entrusted Party shall, in accordance with applicable laws and regulations:

(1) defend and hold the Indemnified Party harmless from claims against the Indemnified Party arising out of or in connection with any Default by the Entrusted Party and indemnify the Indemnified Party accordingly regarding such claims; and

(2) assist the Indemnified Party in defending claims, always act in accordance with the instructions of the Indemnified Party, hold the Indemnified Party harmless, and assume any other losses or legal liabilities arising therefrom at its own cost.

10. Miscellaneous

10.1. The Agreement shall come into force on [Please insert the effective date YY/MM/DD] and remains in force until [Please insert the expiration date (consistent with the commercial contract) YY/MM/DD]. If the Entrusted Party defaults, the Entrusting Party may terminate the Agreement at any time by giving a written notice to the Entrusted Party without taking any liability for the breach of the Agreement, provided that the rights and remedies granted by laws and regulations and the Agreement to the Entrusting Party are not affected.

10.2. Upon expiration or termination of the Agreement, the Entrusted Party shall, at the request of the Entrusting Party, immediately return all entrusted processed personal information and its copies to the Entrusting Party and/or permanently and securely delete or destroy all entrusted processed personal information and its copies. If the personal information has been deleted, the Entrusted Party shall ensure that the personal information cannot be reconstructed. The Entrusting Party has right to reasonably request the Entrusted Party to provide relevant materials to prove its fulfillment of the aforementioned requirements.

10.3. Any Changes, amendment or revisions to the Agreement and any part thereof require the

written consent of both parties.

10.4. The execution, interpretation and performance of the Agreement and any disputes arising out of or in connection with the Agreement shall be governed by laws of the People's Republic of China.

10.5. If any provision of the Agreement is held to be invalid or unenforceable, the invalidity of such provision shall not affect the other provisions of the Agreement, and all provisions that are not affected by such invalidity shall remain in full force and effect.

10.6. Any Annexes to the Agreement shall be deemed as an integral part of the Agreement and shall have the same effect as the text of the Agreement.

10.7. The Agreement is made in two counterparts, with the Entrusting Party and the Entrusted Party each holding one copy. Each copy shall be an original and have the same legal effect.

Signature and Chop

Entrusting Party: Click here to insert

Name: Click here to insert

Title: Click here to insert

Signature:

Date:

Location:

(Chop)

Name: Click here to insert

Title: Click here to insert

Signature:

Date:

Location:

Entrusted Party: Click here to insert

Name: Click here to insert

Title: Click here to insert

Signature:

Date:

Location:

(Chop)

Annex 1：Data Processing Questionnaire

This Annex is a part of the Personal Information Processing on Behalf Agreement, consisting of **Part A. Basic Information of Entrusted Processing**, **Part B. Data Protection and Information Security Measures**, and **Part C. Approved Subcontractors**.

Part A. Basic Information of Entrusted Processing

1 Subject Matter

Please describe if Master Agreement or other (service) agreement ("Relevant Agreement") exists, to which the above entrusted processing relates, and services provided by the Entrusted Party. For example, the Entrusted Party signs XXX Agreement with the Entrusting Party, providing XXX products/service via XXX, processing and/or involving personal information.

2 Term of Entrusted Processing

Under general circumstances, the term of entrusted processing shall be consistent with that specified in clause 10.1 under the Agreement. If the term of entrusted processing is inconsistent with that specified in clause 10.1 under the Agreement, please specify the term of entrusted processing.

3 Types of Personal Information Processed

Please list relevant personal information types (**bold and underline** sensitive personal information), e.g. name, address, phone number, user-ID, vehicle data (please specify the specific types), **credit card information**, **ID number**, **scanned copies of ID card**, **driver's license number**, **scanned copies of driver's license**, etc.

4 Locations of Data Processing and Storage

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

5 Possible Processing Activities and Purposes of Personal information

The Entrusted Party shall provide the following services for the Entrusting Party in relation to the data specified in Section 3:

Please describe in detail which processing operations the Entrusted Party performs with regard to personal information provided by the Entrusting Party. Processing of personal information means almost any kind of actions relating to personal information, such as collection, storage, usage, processing, transmission, provision, disclosure, deletion, etc. Should such actions already be described in the Relevant Agreement, a reference to the Relevant Agreement may be used: e.g. "According to article XXX in Relevant Agreement, the Entrusted Party provides services about the personal information under Section 3 under this Part A."

6 Personal Information Subject Involved

In the context of the Agreement, the natural person (personal information subject) identified or associated with the personal information entrusted to be processed is as follows:

Please describe in detail the types of natural persons identified or associated with the personal information entrusted to be processed in the service, e.g. employees of company XXX, customer of service XXX, users of application XXX, drivers, suppliers, etc. In case this is already described in the Master Agreement, a reference to the Master Agreement shall be used: e.g. "The persons concerned by the services are described under article XXX of the Relevant Agreement/Annex XX." If personal information of minors under the age of 14 is involved, please state and describe the reasons.

Part B. Data Protection and Information Security Measures

The Entrusted Party has implemented the following basic measures and additional measures (if applicable) in order to safeguard the data and information security (Enter "Yes" for the measures taken or "No" for the measures not taken, and add descriptions when necessary).

This part shall be used to document the data protection and information security measures implemented by the Entrusted Party in order to safeguard the security of data processing activities.

The individual data protection and information security measures are categorized according to their primary protection objectives: the confidentiality, integrity, availability and resilience (recoverability) of the systems and services involved in the processing of personal information. Organizational and process-related measures supplement the primary protection objectives.

All the basic measures listed below are mandatory. Please respectively state the reasons or alternatives if the basic measure has not been taken. The Entrusted Party 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; national or international standards offer greater specification (e.g. ISO27000, ISO27701, BSI, ENISA, NIST, TeleTrust etc.).

1 Confidentiality-Physical protection of confidentiality

1.1 Basic measures

No	Basic measure	Whether the measure has been taken (Enter "Yes" or "No")	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken
1	Definition and documentation of people with access authorization, including scope of authority.		Click here to insert
2	Access / entrance rules for external visitors (e.g. accompaniment, access bans, ID cards) in place.		Click here to insert
3	Access protection in the form of an external enclosure/fence.		Click here to insert
4	Rules governing key usage (incl. secure locking systems) are implemented.		Click here to insert

(Please add here if necessary)

1.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of physical access control?

No.	Additional measure	Whether the measure has been taken (Enter "Yes" or "No")
1	All individuals recorded in and out, and the recording is ready to review if needed.	
2	Outdoor security measures (e.g. access barriers, video surveillance and detection sensors).	
3	Access authorization IDs are distributed.	

4	ID requirement or open carry of employee ID on company premises and buildings.	
5	Gate and reception personnel during work hours.	
6	Security service for properties outside of working hours.	
7	Entrance secured by ID readers	
8	Burglar-resistant windows on the ground floor / basement	
9	Equipment secured against theft, physical manipulation and damage	
10	Creation of different security zones (e.g. visitor meeting rooms, workstations, server rooms, development)	
11	At higher security level: Surveillance device (e.g. alarm system, video surveillance)	
12	Separation plants	
13	Work computers kept in locked rooms	
14	Rooms containing servers are alarm-monitored	
15	Measures to prevent simple eavesdropping or illegitimate disclosure (esp. at customer reception, shared spaces or mobile work)	
16	Printing confined to defined zones of the building, or in person	
17	Destruction of documents exclusively within defined zones (e.g. by shredding)	
18	For server rooms used jointly with other companies, hardware (interfaces) are secured using locked racks, cabinets, cages or other means	
19	Movement sensors, glass breakage sensors or video surveillance	
20	Prompt handling of alarms in accordance with the alarm plan	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

1.3 Description of inapplicability

If physical access control is not applicable to the Agreement, please briefly state the reasons or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

2 Confidentiality-System access control

2.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter “Yes” or “No”)	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Mandatory use of strong passwords according to state-of-the-art recommendations (e.g. from BSI, NIST, ENISA)		Click here to insert
2	Passwords are not stored in plain text		Click here to insert
3	Passwords are stored hashed in accordance with the state of the art		Click here to insert
4	Authorization concept and device		Click here to insert

	management for IT devices		
5	Authorization concept for IT applications/IT systems		Click here to insert
6	Further interactions with the IT system are only possible following successful authentication		Click here to insert
7	Only strong passwords are used for admin accounts of IT systems (e.g. at least 15 characters, complex and without common word components)		Click here to insert
8	A segmentation of the networks used has been defined		Click here to insert
9	Installed anti-malware		Click here to insert
10	Installed firewall		Click here to insert

(Please add here if necessary)

2.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of systems access control?

No.	Additional measure	Whether the measure has been taken (Enter "Yes" or "No")
1	Publication of password rules for employees (e.g. prohibition of disclosure, storage in the browser of multiple use)	
2	Passwords are blocked after a personal information security incident, even in case of suspicion, and must be reassigned by the user	
3	Secure delivery of user credentials (e.g. encrypted mail, separate letters for username and password)	
4	Automatic blocking of access in case of many failed attempts	
5	Delay between multiple login attempts (especially when logging in via the internet)	
6	The user authentication procedure was chosen on the basis of a risk assessment and potential attack scenarios were taken into consideration (e.g. possibility of direct access from the Internet)	
7	Use of two-or multi-factor authentication for system access to critical content and admin accounts	
8	Implementation of a central IT-system to administer user identities (Identity and Access Management System)	
9	Network segmentation rules and procedures have been defined and implemented	
10	Information access categorized by sensitivity level	
11	Clear authority allocation for system access accounts	
12	Penetration test has been proactively carried out to check the security of application systems	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

2.3 Description of inapplicability

If systems access control is not applicable to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

3 Confidentiality-Authorization management

3.1 Basic measures

No	Basic measure	Whether the measure has been taken (Enter "Yes" or "No")	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Use of distinct and personal user accounts		Click here to insert
2	The authorization and role concepts for IT applications and systems are documented and implemented		Click here to insert
3	Access authorizations only according to necessity ("need-to-know") and with least possible rights("least privilege")		Click here to insert
4	Regular review of authorizations (at least once a year)		Click here to insert
5	Authorizations are reviewed and access rights are checked for all users within an IT system (e.g. module, table, data set)		Click here to insert
6	The use of "shared accounts" is regulated (e.g. restricted, only when proof of activity is not required)		Click here to insert
7	Changes in the responsibility or employment relationship of employees are immediately reflected in access authorizations		Click here to insert
8	Read-access logged		Click here to insert
9	Unauthorized access attempts are logged		Click here to insert
10	Regular evaluation of logging		Click here to insert
11	Occasion-related evaluation of logging		Click here to insert
12	A management process (approval / change / deletion) for privileged user IDs is documented and established		Click here to insert
13	User accounts with privileged rights are documented and regularly reviewed		Click here to insert

(Please add here if necessary)

3.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of authorization management?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)
1	Audit-proof documentation of user authorizations	
2	User accounts are set up in accordance with an approval process that follows the principle of dual control	
3	User-specific access to the Controller's data shall not be used by multiple users	
4	A basic user account with minimal access rights and functionalities is available and is used	
5	Write-access logged (including deletion/overwriting)	
6	Authorization and role concepts at the system application level are documented and described	
7	Availability time can be set for relevant accounts	
8	Separated development test and production environment	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

3.3 Description of inapplicability

If authorization management is not applicable to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

4 Confidentiality-Encryption

4.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter “Yes” or “No”)	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	The storage of personal information is encrypted		Click here to insert
2	All encryption technologies used correspond to the state of the art		Click here to insert
3	Pseudonymization of personal information by means of disposable functions		Click here to insert

(Please add here if necessary)

4.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of encryption?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)

1	The electric transmission of data is encrypted	
2	All personal information on mobile devices and mobile storage media is encrypted	
3	The administration of the key material has been defined and documented for the relevant IT systems	
4	Transport layer encryption is exclusively implemented on an end-to-end basis	
5	A set of rules with requirements for encryption strength, algorithm and key management is implemented	
6	Pseudonymization by assignment tables, these are separated from the rest of the data processing	
7	Available records of modifications and deletions to personal information	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

4.3 Description of inapplicability

If encryption is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

5 Integrity-Protection of data transmission

5.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter “Yes” or “No”)	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Definition and documentation of the entrusted party of personal information in the context of the processing on behalf agreed in this Agreement		Click here to insert
2	Secure physical transportation (e.g. secure vehicle, container, encryption of storage media, handover protocols)		Click here to insert
3	Documentation of all interfaces for the electronic transmission of personal information		Click here to insert
4	Restriction of employees’ powers to transfer data		Click here to insert
5	Documentation of the transmission routes of personal information under this Personal Information Processing on Behalf Agreement (e.g. printout, media, automated delivery)		Click here to insert

5.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of protection of data transmission?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)
1	Use of digital signature methods to ensure the authenticity of data transmissions	

2	USB interface deactivation	
3	Own virtual lines for data transmission	
4	Use of a web proxy that all HTTP(S) connections must go through	
5	Connection of branches or home office only via VPN connections	
6	Regular checks of permitted recipients	
7	Technical restriction of forwarding to only permitted recipients	
8	In cases of mass e-mail distribution, the disclosure of all recipients is prevented by technical or organizational means	
9	Logging of electronic data transfer or transmission	
10	Plausibility, completeness and accuracy checks are carried out	
11	An Intrusion Detection/ Prevention System in place	
12	Available forwarding log records involving personal information	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

5.3 Description of inapplicability

If protection of data transmission is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

6 Integrity-Input control

6.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter “Yes” or “No”)	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Inputs/changes of personal information are logged		Click here to insert
2	Regular (indiscriminate) evaluation of log files to detect unusual inputs		Click here to insert

6.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of ensuring the integrity of the input control?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)
1	Inputting responsibilities specified in organizational structure	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

6.3 Description of inapplicability

If the integrity of input control is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

7 Integrity-Other measures to ensure the integrity of systems and services

7.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter "Yes" or "No")	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	System hardening measures are implemented (e.g. limitation / deactivation of unnecessary permissions, ports, protocols, servers)		Click here to insert
2	Multi-tenant capability: Segregation at the data level		Click here to insert
3	The inputting of data is validated on the basis of semantic criteria (semantic input validation)		Click here to insert
4	All data held in all systems is regularly checked for malware		Click here to insert

7.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of ensuring the integrity of other systems and services?

No.	Additional measure	Whether the measure has been taken (Enter "Yes" or "No")
1	Multi-tenant capability implemented by dedicated physical servers	
2	Multi-tenant capability implemented by separation at the system level	
3	Description of the implementation of tenant segregation	
4	Use of a mobile device management solution for smartphones	
5	System hardening regarding shared virtual machines and/or application instances	
6	Received data and programs that are automatically checked for malware before being opened (on-access scan)	
7	Data loss prevention solutions are used	
8	Purpose attributes have been defined for data fields and sets	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

7.3 Description of inapplicability

If other measures ensuring the integrity of systems and services are not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

8 Availability-Ensuring the Availability of Personal Information

8.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter "Yes" or "No")	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Redundant IT systems are in place (end devices, servers, storage etc.)		Click here to insert
2	Technical protection systems for fire protection, power supply, air conditioning		Click here to insert
3	Server rooms and data processing centers have fire and smoke alarms		Click here to insert
4	Server rooms and data processing centers have fire extinguishers or fire extinguishing systems		Click here to insert
5	Server rooms and data processing centers have systems for monitoring temperature and humidity		Click here to insert
6	System status is regularly checked (monitoring)		Click here to insert

8.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of ensuring the availability of personal information?

No.	Additional measure	Whether the measure has been taken (Enter "Yes" or "No")
1	Uninterrupted power supply (UPS)	
2	Differently designed IT systems are in place (same functionality from different manufacturers)	
3	Regular stock checks carried out for print-outs and storage media	
4	Contingency plans in place	
5	Documentation of contingency plan tests	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

8.3 Description of inapplicability

If the availability of the personal information is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

9 Availability-Deletion

9.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter "Yes" or "No")	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Feasibility of implementation of deletion periods for controller's personal information according to the specifications by the controller		Click here to insert
2	Definition and documentation of procedures to dispose of and destroy data storage media		Click here to insert

9.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of ensuring the unavailability of the data deleted?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)
1	Documentation of a deletion concept for processing on behalf	
2	Implementation of regulations for the disposal of storage media	
3	Integrity control for deletions or deletion routines	
4	Deletion implemented for development, test and production environments	
5	Shredder (min. Level 3, cross cutting) for paper documents	
6	External shredder (DIN 32757)	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

9.3 Description of inapplicability

If ensuring the unavailability of data deleted is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

10 Resilience-Safeguard against disruptions (continuity assurance)

10.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter “Yes” or “No”)	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Virus scanner with up-to-date search patterns on all end-user devices		Click here to insert
2	Patch management process (among others update plan for the software used)		Click here to insert
3	Use of firewall systems (e.g. at the central transition to the internet, securing databases on web servers)		Click here to insert

10.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of ensuring resilience and preventing system disruption?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)
1	Load balancer	
2	Redundant IT systems	
3	Execution of penetration tests (in other applications for web applications)	
4	Regulated process for proper configuration of firewall systems, including shares / exceptions	

5	Data storage in a RAID system	
6	Intrusion Detection Systems	
7	Intrusion Prevention Systems	
8	Measures to improve the error tolerance of systems and services	
9	For websites and web applications: A Content Security Policy (CSP) has been defined and implemented	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

10.3 Description of inapplicability

If the standard preventing disruptions is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

11 Resilience-Restarting and restoring of availability

11.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter “Yes” or “No”)	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Back-up and restarting concept (data backed up regularly)		Click here to insert

11.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of ensuring restarting and recovering of availability?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)
1	Appropriate physical storage of backup media (e.g. safe, fire protection, spatial separation)	
2	Appropriate protection of backups against encryption by ransomware	
3	Restart concept (measures to restore availability immediately in the event of system failure)	
4	Documented and tested emergency operational concept (IT service continuity)	
5	Documented and established Business Continuity Management	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

11.3 Description of inapplicability

If the standard of restarting and restoring availability is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

12 Organizational measures and processes-Organizational Security Measures

12.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter "Yes" or "No")	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	The roles and responsibilities in the field of data security are described, staffed and known internally		Click here to insert
2	Implementation of an appropriate information security management system		Click here to insert
3	Existence of adequate incident management (response to security breaches)		Click here to insert
4	An attack identification and reporting is in place (incident response)		Click here to insert
5	Information about technical vulnerabilities about the systems and software (assets) used is collected and assessed in terms of impact		Click here to insert
6	Classification of all information according to its protection needs (e.g. confidentiality, availability, integrity)		Click here to insert
7	Only synthetic data, i.e. no genuine or personal information, is processed in the test and development environment		Click here to insert
8	Prohibition of the storage of personal information in source code (repositories)		Click here to insert
9	Regular verification of the intended use of information and IT systems (e.g. audits by IT security or data protection officers)		Click here to insert
10	Process for regular review of the effectiveness of all protective measures and, where appropriate, their adaption (PDCA cycle)		Click here to insert

12.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of organization security measures?

No.	Additional measure	Whether the measure has been taken (Enter "Yes" or "No")
1	Security guidelines for the handling of information are defined, adopted by the management and communicated to the employees	
2	Implementation of a Change Management process for IT systems documents in the context of this Agreement	
3	Awareness measures for all users regarding data protection and data security	
4	Training measures or appropriate in-house education in data protection	
5	Separation of production systems and development / test systems	
6	Regulations on the mobile / private use of terminal devices (e.g. smartphones, notebooks) by employees have been made	
7	Legal department and information technology department in place	

8	Relevant information security management qualifications: such as ISO27001, multi-level protection certification GB / T 22239, please provide qualification certifications)	
9	Management and implementation process of personal information security incidents	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

12.3 Description of inapplicability

If the standard of organizational security measures is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

13 Organizational measures and processes-Monitoring of Assignment

13.1 Basic measures

No.	Basic measure	Whether the measure has been taken (Enter “Yes” or “No”)	Basic measures are mandatory, please state your reasons or alternatives if the basic measure has not been taken.
1	Documentation of all subprocessors used to process the personal information for the purpose of this Agreement		Click here to insert

13.2 Additional measures

In addition to the basic measures listed in the Personal Information Processing on Behalf Agreement, which of the following measures have been implemented for the purpose of monitoring of assignment?

No.	Additional measure	Whether the measure has been taken (Enter “Yes” or “No”)
1	There are historicized and versioned service level agreements (SLAs) with relevant entrusted processors	
2	There is a quality management system at the relevant subprocessors that fully covers processing on behalf	
3	There is an information security management system (ISMS) among the relevant subprocessors that fully covers processing on behalf	
4	All relevant subprocessors have established certification in the field of information security (e.g. ISO 27001, TISAX, SOC 2, BSI IT-Grundschutz)	
5	Regular monitoring of relevant subprocessors by submitting self-assessments	
6	Regular third-party checks of relevant subprocessors (e.g. auditors, data protection auditors)	
7	Regular inspection of the relevant subprocessors by examining contracts with (further) subprocessors	
8	The implementation of checks at subcontractors	
9	The existence of internal policies and work instructions for processing on behalf	

If none of the additional measures has been taken, please state the alternatives or reasons

(Please add here if necessary)

13.3 Description of inapplicability

If the standard of monitoring of assignment is not relevant to the service subject to the Agreement, please briefly state the reasons and/or provide additional remediation control descriptions below:

(Please use an additional sheet if necessary)

Part C. Approved Subcontractors (if applicable)

1 Approved Subcontractors

Subcontractor name, address	
Name	Click here to insert
Address	Click here to insert
Contact person	Click here to insert
Contact Information	Click here to insert

2 Brief description of the function carried out by the subcontractor

Click here to insert

(Provide other details of subcontractors)

The Entrusted Party offers assurance that the subcontractors listed here are bound by the obligations of the **Personal Information Processing on Behalf Agreement** and have implemented corresponding data protection and information security measures specified in Part B.