Article 28 (3) General Data Protection Regulation (GDPR) Controller Processor Agreement

between

Party 1
(hereinafter referred to as processor – [insert name and contact details])

and

Party 2
(hereinafter referred to as controller [insert name and contact details])

Preamble

The Controller would like to task the Processor with the services outlined in § 3 of this Agreement. Contract implementation also includes the processing of personal data. The General Data Protection Regulation (GDPR), particularly Article 28, places certain requirements on processing of personal data carried out on behalf of a controller. To comply with these requirements, the Parties hereby enter into the following agreement. The implementation of the Agreement shall not be compensated separately, unless explicitly stated otherwise.

§ 1 Definitions

Terms used in this Agreement which are defined by Article 4, 9 and 10 GDPR shall have the same meaning as those established by the relevant GDPR provision.

§ 2 Representatives in the European Union

[if applicable:] As representative under Article 27 (1) GDPR, the Processor has appointed

---

Surname, first name, company (if applicable), e-mail, phone number (if applicable) of the Representative.

§ 3 Object

(1) On behalf of the Controller and based on the Contract agreed to on [DD/MM/YYYY] ("Principal Agreement"), the Processor shall carry out services in the following sectors for the Controller:

---------- .

In doing so, the Processor shall gain access to personal data and shall process said data exclusively on behalf of and according to the instructions given by the Controller, unless otherwise required by EU law or a legal provision of one of the Member States applicable to the Processor. The scope and purpose of the Processor's data processing are as concluded in the Principal Agreement (and, if applicable, the corresponding service description), as well as described in **Annex 1** to this Agreement. The Controller shall be the sole judge of the lawfulness of the processing under Article 6 (1) GDPR.

(2) The Parties have agreed to the following in order to specify their mutual rights and obligations under data protection law. In case of doubt, the provisions of this Agreement shall supersede the provisions of the Principal Agreement.

(3) The provisions laid out by this Agreement shall be applicable to all activities which are performed in connection with the Principal Agreement and by the Processor, their employees or agents when encountering personal data originating from, collected for or otherwise processed on behalf of the Controller.

(4) The duration of this Agreement shall be the same as the duration of the Principal Agreement, unless the following provisions stipulate further obligations or rights of termination.

(5) Any agreed-upon data processing shall take place solely in a Member State of the European Union or in the state of another Contracting Party to the Agreement about the European Economic Area. Any relocation of any or whole part of the service to a Third country may only occur if the special requirements of Article 44 et seq. GDPR are fulfilled, and shall be subject to the Controller's prior agreement in writing or documented electronic format.

§ 4 Nature of the data processed, group of data subjects

In applying the Principal Agreement, the Processor shall receive access to the personal data specified in **Annex 1**, belonging to the group(s) of data subjects also specified in **Annex 1**. This data includes

[Option 1:] no special categories of personal data

[Option 2:] as the specified in **Annex 1** and marked as such.

§ 5 Right to instruct

(1) The Processor may only collect, use or otherwise process data within the scope of the Principal Agreement and according to the Controller's instructions; this is particularly applicable with regard to transfer of personal data to a Third country or to an international organisation. If the Processor must carry out further processing due to EU law or the law in an EU Member State applicable to the Processor, the Processor shall notify the Controller of these legal requirements before any such processing takes place.

(2) The Controller's instructions shall be initially determined by this Agreement, though it may be changed, amended or replaced by individual instructions in written or documented electronic format ("Individual Instruction"). The Controller shall have the right to issue such instructions at any time. Changes may include instructions regarding the rectification, erasure and blocking of data. Persons authorised to give, or respectively receive, instructions are specified in **Annex 5**. In case of a change or longer-term hindrance of the designated persons, the successor or substitute shall be made known to the other Contracting Party without undue delay. Text form notification as mandated by Sect. 126b German Civil Code shall be sufficient.

(3) The Controller and Processor shall document all instructions given and keep such documentation for the duration of their validity, and for three full calendar years thereafter. Instructions going beyond the service as agreed-upon by the Principal Agreement shall be deemed a Change Request. [if applicable:] Arrangements regarding possible compensation of additional expenses resulting from supplementary instructions given to the Processor by the Controller shall remain unaffected.

(4) Should the Processor suspect that an instruction given by the Controller goes against data protection requirements; the Processor shall notify the Controller accordingly without undue delay. The Processor is entitled to suspend execution of the instruction in question until confirmation or change by the Controller is received. The Processor is entitled to refuse execution of an evidently unlawful instruction.

§ 6 Protective measures by the Processor

(1) The Processor shall comply with legal data protection requirements and shall not transfer or make accessible to third parties information originating in the Controller's sphere. Taking into account the state of the art, documents and data shall be appropriately secured against accessibility by unauthorised persons.

(2) In regards to its area of responsibility, the Processor shall shape its internal organisation in a manner that is compliant with the special requirements of data protection. The Processor shall also ensure that it has implemented all necessary technical and organisational measures under Article 32 GDPR; particularly in regards to the measures specified in **Annex 2**. Insofar as the processing includes special categories of personal data, the Processor shall additionally implement the adequate and specific measures laid down by para. 22 sect. 2 of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). Upon the Controller's request, the Processor shall disclose the particulars of how these measures are determined and implemented.

The Processor reserves the right to change the implemented security measures, provided that it ensures that these do not fall short of the contractually agreed upon level of protection.

(3) As

[Option 1] Data Protection Officer

[Option 2] Advisor for data protection (*if the Processor is not obligated to appoint a Data Protection Officer under Article 37 (1) GDPR)*

the Processor has appointed:

---

first name, surname, e-mail (relating to the role (no personal email necessary)), phone no.

---

regarding an external Data Protection Officer, add the following: company, address

(4) The persons tasked with data processing and employed by the Processor are prohibited from collecting, using or otherwise processing personal data without authorisation. The Processor shall ensure that all persons (hereafter referred to as "personnel") tasked with processing and fulfilling this Agreement have committed themselves according to the obligation of confidentiality under Article 28 (3) lit. b GDPR). The Processor has a duty to instruct personnel about the special data protection obligations arising from this Agreement, as well as the existing purpose limitation and binding commitment to instructions. The Processor shall take due care to ensure compliance with the abovementioned obligation. Obligations shall be composed to remain in force beyond the termination of this Agreement or of the employment relationship between the employee and the contractor. Upon the Controller's request, the Processor shall provide proof of these obligations in an adequate manner.

(5) The processing of data under this Agreement in private homes (telework or home-office by the Processor's personnel) shall only be permitted with the Controller's consent. When data is processed in a private home, prior employer access to the employee's apartment for control purposes must be contractually ensured. Compliance with the protective measures pursuant to Article 6 (1) and (2) of this Agreement and with the provisions of Article 32 GDPR shall also be ensured in this case.

§ 7 Processor Information Obligations

(1) In case of disturbances, suspected data breaches, breaches of contractual obligations on the part of the Processor, suspected security incidents or other irregularities with regards to the processing of personal data by the Processor, by persons tasked within the framework of the Agreement or by third persons, the Processor shall inform the Controller accordingly in writing or in a documented electronic format without undue delay. The same applies to audits of the Processor carried out by the Data Protection Authority. To the extent possible, notification about a personal data breach shall contain the following information:

a) a description of the nature of the personal data breach including, where possible, the categories and number of data subjects potentially affected, and the categories and number of personal data records concerned;

b) a description of the likely consequences of the personal data breach, and

c) a description of the measures taken or proposed by the Processor to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

(2) The Processor shall take all necessary measures to secure the data and mitigate possible adverse effects on the data subject(s) without undue delay. The Processor shall also inform the Controller of these measures and request further instructions.

(3) Additionally, insofar as the Controller's data is concerned by a breach outlined in § 7 (1) of this Agreement, the Processor shall provide details to the Controller at any time.

(4) The Processor shall, in an adequate manner, assist the Controller in ensuring compliance with the Controller's obligations under Articles 33 and 34 GDPR (Article 28 (3) sent. 2 lit. f GDPR). The Processor shall only execute notifications under Articles 33 or 34 GDPR on behalf of the Controller upon the Controller's prior instruction as outlined in § 5 of this Agreement.

(5) In case the Controller's data is put at risk due to seizure or confiscation taking place at the Processor's, because of insolvency or composition proceedings or because of other events or measures taken by third parties, the Processor shall inform the Controller accordingly and without undue delay, unless prohibited from doing so by court or administrative order. In this context, the Processor shall, without undue delay, inform all competent entities that, as "Controller" under the GDPR, the Controller bears sole decision-making authority with regard to the data.

(6) In case of substantial changes to the security measures under § 6 (2) of this Agreement, the Processor shall notify the Controller accordingly, without undue delay.

(7) In case of a change of the person fulfilling the role of the

[Option 1:]Data Protection Officer

[Option 2:] Advisor for data protection

the Processor shall, without undue delay, notify the Controller accordingly.

(8) The Processor, and if applicable, his representative, shall maintain a record of all processing activities carried out on behalf of the Controller, containing all specifications required under Article 30 (2) GDPR. The record shall be made available to the Controller upon request.

(9) The Processor shall, to adequate extent, also contribute to the record the Controller establishes regarding the processing activities. The Processor shall also contribute to any data protection impact assessment the Controller establishes under Article 35 GDPR, and if applicable, when a prior consultation of supervisory authorities under Article 36 GDPR takes place. The Processor shall in each case convey the necessary specifications to the Controller in an appropriate manner.

§ 8 Control rights of the Controller

(1) Prior to the start of the data processing, and then on a regular basis, the Controller shall convince himself of the technical and organisational measures taken by the Processor. To this end, he can, for example, obtain information from the Processor or require seeing existing attestations by experts, certifications or of internal audits. The Controller may, after timely coordination and during normal business hours, also personally check the Processor's technical and organisational measures or have them checked by an expert third party, unless the latter is in a competitive relationship with the Processor. The Controller shall conduct controls only to the extent necessary so as to not unduly disturb the Processor's business operations.

(2) Upon the Controller's verbal, written or electronic request, the Processor shall, in a timely manner, provide him with all information and records necessary for controlling the Processor's technical and organisational measures.

(3) The Controller shall document the control result and notify the Processor accordingly. In case of mistakes or irregularities detected by the Controller, particularly when assessing order results, the Controller shall inform the Processor accordingly without undue delay. If the control reveals issues to be avoided in the future that require changes to the ordered process, the Controller shall, without undue delay, notify the Processor of the necessary changes.

(4) Upon request, the Processor shall provide the Controller with a comprehensive and up-to-date data protection and security concept for the data processing and regarding authorised persons for access.

(5) Upon request, the Processor shall provide the Controller with the employee obligation under § 6 (4) of this Agreement.

[Optional: (6) The Controller shall reimburse the Processor for the expenses incurred in the course of the control.]

§ 9 Engagement of subcontractors

(1) [Option 1:] Within the framework of its contractual obligations, the Processor shall not be entitled to establish subprocessing relationships with subcontractors ("Subcontracting Relationship").

[Option 2:] The contractually agreed-upon services, or the parts of the services described hereafter, will be executed with the aid of subcontractors named in **Annex 4**. Within the scope of his contractual obligations, the Processor shall be entitled to establish further subcontracting relationships, provided that the Controller agrees in writing or documented electronic format prior to the assignment of the subcontractor and the Controller is notified as to such relationship in advance. The Processor shall carefully select subcontractors according to their suitability and reliability. When engaging subcontractors, the Processor shall ensure their commitment to confidentiality in line with the provisions of this Agreement and ensure that the Controller is able to directly exercise its rights under the Agreement (particularly the rights of audit and control) against the subcontractors. If subcontractors from a third country are involved, the Processor shall ensure that an adequate level of data protection is guaranteed by the subcontractor in question (for example, by establishing an agreement according to the EU standard data protection clauses). Upon request, the Processor shall demonstrate the conclusion of the aforementioned agreements with his subcontractors.

[Option 3:] The contractually agreed-upon services, or the parts of the services described hereafter, will be executed by involving the subcontractors named in **Annex 4**. Within the scope of his contractual obligations, the Processor shall be entitled to establish further subcontracting relationships. The Processor shall, without undue delay, notify the Controller thereof. The Processor shall carefully select subcontractors according to their suitability and reliability. When engaging subcontractors, the Processor shall ensure their commitment to confidentiality in line with the provisions of this Agreement and ensure that the Controller is able to directly exercise its rights under the Agreement (particularly the rights of audit and control) against the subcontractors. If subcontractors from a third country are involved, the Processor shall ensure that an adequate level of data protection is guaranteed by the subcontractor in question (for example, by establishing an agreement according to the EU standard data protection clauses). Upon request, the Processor shall demonstrate the conclusion of the aforementioned agreements with his subcontractors.

(2) When the Processor charges a third party with a purely ancillary service, this shall not constitute a subcontractor relationship within the meaning of these provisions. . Such ancillary services include, but are not limited to, postal, transport and shipping services, cleaning services, security services, and telecommunications services without concrete reference to services provided by the Processor provides to the Controller. Maintenance and testing services constitute subcontractor relationships requiring approval insofar as they are provided for IT systems also used in connection with the Processor's provision of services on behalf of the Controller.

§ 10 Data subject inquiries and rights

(1) The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligations as established under Articles 12-22, 32, and 36 GDPR.

(2) If a data subject asserts her rights regarding to her data directly against the Processor, the Processor shall not react independently. Rather, the Processor shall refer the data subject to the Controller without undue delay and wait on the Controller for instructions on how to proceed.

[Optional: (3) The Controller shall reimburse the Processor for the expenses incurred in the course of the supportive services.]

§ 11 Liability

(1) The Controller and the Processor shall be liable to the data subjects in accordance with the provisions of Article 82 GDPR. The Processor shall coordinate with the Controller regarding any possible fulfilment of liability claims.

(2) At first request, the Processor shall exempt the Controller from all claims data subjects assert against the Controller due to the breach of an obligation imposed on the Processor by the GDPR, or due to the Processor's failure to comply with an instruction outlined in this Agreement or given separately by the Controller.

(3) The Parties shall each release themselves from liability if/insofar as one Party proves that they are in no way responsible for the circumstance through which the damage occurred to a data subject. Apart from that, Article 82 (5) GDPR shall apply.

(4) Unless otherwise stipulated above, the liability within the scope of this Agreement shall correspond to that of the Principal Agreement.

§ 12 Right to extraordinary termination

The Controller may terminate the Principal Agreement, in whole or in part, without notice if the Processor fails to fulfil his obligations under this Agreement, intentionally or through gross negligence violates the provisions of the DS-GVO or other applicable data protection provisions, is unable or unwilling to execute an instruction given by the Controller, or opposes the Controller's rights of control in a manner contrary to the contractual terms. In particular, failure to comply with the obligations agreed in this contract and derived from Art. 28 DS-GVO constitutes a serious infringement.

§ 13 Termination of the Principal Agreement

(1) After termination of the Principal Agreement, or at any time upon the Controller's request, the Processor shall return to the Controller all documents, data and data carriers made available to him or delete them at the Customer's request, unless such deletion is prohibited by EU law or the laws of the Federal Republic of Germany. This also applies to any data backups made by the Processor. The Processor must provide documentation of proper deletion of any data still available.

[Optional: Documents to be disposed of must be destroyed with a document shredder in accordance with DIN 32757-1. Data media to be disposed of must be destroyed in accordance with DIN 66399.]

(2) The Controller has the right to verify that the Processor has completed the contractually correct return or deletion of the data in an appropriate manner. Conversely, the Controller may have such verification done through an expert third party, provided that the third party is not in a competitive relationship with the Processor.

(3) The Processor must retain the confidentiality of any data that has become known to it in connection with the Principal Agreement beyond the end of the Principal Agreement. This Agreement shall remain valid beyond the end of the Principal Agreement for as long as the Processor has personal data supplied by or collected for the Controller at the Processor's disposal.

§ 14 Final provisions

(1) The Parties agree that the Processor's right to assert retention under Section 273 of the German Civil Code (Bürgerliches Gesetzbuch, BGB) is excluded with regard to the data to be processed and the corresponding data carriers.

(2) [Option 1:] To be valid, any changes and amendments to this Agreement must be rendered in writing. This applies also to a change of this formal requirement. The written form may not be replaced by an electronic form (Sections 126 (3), 126a of the German Civil Code) or text form (Section 126b of the German Civil Code).

[Option 2:] To be valid, any changes and amendments to this Agreement must be rendered in writing in a documented electronic format. This also applies to a change in this formal requirement

This shall not apply to the priority of individual contract agreements.

(3) Should any provision of this Agreement be invalid or become partially or entirely invalid or unenforceable, the remainder of this Addendum shall remain valid and in force.

(4) This agreement shall be governed by and construed in accordance with German Law. Each Party agrees to submit to the sole jurisdiction of

---

[place of jurisdiction].

Annexes:

Annex 1 – Description of the data subjects/groups of data subjects as well as the data/data categories requiring special protection

Annex 2 – Technical and organisational measures by the Processor

Annex 3 – Approved Subcontractors

Annex 4 – Persons allowed to issue/receive instructions

For the Controller:	For the Processor:
----------	----------
(Surname, first name, role (CEO etc.))	(Surname, first name, role (CEO etc.))
----------	----------
Place and date, signature	Place and date, signature

Annex 1 – Description of the data subjects / groups of data subjects as well as the data / data categories requiring special protection
[for example employees, suppliers, clients etc.]
[for example first name, surname, e-mail address etc.]

Annex 2 – Technical and organisational measures by the Processor

Annex 3 – Approved Subcontractors
The following companies are approved subcontractors under § 9 of this Agreement:
[COMPANY WITH NAME, LEGAL FORM, CONTACT DATA AND ADDRESS TO WHICH A SUMMONS MAY BE SERVED]

Annex 4 – Persons allowed to issue / receive instructions and communication channels for instructions
The following person(s) shall be allowed to issue instructions for the Controller:

For the Processor, shall be recipient(s) of instructions:

Communication channels to be used for instructions:

(exact (post) mailing address / e-mail / phone no.)