

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

[REDACTED]

(Name des beauftragten Unternehmens)

(nachfolgend „**Auftragsverarbeiter**“ im Sinne des Art. 4 Nr. 8 DSGVO)

und

[REDACTED]

(Name der beauftragenden Konzern Gesellschaft)

(nachfolgend „**Verantwortlicher**“ im Sinne des Art. 4 Nr. 7 DSGVO)

über die Verarbeitung personenbezogener Daten im Auftrag.

1. Allgemeines

Der Auftragsverarbeiter verarbeitet personenbezogene Daten für den Verantwortlichen im Auftrag. Der Verantwortliche hat den Auftragsverarbeiter im Rahmen der Sorgfaltspflichten des Art. 28 DSGVO als Dienstleister hierfür ausgewählt. Voraussetzung für die Zulässigkeit einer Auftragsverarbeitung ist, dass die Verarbeitung auf Grundlage eines Vertrages erfolgt, der den Auftragsverarbeiter an den Verantwortlichen bindet und der den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Dieser Vertrag regelt vor diesem Hintergrund die Rechte und Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung („Auftrag“). Für das Verständnis dieses Ver-

Contract for Processing pursuant to Art. 28 GDPR

between

[REDACTED]

(name of the company performing the data processing as ordered)

(hereinafter '**Processor**' pursuant to Art. 4 para. 8 GDPR)

and

[REDACTED]

(name of the group company ordering the data processing)

(hereinafter '**Controller**' pursuant to Art. 4 para. 7 GDPR)

regarding the processing of personal data on behalf of the Controller.

1. General

The Processor processes personal data for and on behalf of the Controller. The Controller has selected the Processor as service provider with due diligence pursuant to Art. 28 GDPR. Processing is permissible only provided that it is based on a contract that is binding on the Processor with regard to the Controller and that sets out the subject-matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects and the rights and obligations of the Controller. Based on this understanding, the present contract stipulates the rights and obligations of the parties relating to the data processing ('Order'). The terms used in this contract shall have the meaning as defined in Art. 4 GDPR.

trags sind für die jeweiligen Begrifflichkeiten die Definitionen des Art. 4 DSGVO maßgeblich.

2. Gegenstand und Dauer des Vertrages

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich [...] auf Grundlage des Vertrags vom [...] („Hauptvertrag“). Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, welche dieser ausschließlich im Auftrag und nach Weisung des Verantwortlichen zu verarbeiten hat.

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter beauftragte Unterauftragsverarbeiter mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Vertrages nicht länger fortwährende Verpflichtungen ergeben.

Ergänzend und ggf. abweichend zu sonstigen Kündigungsregelungen kann der Verantwortliche diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein vorsätzlicher oder fahrlässiger schwerwiegender Verstoß des Auftragsverarbeiters gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter den Zutritt des Verantwortlichen oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

Die Erbringung der Leistungen unter diesem

2. Object and Term of the Order

Based on the contract dated [...] ('Master Contract'), the Processor will provide services in the area of [...] to the Controller. In this context, the Processor will be provided access to personal data and agrees that he will process these data solely on behalf of the Controller and in accordance with the Controller's instructions.

The object, nature and purpose of the processing, the type of personal data and the categories of persons affected are determined in **Appendix 1** to this contract.

The provisions of this contract apply to any and all activities undertaken in connection with the Master Contract that result in the Processor and his employees, or subcontractors as contracted by the Processor, having access to personal data that originate with the Controller or that have been collected for the Controller. The term of this contract depends on the term of the Master Contract unless the provisions of this contract stipulate obligations of a longer duration.

In addition to and, if applicable, in divergence from other regulations governing termination, the Controller can terminate this contract at any time and without notice in case of intentional or negligent serious breach of applicable data protection rules or of obligations under this contract on the part of the Processor, or if the Processor is not able or not willing to carry out instructions given by the Controller, or if the Processor denies access to the Controller or to the responsible supervisory authority in violation of his contractual duties.

Services under this Contract shall be provided exclusively in Member States of the European

<p>Vertrag erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR).</p> <p>Jede Verarbeitung von Daten in einem Drittstaat bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die Voraussetzungen der Art. 44 ff. DSGVO gegeben sind. Insbesondere bedarf es eines angemessenen Schutzniveaus im Drittland. Dieses kann insbesondere durch einen Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 Abs. 3 DSGVO), verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DSGVO), genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. c/d DSGVO), Zertifikate auf Basis eines genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO) oder sonstige anerkannte Maßnahmen versichert werden.</p> <p>3. Pflichten des Auftragsverarbeiters</p> <p>Der Auftragsverarbeiter gewährleistet die Einhaltung der ihm im Rahmen dieses Vertrages sowie der im Rahmen der gesetzlichen Regelungen, insbesondere der Art. 28 bis 32 DSGVO, auferlegten Pflichten im Zusammenhang mit der Datenverarbeitung. Insbesondere treffen ihn die folgenden Pflichten:</p> <p>(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und in Übereinstimmung mit geltendem Datenschutzrecht. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den im Hauptvertrag und in Anlage 1 dokumentierten Weisungen des Verantwortlichen. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragsverarbeiter untersagt, es sei denn, dass der Verantwortliche dieser schriftlich zugestimmt hat oder er gesetzlich zur Verarbeitung verpflichtet ist. Der Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen</p>	<p>Union (EU) or in another signatory state to the Agreement on the European Economic Area (EEA).</p> <p>Any processing of data in a third country requires prior consent by the Controller and may only be undertaken if the requirements of Art. 44 et seq. GDPR are met. In particular, the level of data protection in the third country must be adequate. This may be established, in particular, by way of an adequacy decision by the European Commission (Art. 45 para. 3 GDPR), binding corporate rules (Art. 46 para. 2 lit. b in conjunction with Art. 47 GDPR), an approved code of conduct (Art. 46 para. 2 lit. c/d GDPR), certificates based on an approved certification mechanism (Art. 46 para. 2 lit. f in conjunction with Art. 42 GDPR) or other recognised measures.</p> <p>3. Processor's Obligations</p> <p>The Processor warrants that he will comply with the obligations in relation to data processing as stipulated in this contract and by law, in particular with the obligations pursuant to Articles 28 to 32 GDPR. In particular, the Processor shall have the following obligations:</p> <p>(1) The Processor processes personal data solely within the frame of existing agreements with the Controller and in compliance with applicable data protection laws. The purpose, nature and scope of the processing are determined exclusively by the Controller's instructions as documented in the Master Contract and in Appendix 1 hereto. The Processor may not process data in any manner divergent from such instructions unless the Controller has given his consent in writing or the Processor is obliged by law to process the data in such divergent manner. A Processor who determines the purposes and means of processing in a manner that violates such</p>
---	---

<p>diese Weisungen bestimmt, gilt in Bezug auf diese Verarbeitung selbst als Verantwortlicher.</p> <p>(2) Der Auftragsverarbeiter garantiert, dass geeignete technische und organisatorische Maßnahmen (TOMs) gemäß Art. 28 Abs. 3, S. 2 lit. c i.V.m. Art. 32 DSGVO so umgesetzt und eingehalten werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt. Bei den Maßnahmen handelt es sich im Sinne der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 DSGVO um solche der Datensicherheit und zur Gewährleistung eines dem Risiko der Datenverarbeitung angemessenen Schutzniveaus im Hinblick auf die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Datenverarbeitungssysteme. Bei der Planung und Implementierung der Maßnahmen sind der Stand der Technik, die Implementierungskosten, Art, Umfang und Zwecke der Verarbeitung sowie die Wahrscheinlichkeit des Eintritts und der Schwere zu prüfender Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Der Auftragsverarbeiter ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnissnahme Dritter geschützt sind. Die bei Vertragsschluss aktuellen TOMs ergeben sich aus Anlage 2 zu diesem Vertrag. Der Auftragsverarbeiter verpflichtet sich, die Maßnahmen nach diesem Maßstab während der Datenverarbeitung laufend zu überprüfen. Er ist berechtigt, etwaige Anpassungen eigenverantwortlich vorzunehmen. Der Auftragsverarbeiter garantiert hierbei, dass das Sicherheitsniveau der im Ausgangspunkt festgelegten Maßnahmen infolge der Anpassung der Maßnahmen zu keinem Zeitpunkt unterschritten wird. Etwaige Anpassungen der TOMs hat der Auftragsverarbeiter dem Verantwortlichen innerhalb angemessener Frist schriftlich mitzuteilen.</p> <p>(3) Der Auftragsverarbeiter ist nicht befugt, Rechte betroffener Personen eigenmächtig wahrzunehmen. Insbesondere darf er über Daten, die er im Auftrag für den Ver-</p>	<p>instructions is considered as Controller in respect of that processing.</p> <p>(2) The Processor warrants that appropriate technical and organisational measures (TOMs) pursuant to Art. 28 para. 3, 2nd sentence lit. c in conjunction with Art. 32 GDPR will be implemented and observed in a manner that ensures processing in compliance with the requirements of the GDPR. These measures are (pursuant to the principles relating to processing of personal data under Art. 5 GDPR) measures of data security and measures designed to ensure a level of security appropriate to the risk of the data processing relating to confidentiality, integrity, availability and resilience of the processing systems. Planning and implementation of such measures shall take into account state-of-the-art technology, implementation costs, nature, scope and purposes of the processing, and the probability and severity of risks to the rights and freedoms of natural persons. The Processor is obliged to organise his company and operating processes in a manner to ensure that the data processed on behalf of the Controller is secured and protected against unauthorised third parties gaining knowledge, with protective measures as required by the individual case. The TOMs applicable at the time this contract enters into force are listed in Appendix 2. The Processor agrees to carry out on-going monitoring of the measures during the processing in order to verify that they meet the aforementioned standard. The Processor may, under his own responsibility, effect adaptations. The Processor warrants that the security provided by the measures initially determined will not, at any time, fall below the level as initially determined as a consequence of such adaptations. The Processor shall inform the Controller of any adaptations of the TOMs in writing and within a reasonable time frame.</p> <p>(3) The Processor may not defend interests of data subjects on his own authority. In particular, the Processor may only give out information about data he is processing on</p>
---	--

antwortlichen verarbeitet, nur nach dokumentierter Weisung des Verantwortlichen Auskunft erteilen und solche berichtigen, löschen oder deren Verarbeitung einschränken. Sofern sich eine betroffene Person diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, hat dieser dem Verantwortlichen die erforderlichen Informationen zur Bearbeitung des Anliegens unverzüglich schriftlich zukommen zu lassen. Der Auftragsverarbeiter hat den Verantwortlichen mit allen erforderlichen Mitteln und Maßnahmen bei der Umsetzung der Betroffenenrechte der Art. 12 bis 23 DSGVO zu unterstützen, insbesondere diesbezügliche Weisungen seitens des Verantwortlichen unverzüglich umzusetzen.

(4) Der Auftragsverarbeiter verpflichtet sich auf die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3, S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten des Verantwortlichen befassten Mitarbeitern und anderen für den Auftragsverarbeiter tätigen Personen untersagt ist, die Daten ohne oder entgegen der Weisung des Verantwortlichen zu verarbeiten. Ferner gewährleistet der Auftragsverarbeiter dass die zur Verarbeitung der personenbezogenen Daten befugten Personen schriftlich zur Vertraulichkeit verpflichtet worden und hinsichtlich der für sie relevanten Bestimmungen zum Datenschutz ausreichend geschult worden sind. Die Vertraulichkeitsverpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Vertrages, welcher der Tätigkeit einer Person für den Auftragsverarbeiter zugrunde liegt, bestehen bleiben. Dem Verantwortlichen sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

(5) Der Auftragsverarbeiter bestätigt, dass er, soweit erforderlich, einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 bis 39 DSGVO, § 38 BDSG bestellt hat und benennt diesen in **Anlage 4** gegenüber dem Verantwortlichen mit allen Kontaktdaten, die eine unmittelbare Kontaktaufnahme seitens des Verantwortlichen ermöglichen:

(6) Ein Wechsel des Datenschutzbeauftragten oder seiner Kontaktdaten wird dem

behalf of the Controller, and may only correct, erase or limit the processing of data, if the Controller has instructed the Processor to do so and such instruction is documented. Should a data subject approach the Processor directly concerning the aforementioned, the Processor must convey to the Controller the information required to respond to the data subject's query without delay and in writing. The Processor is obliged to assist the Controller, by all means and measures required, in implementing the rights of data subjects pursuant to Articles 12 to 23 GDPR; this obligation comprises, in particular, a duty to implement without delay any instructions by the Controller.

(4) The Processor agrees to comply with the confidentiality requirements pursuant to Articles 28 para. 3, 2nd sentence lit. b, 29, 32 para. 4 GDPR. The Processor warrants that his employees tasked with processing the Controller's data and other persons acting on behalf of the Processor are prohibited from processing the data without respective instructions by the Controller or in contravention of the Controller's instructions. The Processor furthermore warrants that any persons authorised to process personal data are bound by written confidentiality obligations and that they have been adequately trained with regard to data protection provisions relevant to their activities. The confidentiality obligations must be worded in such a way that they remain in force even after termination of this contract or after termination of the contract on which the activity of a person for the Processor is based. Upon request by the Controller, the Processor must show appropriate proof of these obligations.

(5) The Processor confirms that he has appointed a data protection officer pursuant to Articles 37 to 39 GDPR and § 38 German Federal Data Protection Act (BDSG), provided such is necessary, and in **Appendix 4** will furnish the Controller with all contact details that enable the Controller to contact such data protection officer directly.

(6) Should a new data protection officer be appointed, or should the contact details change, the Processor will inform the Control-

<p>Verantwortlichen unverzüglich schriftlich mitgeteilt. Für die Meldung des Datenschutzbeauftragten bei der zuständigen Aufsichtsbehörde ist der Auftragsverarbeiter selbst verantwortlich. Sollte der Auftragsverarbeiter gesetzlich nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet sein, benennt er gegenüber dem Verantwortlichen stattdessen schriftlich einen Ansprechpartner für den Verantwortlichen; dieser kann mit einer weisungsempfangsberechtigten Person unter dieser Ziffer des Vertrags identisch sein. Sofern der Auftragsverarbeiter seinen Sitz außerhalb der Union hat, benennt er in Anlage 4 nach Maßgabe des Art. 27 DSGVO schriftlichen einen Vertreter in der Union.</p> <p>(7) Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen jegliche Störung und jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Verantwortlichen unverzüglich schriftlich oder in Textform mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.</p> <p>Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:</p> <ul style="list-style-type: none"> - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze; - eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen. <p>Der Auftragsverarbeiter ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht diesen um weitere Weisungen.</p>	<p>ler hereof without delay and in writing. The Processor is responsible for notifying the responsible supervisory authority of the data protection officer's details. If the Processor is not obliged by law to appoint a data protection officer, he will instead furnish the Controller in writing with the name of a contact person; such contact person may be identical with a person authorised to receive instructions under this number of the contract.</p> <p>If the Processor is domiciled in a non-EU Member State, he will provide the Controller in writing, in Appendix 4, in accordance with Art. 27 GDPR, the details of a representative domiciled within the EU.</p> <p>(7) The Processor is obliged to notify the Controller, without delay and in writing or in text form, of any disruption and of any violation of data protection laws or regulations, or breach of contractual stipulations, or activity in contravention of the Controller's instructions, that has been committed in the course of the processing by the Processor or other persons engaged in the processing.</p> <p>A notification of a violation of personal data must contain, at minimum, the following information:</p> <ul style="list-style-type: none"> - a description of the type of violation of personal data; this shall include, as far as possible: the category and number of persons affected, the data categories affected, and the number of data sets affected; - a description of the measures taken or proposed by the Processor to remediate the violation and, if applicable, measures to mitigate possible negative consequences. <p>The Processor will implement, without delay, the necessary measures to secure the affected data and to mitigate possible negative consequences for the persons affected, will inform the Controller thereof, and will ask for further instructions.</p> <p>The Controller in turn will notify the Processor without delay if he becomes aware of errors or irregularities in the context of the processing of personal data as carried out by the Processor.</p>
--	--

<p>Der Verantwortliche informiert seinerseits unverzüglich den Auftragsverarbeiter, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter feststellt.</p> <p>(8) Die Verarbeitung von Daten im Auftrag des Verantwortlichen außerhalb von Betriebsstätten des Auftragsverarbeiters oder vertragsgemäß eingesetzten Subunternehmern ist nur mit Zustimmung des Verantwortlichen zulässig. Eine Verarbeitung von Daten für den Verantwortlichen in Privatwohnungen ist nur mit Zustimmung des Verantwortlichen im Einzelfall zulässig. Soweit eine betriebliche Vereinbarung zur Telearbeit vorliegt, gilt die Zustimmung als erteilt.</p> <p>(9) Der Auftragsverarbeiter wird die Daten, die er im Auftrag für den Verantwortlichen verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragsverarbeiter die Daten mit dem jeweiligen Zweck kennzeichnen und getrennt voneinander verarbeiten.</p> <p>(10) An der Erstellung des Verarbeitungsverzeichnisses durch den Verantwortlichen hat der Auftragsverarbeiter mitzuwirken. Er hat dem Verantwortlichen die jeweils erforderlichen Angaben nach Art. 30 DSGVO in geeigneter Weise mitzuteilen. Er hat seinerseits ein Verzeichnis aller Kategorien von Verarbeitungen nach Maßgabe des Art. 30 Abs. 2 DSGVO zu führen, die er im Auftrag des Verantwortlichen durchführt.</p> <p>(11) Der Auftragsverarbeiter verpflichtet sich, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen nach Aufforderung bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, namentlich der Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten, der Durchführung einer Datenschutz-Folgenabschätzung sowie Prüfverfahren und Anhörungen der für den Verantwortlichen zuständigen Aufsichtsbehörde zu unterstützen. Zu diesem Zweck hat er sich stets aus-</p>	<p>(8) The Processor may only process data on behalf of the Controller outside his own premises or those of a subcontractor under this contract if the Controller gives his consent. Processing of data on behalf of the Controller in private accommodation is only permissible in individual cases and with the Controller's consent. In case of a works agreement on teleworking, such consent shall be deemed given.</p> <p>(9) The Processor will tag data he is processing on behalf of the Controller in a suitable manner. In the case of data being processed for diverse purposes, the Processor will tag the data with the respective purpose and will process such data separately.</p> <p>(10) The Processor is obliged to cooperate with the Controller in establishing a processing record. He must furnish the Controller with the necessary information pursuant to Art. 30 GDPR in an adequate manner. The Processor in turn must keep a record of all categories of processing activities carried out on behalf of the Controller pursuant to Art. 30 para. 2 GDPR.</p> <p>(11) The Processor undertakes to assist the Controller, after having been asked to do so and taking into account the manner of processing and the information available to the Processor, in complying with the obligations specified in Articles 32 to 36 GDPR, in particular the obligations to: notify the responsible supervisory authority of violations of rules protecting personal data; notify data subjects of violations of rules protecting personal data; carry out a data protection impact assessment; and cooperate in assessment proceedings and in hearings instigated by the responsible supervisory authority. To this purpose, the Processor must always and exclusively contact the Controller, who will initiate the required steps. In the event that processing services under this Contract become subject</p>
---	--

<p>schließlich an den Verantwortlichen zu wenden, der die erforderlichen Schritte einleiten wird. Über Kontrollhandlungen und sonstige Maßnahmen der Aufsichtsbehörde oder sonstiger staatlicher Stellen, die sich auf die Datenverarbeitung unter diesem Auftrag beziehen, wird der Auftragsverarbeiter den Verantwortlichen stets unverzüglich informieren.</p> <p>(12) Der Auftragsverarbeiter soll dem Verantwortlichen die Person(en)/ Rollen benennen, die zum Empfang von Weisungen des Verantwortlichen berechtigt sind.</p> <p>Weisungsempfangsberechtigte Personen / Rollen des Auftragsverarbeiters sind:</p> <p>a) _____</p> <p>b) _____</p> <p>c) _____</p> <p>d) _____</p> <p>(13) Im Falle einer Inanspruchnahme des Verantwortlichen durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragsverarbeiter den Verantwortlichen bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.</p> <p>4. Umfang der Weisungsbefugnis</p> <p>(1) Der Verantwortliche hat das Recht, dokumentierte Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Die initialen Weisungen ergeben sich aus dem Hauptvertrag und diesem Vertrag. Mündliche Weisungen sind unverzüglich vom Verantwortlichen schriftlich oder in Textform zu bestätigen. Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragsverarbeiter zu erteilen. Dem Auftragsverarbeiter soll eine angemessene Frist zur Umsetzung der Weisungen gesetzt werden. Weisungen, über die hauptvertraglich vereinbarte Leistung</p>	<p>to audit activities and other measures by the supervisory authority or other government authorities, the Processor will inform the Controller without delay.</p> <p>(12)The Processor will notify the Controller of the person(s)/ roles authorised to receive instructions from the Controller.</p> <p>Persons / roles authorised to receive instructions on behalf of the Processor are:</p> <p>a) _____</p> <p>b) _____</p> <p>c) _____</p> <p>d) _____</p> <p>(13) In the event the Controller receives a claim for damages pursuant to Art. 82 GDPR from a data subject affected by the data processing, the Processor agrees to support the Controller in defending against such claims according to his abilities.</p> <p>4. Authority to Issue Instructions</p> <p>(1) The Controller may issue documented instructions regarding the nature, scope and procedure of the processing. The initial instructions are as set forth in the Master Contract and this Contract. Oral instructions must be confirmed by the Controller without delay, in writing or in text form. The Controller may, at any time, issue complementary instructions to the Processor regarding purpose, nature and scope of the processing. The Processor shall receive an appropriate deadline for implementing the instructions. Instructions that exceed the Processor's performance obligations as agreed upon in the Master Contract are deemed to be proposals for a change of performance obligations.</p>
--	---

hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(2) Weisungsberechtigte Personen / Rollen des Verantwortlichen sind:

a) _____

b) _____

c) _____

d) _____

Für den Fall, dass sich die weisungsberechtigten Personen/ Rollen beim Verantwortlichen ändern, wird der Verantwortliche dies dem Auftragsverarbeiter schriftlich mitteilen.

(3) Der Auftragsverarbeiter darf Daten, die dem Verantwortlichen zugeordnet sind, nur im Rahmen des Auftrages und der Weisungen des Verantwortlichen verarbeiten, sofern er nicht gesetzlich zu einer abweichenden Vereinbarung verpflichtet ist (Art. 28 Abs. 3 a) DSGVO). Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung(en) solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird.

5. Unterauftragsverhältnisse

(1) Der Verantwortliche ist damit einverstanden, dass der Auftragsverarbeiter zur Erfüllung seiner vertraglich vereinbarten Leistungen unter diesem Vertrag und dem Hauptvertrag sowohl im Konzernverbund zum Unternehmen des Verantwortlichen als auch des Auftragsverarbeiters stehende Unternehmen zur Leistungserfüllung heranzieht bzw. diese Unternehmen mit Leistungen unterbeauftragt.

(2) Persons / roles authorised to issue instructions on behalf of the Controller:

a) _____

b) _____

c) _____

d) _____

In case of a change of the person(s)/roles authorised to issue instructions on behalf of the Controller, the Controller will notify the Processor hereof in writing.

(3) The Processor may process data that are attributed to the Controller only within the scope of the Order and in compliance with the Controller's instructions, unless he is obliged by law to carry out divergent processing (Art. 28 para. 3 a) GDPR). The Processor will inform the Controller without delay if he considers an instruction issued by the Controller to be in contravention of the law. The Processor may pause the implementation of the instruction(s) in question until such time as these are either confirmed or changed by the Controller.

5. Subcontracting

(1) The Controller agrees that the Processor may engage or subcontract other companies in order to fulfil his obligations under this Contract and under the Main Contract, provided that such other companies belong either to the Controller's company group or to the Processor's company group.

(2) Other companies may be subcontracted only with the Controller's prior written consent. In case of the subcontractors listed in **Appendix 3**, such consent is deemed to be given.

<p>(2) Aufträge an andere Subunternehmer dürfen nur mit schriftlicher vorheriger Einwilligung des Verantwortlichen vergeben werden. Für die in Anlage 3 aufgeführten Subunternehmer gilt die Einwilligung als erteilt.</p> <p>(3) Der Auftragsverarbeiter hat den Subunternehmer sorgfältig auszuwählen und im Vorwege zu prüfen, dass dieser die zwischen Verantwortlichen und Auftragsverarbeiter getroffenen Verpflichtungen einhalten kann und erlegt diesem die Pflichten, die auch für ihn gelten, sowie die seitens des Verantwortlichen erteilten Weisungen im Rahmen einer schriftlichen Vereinbarung auf. Der Auftragsverarbeiter hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragsverarbeiter zu dokumentieren und auf Anfrage dem Verantwortlichen zu übermitteln. Der Auftragsverarbeiter ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser, soweit gesetzlich erforderlich, einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 bis 39 DSGVO, § 38 BDSG bestellt hat. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten bzw. deren Verletzung durch den Subunternehmer. Sollte der Einsatz eines Subunternehmers die Verarbeitung von personenbezogenen Daten in einem Drittstaat erfordern, müssen vor Übermittlung von Daten an den Subunternehmer die besonderen Voraussetzungen der Art. 44 ff. DSGVO für ein angemessenes Datenschutzniveau vorliegen.</p> <p>(4) Eine Übergabe von Daten an den Subunternehmer ist erst zulässig wenn der Subunternehmer sämtliche Anforderungen an eine Unterbeauftragung, insbesondere die Erfordernisse nach Abs. 3 dieser Ziffer erfüllt hat, insbesondere dokumentierte und auf Anfrage zu übermittelnde Nachweise vorliegen, dass der Auftragsverarbeiter dem Subunternehmer sämtliche vertraglichen Regelungen in der Vertragskette auferlegt hat und</p>	<p>(3) The Processor must exercise great care in selecting a subcontractor and must verify that the subcontractor is able to fulfil the obligations agreed upon between Controller and Processor. The Processor will, by way of a written agreement, enjoin the subcontractor to be bound by the same obligations applicable to the Processor and to comply with the instructions issued by the Controller. In particular, the Processor must monitor, prior to and regularly during the contract period, that the subcontractor has implemented the technical and organisational measures required by Art. 32 GDPR to ensure protection of personal data. The results of such monitoring must be recorded by the Processor and must, upon request, be furnished to the Controller. The Processor must obtain from the subcontractor a confirmation that the subcontractor has appointed a data protection officer pursuant to Articles 37 to 39 GDPR and § 38 German Federal Data Protection Act (BDSG), provided that the subcontractor is legally obliged to do so. If the subcontractor fails to comply with his data protection obligations, the Processor is liable to the Controller for compliance with obligations and for violations by the subcontractor. Should the engagement of a subcontractor necessitate the processing of personal data in a third country, the special requirements of Articles 44 et seq. GDPR regarding an appropriate level of data protection must be met.</p> <p>(4) Data may only be transmitted to a subcontractor if and when such subcontractor fulfils any and all requirements of a subcontracting relationship, in particular as stipulated in para. 3 of this number; in particular, there must be documented evidence, to be transmitted upon request, that the Processor has enjoined the subcontractor to be bound by any and all stipulations contained in the chain of contracts and that the subcontractor will fulfil the relevant obligations.</p> <p>(5) The subcontractor's engagement must be recorded in writing. Upon the Controller's</p>
---	---

die entsprechenden Pflichten erfüllt werden.

(5) Die Verpflichtung des Subunternehmens muss schriftlich erfolgen. Dem Verantwortlichen ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

(6) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind und nicht den Zugriff auf personenbezogene Daten, die dem Verantwortlichen zugeordnet sind, erfordern. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

6. Kontrollbefugnisse

(1) Der Verantwortliche hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz nach Art. 28 DSGVO sowie die Einhaltung der unter diesem Vertrag getroffenen Pflichten des Auftragsverarbeiters, der seitens des Verantwortlichen ergangenen Weisungen oder aus jeder Art der Kontaktaufnahme oder Inanspruchnahme seitens staatlicher Stellen resultierende Erfordernisse bei der Datenverarbeitung im Rahmen dieses Auftrags jederzeit im erforderlichen Umfang zu kontrollieren. Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Auskünfte erteilen, Informationen zur Verfügung stellen und den Verantwortlichen oder einen von diesem beauftragten, unabhängigen Prüfer bei der Durchführung von Vor-Ort-Kontrollen dieses Vertrags im erforderlichen Maße unterstützen und an der vollständigen und zügigen Abwicklung der Kontrolle mitwirken.

(2) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe

request, the Processor will furnish the Controller with a copy of such written record.

(6) It shall not be considered to constitute subcontracting pursuant to these provisions if the Processor employs third parties for services that are clearly ancillary services and that do not require access to personal data attributed to the Controller. This comprises, for example, postal services; transport and shipment services; cleaning services; telecommunications services without concrete reference to services that the Processor performs for the Controller; and security services. Maintenance and testing services constitute subcontracting requiring the Controller's consent if and insofar as they are performed for IT systems that are also used in the context of services rendered for the Controller.

6. Monitoring and Inspection

(1) The Controller has the right to verify, at any time and to the extent necessary, whether the Processor complies with data protection provisions pursuant to Art. 28 GDPR, with his contractual obligations as set forth in this contract, with the instructions issued by the Controller or with requirements for data processing under this Order resulting from contact with, or from being charged by, a government authority. The Processor will furnish the Controller with all necessary information and will support the Controller, or an independent auditor tasked by the Controller, in on-site monitoring of this contract to the extent necessary, and will cooperate in the full and expeditious execution of such monitoring.

(2) The Processor is obliged to carry out, prior to commencing the processing activities, the required technical and organisational measures pursuant to Art. 32 GDPR as described in the lead-up to the order procurement, and to document these in particular with regard to the concrete execution of the Order. The Processor is furthermore obliged to hand over such documentation as well as any other documentation that is referred to (for example access authorisation concepts, emergency

<p>dargelegten und erforderlichen technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DSGVO vor Beginn der Verarbeitung vorzunehmen und insbesondere mit Blick auf die konkrete Auftragsdurchführung zu dokumentieren und dem Verantwortlichen nebst allen Verweisdokumenten (bspw. Zugriffsberechtigungskonzepte, Notfallmanagement, Datenschutzfolgenabschätzungen, ISO-Zertifizierungen, Prüfberichte unabhängiger Instanzen) zur Kontrolle zu übergeben. Gleiches muss der Auftragsverarbeiter für die technischen und organisatorischen Maßnahmen seiner Unterauftragnehmer gewährleisten. Der Verantwortliche hat das Recht, sich jederzeit während der Datenverarbeitung unter diesem Auftrag von der Einhaltung der beim Auftragsverarbeiter und seinen Unterauftragsverarbeitern im Sinne des Art. 28 Abs. 3 lit. c) i.V.m. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.</p> <p>(3) Der Verantwortliche kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragsverarbeiters zu den jeweils üblichen Geschäftszeiten vornehmen. Der Verantwortliche wird dabei Sorge dafür tragen, dass die Kontrollen, sofern davon die Betriebsabläufe des Auftragsverarbeiters gestört werden, nur im erforderlichen Umfang durchgeführt werden.</p> <p>(4) Sofern Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung zuvor mit dem Auftragsverarbeiter abzustimmen. Der Auftragsverarbeiter sichert zu, dass auch etwaige andere Mitbewohner der Privatwohnung mit dieser Regelung einverstanden sind.</p> <p>(5) Der Verantwortliche dokumentiert das Ergebnis von Kontrollen nach Absatz 1 und teilt es dem Auftragsverarbeiter hinsichtlich festgestellter Fehler oder Unregelmäßigkeiten mit. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, werden sich Verantwortlicher und Auftragsverarbeiter auf die notwen-</p>	<p>management, data protection impact assessment, ISO certifications, audit report from independent parties) to the Controller for review. The Processor warrants that the same applies to the technical and organisational measures of his subcontractors. The Controller has the right, at any time during the processing under this Order, to verify whether the Processor's and his subcontractors' technical and organisational measures pursuant to Art. 28 para. 3 lit c) in conjunction with Art. 32 GDPR are being observed.</p> <p>(3) The Controller may, upon prior notice and giving an adequate time frame, exercise his right under para. 1 and inspect the Processor's premises during the usual business hours. In doing so, the Controller will take care that if such inspections impact the Processor's operations, they are carried out only to the extent necessary.</p> <p>(4) In the event that data processing is carried out in private accommodation, access to such location must be coordinated with the Processor in advance. The Processor agrees to ensure that other occupants of such private accommodation consent to this stipulation.</p> <p>(5) The Controller will document the result of inspections pursuant to para. 1 and will notify the Processor of any errors or irregularities that may have been determined. Should the inspections show that certain situations should be avoided and this requires changes to the processes as stipulated, the Controller and the Processor will agree upon the necessary changes.</p> <p>(6) In the event a data protection authority or other governmental supervisory authority carry out an inspection in the context of this order, para. 1 shall apply correspondingly.</p>
---	--

<p>digen Änderungen verständigen.</p> <p>(6) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde eine Inspektion der Datenverarbeitung unter diesem Auftrag vornehmen, gilt grundsätzlich Absatz 1 entsprechend.</p> <p>7. Vergütung</p> <p>Tätigkeit des Auftragsverarbeiters im Rahmen des Auftrags wird nicht gesondert vergütet, soweit dies nicht ausdrücklich vereinbart ist.</p> <p>8. Löschung und Rückgabe personenbezogener Daten</p> <p>(1) Kopien oder Duplikate der Daten werden ohne Wissen und ausdrückliche Zustimmung des Verantwortlichen nicht gefertigt. Dies gilt nicht für Sicherheitskopien und solche Aufzeichnungen, die zur Gewährleistung einer den technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO entsprechenden Datenverarbeitung oder zur Einhaltung gesetzlicher Aufbewahrungs- und Nachweispflichten erforderlich sind.</p> <p>(2) Nach Beendigung des Auftrages oder früher nach Anforderung durch den Verantwortlichen hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, Datenträger, Datenbestände und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftrag stehen, inklusive etwaiger Datensicherungen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Die Datenträger des Auftragsverarbeiters sind nach Aushändigung physisch zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung ist in geeigneter Weise zu dokumentieren. Sofern für die genannten Unterlagen, Datenbestände oder Datenträger gesetzliche Aufbewahrungsfristen gelten, sind diese unverzüglich nach Ablauf der betreffenden Fristen zu löschen und zu vernichten. Sowohl die gesetzlichen Aufbewahrungsfristen als auch die Löschung der betreffenden Daten nach deren Ablauf sind zu dokumentieren.</p>	<p>7. Remuneration</p> <p>The Processor will not receive separate remuneration for work performed in the context of this Order, unless such is specifically agreed upon.</p> <p>8. Erasing and Returning Personal Data</p> <p>(1) It is not permitted to make copies or duplicates of data without the Controller's knowledge and his express consent to do so. The foregoing does not apply to safety copies and recordings made to ensure that the processing is carried out in accordance with the technical and organisational measures pursuant to Art. 32 GDPR, or to ensure compliance with statutory obligations to keep records and accounts.</p> <p>(2) After completion of the Order, or earlier upon request by the Controller, the Processor must return to the Controller any and all documentation, data storage mediums, data sets and any results of the processing or use that are connected to the Order, including possible backup, that came into his possession; or to destroy them in accordance with data protection principles, provided the Controller has consented to such destruction. The Processor's data storage mediums must be physically destroyed after having been handed over. The same applies to material used for testing and to waste material. The erasure must be documented in a suitable manner. In the event that there are statutory retention periods for the abovementioned documents, data sets and storage mediums, these must be erased and destroyed immediately after such retention periods have lapsed. Both the statutory retention periods and the erasure of the data in question after lapse of the retention period must be documented.</p> <p>(3) The Controller has the right to verify that the Processor has returned and erased any and all data pursuant to his obligations under this contract. Verification may include</p>
--	---

<p>(3) Der Verantwortliche hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragsverarbeiter zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragsverarbeiters erfolgen. Eine solche Vor-Ort-Kontrolle soll mit angemessener Frist durch den Verantwortlichen angekündigt werden.</p> <p>9. Haftung</p> <p>Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. <i>Für die vertragliche Haftung zwischen Auftraggeber und Auftragnehmer finden die Haftungsregelungen aus dem Hauptvertrag Anwendung.</i></p> <p>10. Schlussbestimmungen</p> <p>(1) Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren. Der Auftragsverarbeiter wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.</p> <p>(2) Die Einrede von Zurückbehaltungsrechten, insb. der §§ 273, 320 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.</p> <p>(3) Unbeschadet der Abreden zur Erteilung von Weisungen unter diesem Vertrag bedürfen Änderungen und Ergänzungen dieses Vertrags und aller ihrer Bestandteile einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrags handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.</p> <p>(4) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit</p>	<p>inspection of the data processing facilities on the Processor's premises, such on-site inspection to be announced by the Controller with a reasonable deadline.</p> <p>9. Liability</p> <p><i>The liability of the Processor and of the Controller towards persons affected by the processing is as stipulated in Art. 82 GDPR. The contractual liability between Controller and Processor is ruled by the liability stipulations of the Master Contract.</i></p> <p>10. Final Provisions</p> <p>(1) Should the Controller's property in the Processor's possession be threatened by measures undertaken by third parties (such as attachment or seizure), insolvency proceedings or other events, the Processor must notify the Controller thereof without delay. The Processor will inform the creditors without delay that this is data which is being processed on behalf of the Controller.</p> <p>(2) The plea of a right of retention, in particular pursuant to §§ 273, 320 German Civil Code (BGB), in relation to data processed hereunder and data storage mediums used for such processing is herewith excluded.</p> <p>(3) No change or addition to this contract or any of its parts shall take effect unless made in writing; this can also be in an electronic format (text form) and must state explicitly that it constitutes a change or addition to the contract. This requirement for changes to be in writing can itself only be waived if such waiver is agreed in writing.</p> <p>(4) Should individual provisions of this contract be void or unenforceable, in parts or as a whole, the remaining provisions shall remain in full force and effect.</p> <p>(5) This contract is governed by German law. The courts of Hamburg shall have exclusive jurisdiction.</p>
--	---

<p>der jeweils übrigen Bestimmungen nicht be- rührt. (5) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Hamburg.</p>	
---	--

Datum, Unterschrift Auftragsverarbeiter
Date, signature on behalf of the Processor

Datum, Unterschrift Verantwortlicher
Date, signature on behalf of the Controller

Hinweis/Note:

Die Parteien sind sich einig, dass die englische Sprachversion dieses Vertrages ausschließlich zu Verständniszwecken erstellt wurde und dass nur die deutschsprachige Version Rechtsgültigkeit hat.

This document was prepared in the German language. Where a translation is provided, into English or any other language, this is for informational purposes only. In the event of any disagreement, ambiguity or lack of clarity, and for all legal purposes, the German original alone shall apply.

Anlage 1 - Gegenstand des Auftrags

<p>Gegenstand des Auftrags</p> <ul style="list-style-type: none"> • <i>Verantwortlicher</i> <p>Was macht der Verantwortliche (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung / den Zugriff auf die personenbezogenen Daten relevant sind):</p> <ul style="list-style-type: none"> • <i>Auftragsverarbeiter</i> <p>Was macht der Auftragsverarbeiter? (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung / den Zugriff auf die personenbezogenen Daten relevant sind):</p>	<p>Kurze Beschreibung der Tätigkeit des Verantwortlichen</p>
<p>Art und Zweck der Verarbeitung</p> <ul style="list-style-type: none"> • <i>Zweck der Verarbeitung</i> <p>Die übermittelten bzw. zugegriffenen personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen (bitte genau angeben):</p>	<p>Kurze Beschreibung der Tätigkeit des Auftragsverarbeiters</p>
<ul style="list-style-type: none"> • <i>Art der Verarbeitung</i> <p>Folgende Formen/Arten der Datenverarbeitung personenbezogener Daten sind Gegenstand dieses Auftrags (Art. 4 Nr. 2 DSGVO):</p>	<p>Detaillierte Angabe aller Mittel und Zwecke der Verarbeitung</p> <p><input type="checkbox"/> bereits erwähnt oben in dem „Zweck der Verarbeitung“</p> <p><input type="checkbox"/> Erheben,</p> <p><input type="checkbox"/> Erfassen,</p> <p><input type="checkbox"/> die Organisation,</p> <p><input type="checkbox"/> das Ordnen</p> <p><input type="checkbox"/> die Speicherung,</p> <p><input type="checkbox"/> die Anpassung oder Veränderung</p> <p><input type="checkbox"/> das Auslesen,</p> <p><input type="checkbox"/> das Abfragen,</p> <p><input type="checkbox"/> die Verwendung,</p> <p><input type="checkbox"/> die Offenlegung durch Übermittlung,</p> <p><input type="checkbox"/> die Verbreitung oder eine andere Form der Bereitstellung,</p> <p><input type="checkbox"/> der Abgleich oder die Verknüpfung</p> <p><input type="checkbox"/> die Einschränkung,</p> <p><input type="checkbox"/> das Löschen oder die Vernichtung,</p> <p><input type="checkbox"/> andere Art der Verarbeitung: _____</p>
<p>Datenarten</p> <ul style="list-style-type: none"> • <i>Kategorien von Daten</i> <p>Die übermittelten bzw. zugegriffenen personenbezogenen Daten betreffen die folgenden Datenkategorien (bitte genau angeben):</p>	<p><input type="checkbox"/> Daten zur Person (Titel, Name, Vorname, Geburtsdatum, Geschlecht, ...)</p> <p><input type="checkbox"/> Adress-Daten (Ort, Straße, PLZ)</p> <p><input type="checkbox"/> Kontaktdaten (E-Mail-Adr., Telefon-Nr., ...)</p> <p><input type="checkbox"/> Zahlungs-/Bank-Daten (Konto-Nr., Kreditkarten-Nr., ...)</p> <p><input type="checkbox"/> Profildaten (Arbeitsleistung, wirtschaftliche Lage, Vorlieben, Interessen, Verhalten, Aufenthaltsort, Auskunftsdaten v. Dritten)</p> <p><input type="checkbox"/> technische Daten (IP-Adresse, Benutzer-Kennung, Passwort, Cookie-ID, Mobil-ID, ...)</p>

	<input type="checkbox"/> _____
<ul style="list-style-type: none"> • <i>besondere Kategorien personenbezogener Daten (falls zutreffend)</i> <p>Die übermittelten bzw. zugegriffenen personenbezogenen Daten betreffen die folgenden speziellen Datenkategorien (bitte genau angeben):</p>	<input type="checkbox"/> bereits erwähnt oben <small>in den „Kategorien von Daten“</small> <input type="checkbox"/> Gesundheit <input type="checkbox"/> genetische Daten <input type="checkbox"/> biometrische Daten <input type="checkbox"/> Daten aus denen die rassistische und ethnische Herkunft hervorgehen <input type="checkbox"/> Daten zum Sexualleben oder sexuellen Orientierung <input type="checkbox"/> politische Meinungen <input type="checkbox"/> religiöse oder weltanschauliche Überzeugungen <input type="checkbox"/> Gewerkschaftszugehörigkeit
<p>Kategorien betroffener Personen</p> <ul style="list-style-type: none"> • <i>Betroffene Personen</i> <p>Die übermittelten bzw. zugegriffenen personenbezogenen Daten betreffen folgende Kategorien von Betroffenen (bitte genau angeben):</p>	<input type="checkbox"/> Beschäftigte (inkl. Bewerber, ehemalige Beschäftigte, Zeitarbeitskräfte) <input type="checkbox"/> Kunden (inkl. Interessenten, ehemalige Kunden) <input type="checkbox"/> Lieferanten <input type="checkbox"/> Auftraggeber <input type="checkbox"/> Nutzer (Webseiten, Mobile-Apps, ...) <input type="checkbox"/> [...] _____

Appendix 1 – Object of the Processing

<p>Object of the Processing</p> <ul style="list-style-type: none"> • <i>Controller</i> <p>What activities does the Controller engage in (please give a short description of the activities that are relevant for the transmission of / access to personal data):</p>	<p>Short description of the Controller's activities</p>
<ul style="list-style-type: none"> • <i>Processor</i> <p>What activities does the Processor engage in (please give a short explanation of the activities that are relevant for the transmission of / access to personal data):</p>	<p>Short description of the Processor's activities</p>

Type and purpose of the processing	Detailed description of all means and purposes of the processing
<ul style="list-style-type: none"> <i>Purpose of processing</i> <p>The personal data transmitted or accessed, respectively, will be processed as follows (please give detailed descriptions):</p>	
<ul style="list-style-type: none"> <i>Type of processing</i> <p>The following forms/types of processing of personal data form the subject matter of this order (Art. 4 No. 2 GDPR):</p>	<input type="checkbox"/> Already mentioned above under 'purpose of processing' <input type="checkbox"/> Collecting, <input type="checkbox"/> Recording, <input type="checkbox"/> Organising, <input type="checkbox"/> Structuring, <input type="checkbox"/> Storing, <input type="checkbox"/> Adaptation or alteration, <input type="checkbox"/> Retrieval, <input type="checkbox"/> Consultation, <input type="checkbox"/> Use, <input type="checkbox"/> Disclosure by transmission, <input type="checkbox"/> Dissemination or otherwise making available, <input type="checkbox"/> Alignment or combination, <input type="checkbox"/> Restriction, <input type="checkbox"/> Erasure or destruction, <input type="checkbox"/> Other form of processing: _____
Types of data <ul style="list-style-type: none"> <i>Data categories</i> <p>The personal data transmitted or accessed concern the following data categories (please specify precisely):</p>	<input type="checkbox"/> Personal data (Salutation, surname, first name, date of birth, gender, ...) <input type="checkbox"/> Address (city, street, post code) <input type="checkbox"/> Contact details (email address, telephone number, ...) <input type="checkbox"/> Payment / bank data (account number, credit card number, ...) <input type="checkbox"/> Profile (performance at work, economic situation, personal preferences interests, behaviour, location, third-party information data) <input type="checkbox"/> Technical data (IP address, user identifier, password, cookie ID, mobile ID, ...) <input type="checkbox"/> _____ <input type="checkbox"/> _____
<ul style="list-style-type: none"> <i>Special categories of personal data (if applicable)</i> <p>The transmitted or accessed personal data concern the following special data categories (please specify precisely):</p>	<input type="checkbox"/> Already mentioned above in the 'data categories' <input type="checkbox"/> Health-related data <input type="checkbox"/> Genetic data <input type="checkbox"/> Biometric data <input type="checkbox"/> Racial or ethnic background <input type="checkbox"/> Sex life and sexual orientation <input type="checkbox"/> Political opinions <input type="checkbox"/> Religious or ideological beliefs <input type="checkbox"/> Membership in trade unions
Categories of persons concerned <ul style="list-style-type: none"> <i>Persons concerned</i> <p>The personal data transmitted</p>	<input type="checkbox"/> Employees (incl. candidates, former employees, temping staff) <input type="checkbox"/> Clients (incl. prospective clients, former clients) <input type="checkbox"/> Suppliers <input type="checkbox"/> Principals <input type="checkbox"/> Users (websites, mobile apps, ...) <input type="checkbox"/> Passengers/visitors

or accessed concern the following categories of persons (please specify precisely):

- _____
- _____

Anlage 2: Technische und organisatorische Maßnahme i.S.d. Art. 32 DSGVO

Dieses Kapitel ist an den Inhalt des Hauptvertrages anzupassen. Die genannten Maßnahmen sind nur Beispiele für mögliche Maßnahmen, die der Auftragsverarbeiter vor- sehen kann. Hier sind die konkret vereinbarten technischen und organisatorischen Maßnahmen aufzuführen.

Der Auftragsverarbeiter wird nachfolgende technische und organisatorische Maßnahmen zur Umsetzung der Anforderungen aus Art. 32 DSGVO bei der Datenverarbeitung berücksichtigen.

a) Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Server sind in verschlossenen, durch Zutrittskontrollsysteme gesicherte Räume zu betreiben
- Protokollierung der Zutritte zu Serverräumen
- Werkschutz, Pförtner
- Videoüberwachung

b) Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Verwendung von Passwörtern
- Einsatz passwortgeschützter Bildschirmschoner
- Verschlüsselung von Datenträgern

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können.:

Appendix 2: Technical and Organisational Measures Pursuant to Art. 32 GDPR

This chapter is to be adapted to the content of the Master Contract. The measures listed serve only as example for possible measures to be undertaken by the Processor. The technical and organisational measures that have been specifically agreed upon are to be listed here.

When processing data, the Processor will take into account the following technical and organisational measures in order to comply with the requirements set forth in Art. 32 GDPR.

a) Physical Access

Measures to bar unauthorised persons from physically entering data processing facilities employed to process or use personal data:

- Servers must be operated in locked rooms that are secured by an entry control system.
- Entries to server rooms must be recorded.
- Factory security service, doorman.
- Video surveillance.

b) Technical Access

Measures to prevent the use of data processing facilities by unauthorised persons:

- Use of passwords.
- Use of screensavers protected by passwords.
- Encryption of data storage mediums.

c) Organisational Access

Measures to ensure that persons authorised to use a data processing system can access only the data for which they have right of access, and that personal data cannot be read, copied, altered or removed during their processing or use, or after storage, without authorisation:

- Creation and use of an authorised user

- Erstellung und Nutzung eines Berechtigungskonzept – bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen
- sämtliche Datenträger sind unter Verschluss zu halten
- Datenträger sind gemäß DIN-Norm (DIN 32757-1 bzw. 33858) zu vernichten
- Verschlüsselung und Pseudonymisierung personenbezogener Daten

d) Trennungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurde, getrennt voneinander verarbeitet werden. Die Trennungskontrolle ist wie folgt realisiert:

- es gibt Produktivinstanzen und Testinstanzen
- die Daten sind kundenbezogen (teilnehmerbezogen) separiert
- die Datensicherung erfolgt auf separaten Datenträgern
- die Erfassung, Veränderung, Löschung und Übermittlung erfolgt durch jeweils eigenständige Funktionen.

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

„Pseudonymisierung“ meint die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

f) Übertragungs-/Weitergabekontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. Maßnahmen, die gewährleisten, dass personenbezogene Daten bei

concept – access rights tailored to need.

- Records of actual access.
- Any and all data storage mediums must be kept under lock.
- Data storage mediums must be destroyed in accordance with the relevant DIN standard (DIN 32757-1 and 33858, respectively).
- Encryption and pseudonymisation of personal data.

d) Separation

Measures to ensure that personal data that has been collected for diverse purposes is processed separately. Such separation control is implemented as follow:

- There are production instances and test instances.
- The data is separated in relation to the client (to the participant).
- Safeguarding of data is effected on separate data storage mediums.
- There are separate, independent functions for collecting, altering, erasing and transferring.

e) Pseudonymisation (Art. 32 para. 1 lit. a GDPR)

‘Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

f) Transmission / Disclosure

Measures to ensure that it is possible to check and establish which instances or authorities are authorised to receive, or have received, personal data by means of data transfer facilities. Measures to ensure that during the electronic transfer of personal

der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- sämtliche Daten sind bei Datenübermittlungen über das Internet zu verschlüsseln
- Transporte von Datenträgern sind in verschlossenen Behältern durchzuführen und werden protokolliert

g) Speicher-/Eingabekontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten. Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Protokollierung sämtliche Aktivitäten mit Angabe des betroffenen Datensatzes, Art der Aktivität, Zeitpunkt und Name der ausführenden Person
- Dokumentation der Administratoraktivitäten (Anlegen, Ändern, Löschen von Benutzern)

h) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können:

- Abschluss von Vereinbarungen analog dieser Vereinbarung

i) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- Einsatz von aktuellen Virens Scanner, Firewalls und Spamfiltern
- Regelmäßige Datensicherung
- Erstellung eines Notfallplanes incl.

data, or their transport, or such time as they are stored on data storage mediums, such data cannot be read, copied, altered or removed without authorisation; and that it is possible to check and establish which instances or authorities are designated to receive personal data by means of data transfer facilities:

- Any and all data must be encrypted when transmitted via the Internet.
- Data storage mediums must be transported in locked containers and such transport must be recorded.

g) Storage/Entry

Prevention of unauthorised entering of personal data and of unauthorised gaining of knowledge, unauthorised alteration and erasure of stored personal data. Measures to ensure that it is possible, post factum, to check who is authorised, if applicable, to enter personal data into data processing systems, to alert or erase it:

- Records of any and all activities including information about the data set concerned, the type of activity, time, and name of the person carrying out such activity.
- Documentation of administrator activities (creating, changing, deleting of users).

h) Compliance with Instructions

Measures to ensure that personal data being processed by the Processor on behalf of the Controller can only be processed in accordance with the Controller's instructions:

- Conclusion of agreements analogous to this order.

i) Availability

Measures to ensure that personal data is protected against destruction or loss:

- Using up-to-date virus scanners, firewalls and spam filters.
- Regular backup.
- Creating an emergency response plan in-

<p>Recovery-Konzeptes</p> <ul style="list-style-type: none"> - regelmäßige Tests der vorhandenen Konzepte - katastrophensichere Aufbewahrung von Datenträgern <p>i) Wiederherstellbarkeit</p> <p>Maßnahmen, die gewährleisten, dass alle Funktionen des Systems und die Verfügbarkeit und der Zugang zu personenbezogenen Daten im Störfall rasch wiederhergestellt werden können.</p> <ul style="list-style-type: none"> - Standardisiertes Notfallmanagement inkl. Notfallpläne und Leitfäden, so dass eine unverzügliche Wiederherstellbarkeit gewährleistet ist. - Regelmäßige Tests der Wiederherstellbarkeit. <p>k) Zuverlässigkeit</p> <p>Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.</p> <ul style="list-style-type: none"> - Elektronisches Fehlermeldungssystem - Reaktions- und Fehlerbehebungszeiten im Störfall - Regelmäßige Testläufe zur Ansprache aller im System enthaltenen Funktionen <p>l) Datenintegrität</p> <p>Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.</p> <ul style="list-style-type: none"> - Rekonstruierbarkeit der Daten aus einem Datenstrom an allen erforderlichen Stellen einer Datenübertragung - Richtungsindikator - Analyse von Sequenznummern <p>m) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)</p> <ul style="list-style-type: none"> - Datenschutzmanagement mit Leitlinien zu Datenschutz und Datensicherheit und 	<p>cluding a recovery concept.</p> <ul style="list-style-type: none"> - Regular testing of existing concepts. - Storage of data storage mediums in a disaster-proof location. <p>j) Restorability</p> <p>Measures to ensure that, in the event of disruption or malfunctions, all systems functions and availability of and access to personal data can be restored swiftly.</p> <ul style="list-style-type: none"> - Standardised crisis management including emergency response plans and guidelines to ensure that data can be restored without delay. - Regular testing of the capacity to restore. <p>k) Reliability</p> <p>Measures to ensure that all systems functions are available and that malfunctions are reported.</p> <ul style="list-style-type: none"> - Electronic system to report malfunctions. - In the event of a failure or malfunction, the time needed to react and resolve the issue. - Regular testing to address all functions within the system. <p>l) Data Integrity</p> <p>Measures to ensure that stored personal data cannot be damaged if a system fails or malfunctions.</p> <ul style="list-style-type: none"> - It must be possible to reconstruct all data pertaining to a particular data flow in all required locations of data transmission. - Directional flag. - Analysis of sequence numbers <p>m) Process for regular testing, assessing and evaluating the effectiveness of the measures undertaken (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)</p> <ul style="list-style-type: none"> - Data protection management including
---	--

<p>Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.</p> <ul style="list-style-type: none"> - Regelmäßige Überprüfung und Anpassung der Richtlinien im Hinblick auf Wirksamkeit und flächendeckender Durchsetzung. - Datenschutz- und Informationssicherheits-Team, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt. - Sensibilisierung und Schulung aller Mitarbeiter hinsichtlich Datenschutzvorfälle und Etablierung von Meldekettten. - Regelmäßige interne Auditierung der TOMs - Regelmäßige externe Auditierung der TOMs - Auffrischung von Zertifizierungen in regelmäßigen Abständen - Regelmäßige Penetrationstests der IT-Systeme - Überprüfung des Datenschutzniveaus bei Abänderung von Datenverarbeitungsprozessen und technischen Neuerungen - Regelmäßige Bewertung des Risikos für Systemangriffe und Anpassung des Kontrollturnus für Abwehrmaßnahmen - Regelmäßige Risikoanalyse in Bezug auf materielle und immaterielle Schäden die im Rahmen der Verarbeitungstätigkeit bzw. bei den zugrundeliegenden Systemen auf-treten können. - Fortschreibung eines Maßnahmenplans auf Basis der identifizierten und bewerteten Risiken. - Entsprechende Auditierung und Nachweise von Subdienstleistern. 	<p><i>guiding principles concerning data protection and data security as well as guidelines to ensure implementation of the guiding principles.</i></p> <ul style="list-style-type: none"> - <i>Regular review and adaptation of the guidelines regarding their effectiveness and comprehensive implementation.</i> - <i>Data protection and information safety team to plan, implement, evaluate and adapt measures of data protection and data security.</i> - <i>Make employees aware of data protection issues and train them accordingly; establish reporting chains</i> - <i>Regular internal auditing of the TOMs</i> - <i>Regular external auditing of the TOMs</i> - <i>Regular renewal of certifications</i> - <i>Regular penetration testing of the IT systems</i> - <i>Review the data protection level in the event of changes to data processing procedures and technical innovations.</i> - <i>Regular assessment of the risk of system attacks and adaptation of the control cycle for defence measures.</i> - <i>Regular risk analysis regarding material and immaterial damage that may occur in the course of the processing or in the underlying systems.</i> - <i>Updating an action plan on the basis of identified and evaluated risks.</i> - <i>Analogous auditing and proof of subcontractors.</i>
--	---

Anlage 3: Subunternehmer

Der Auftragsverarbeiter nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Name des Unternehmens incl. Rechtsform	Ansprechpartner (Kontakt Daten)	Anschrift	Art der Leistung

Appendix 3: Subcontractors

The Processor employs third-party providers who will process data on his behalf as part of the data processing order by the Controller ('subcontractors')

Such third-party providers are as listed below:

Name and legal form of the company	Interlocutor (contact details)	Address	Service provided

Anlage 4: Datenschutzbeauftragter/(EU/EWR-)Vertreter

Auf Grundlage des Art. 37 DSGVO wurde durch den Auftragsverarbeiter ein Datenschutzbeauftragter benannt:

Vor- und Zuname: _____

Anschrift des Datenschutzbeauftragten: _____

Telefonnummer: _____

E-Mail: _____

Auf Grundlage des Art. 27 DSGVO wurde durch den Auftragsverarbeiter ein Vertreter innerhalb EU/EWR benannt:

Vor- und Zuname: _____

Anschrift des Datenschutzbeauftragten: _____

Telefonnummer: _____

E-Mail: _____

Appendix 4: Data Protection Office/(EU / EEA) Representative

On the basis of Article 37 GDPR, a data protection officer has been appointed by the processor:

Name: _____

Address: _____

Phone number: _____

E-Mail: _____

On the basis of Article 27 GDPR, a representative within the EU / EEA has been appointed by the processor:

Name: _____

Address: _____

Phone number: _____

E-Mail: _____