Anlage 1 zum

Vertrag über _____

(im Folgenden „**Hauptvertrag**“)

Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 Abs. 3 Europäische Datenschutz-Grundverordnung

(im Folgenden „**DSGVO**“)

zwischen

der Universität Siegen, Adolf-Reichwein-Str. 2a, 57076 Siegen, vertreten durch den Kanzler

Ulf Richter „**Auftraggeber**“ genannt,

und

_____,

vertreten durch_____,

„**Auftragnehmer**“ genannt,

jeder für sich eine „**Partei**“, zusammen die „**Parteien**“

1. Gegenstand und Dauer des Auftrags; Ort der Datenverarbeitung

1.1 Der Gegenstand dieser Vereinbarung über die Auftragsverarbeitungsvereinbarung von personenbezogenen Daten („**Auftragsverarbeitungsvereinbarung“**) ergibt sich aus dem Hauptvertrag und seinen Anlagen.

1.2 Die Kategorien von Daten, die Gegenstand der Datenverarbeitung nach Maßgabe dieser Auftragsverarbeitungsvereinbarung sind, werden mitsamt Art und Zweck der Verarbeitung durch den Auftragnehmer für den Auftraggeber in **Anhang 1** zu dieser Auftragsverarbeitungsvereinbarung aufgeführt.

1.3 Die Dauer dieser Auftragsverarbeitungsvereinbarung entspricht der des Hauptvertrages. Diese Auftragsverarbeitungsvereinbarung endet nicht vor der Erfüllung des letzten aus dem Hauptvertrag beauftragten Einzelauftrags.

1.4 Soweit dieser Vertrag von dem Hauptvertrag abweichende Regelungen trifft, gehen die Regelungen der Auftragsverarbeitungsvereinbarung vor.

1.5 Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Artikel 4 Nr. 7 DSGVO), sofern der Auftragnehmer die Pflichten aus dieser Auftragsverarbeitungsvereinbarung vollumfänglich beachtet.

1.6 Der Auftragnehmer verarbeitet personenbezogene Daten unter dieser Auftragsverarbeitungsvereinbarung ausschließlich innerhalb der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR).

1.7 Der Auftraggeber stimmt einer Verlagerung des Ortes der Leistungserbringung innerhalb des Leistungslandes gem. Ziff 1.6 zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

1.8 Über eine Verlagerung des Ortes der Leistungsverarbeitung innerhalb der EU oder des EWR wird der Auftraggeber vor Verlagerung schriftlich informiert.

1.9 Eine Verarbeitung außerhalb des Hoheitsgebiets der EU und des EWR bedarf der Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen zu einem angemessenen Schutzniveau gem. Art. 44 ff DSGVO erfüllt sind. Die Einhaltung der diesbezüglichen Vorschriften der DSGVO wird durch den Auftragnehmer durch Vorlage aller hierzu erforderlichen Dokumente und Unterlagen nachgewiesen und die Einhaltung der Vorgaben von dem Auftragnehmer gewährleistet. Ohne Zustimmung ist die Verarbeitung personenbezogener Daten außerhalt dieses Raumes ausdrücklich untersagt.

1.10 Klarstellend wird vereinbart, dass auch mit Wirksamwerden des Austritts eines Landes aus der Europäischen Union oder des Europäischen Wirtschaftsraums eine Verarbeitung personenbezogener Daten durch den Auftragnehmer in diesem Land der ausdrücklichen Zustimmung des Auftraggebers bedarf. Der Auftraggeber ist keinesfalls verpflichtet, seine Zustimmung hierzu zu erteilen.

2. Fernwartung

2.1 Die Regelungen dieser Ziff. finden bei dem räumlich getrennten Zugriff des Auftragnehmers auf IT-Systeme des Auftraggebers zu Wartungs- oder Reparaturzwecken (Fernwartung) Anwendung.

2.2 Der Auftragnehmer darf im Rahmen der Fernwartung nur auf personenbezogene Daten des Auftraggebers zugreifen, wenn dies für die Durchführung der Fernwartung erforderlich ist. Ferner ist dem Auftragnehmer bei der Fernwartung untersagt, personenbezogene Daten des Auftraggebers auf eigenen IT-Systemen bzw. Datenträgern zu speichern, es sei denn der Auftraggeber weist ihn hierzu an.

2.3 Der Auftragnehmer hat dem Auftraggeber Fernwartungsarbeiten im Vorfeld anzukündigen. Der Auftraggeber ist berechtigt, die Durchführung der Fernwartung mit zu verfolgen bzw. Aufzeichnungen (z.B. Screenrecording, Screenshots o.Ä.) von dieser zu erstellen. Auf Anfrage und soweit erforderlich, wirkt der Auftragnehmer an der Konfiguration technischer Kontrolleinrichtungen mit.

2.4 Im Rahmen der beauftragten und zu leistenden Fernwartungsarbeiten hat der Auftragnehmer folgende Rahmenbedingungen bei Zugriff auf das Netzwerk, die IT-Systeme und Anwendungen des Auftraggebers zu beachten:

- Der Auftragnehmer erhält für Arbeiten an den IT-Systemen und Anwendungen personalisierte Benutzerkennungen. Jeder Mitarbeiter des Auftragnehmers erhält eine eigene personalisierte Benutzerkennung. Der Auftragnehmer nutzt die ihm überlassenen personalisierten Benutzerkennungen ausschließlich für die beauftragten Tätigkeiten und gibt diese nicht an Dritte weiter. Die Kennwortrichtlinien des Auftraggebers sind einzuhalten.
- Nutzt der Auftragnehmer für die Ausübung seiner Tätigkeiten eigene technische Geräte stellt er durch adäquate und dem Stand der Technik entsprechende, angemessene Maßnahmen sicher, dass von diesen keine Gefahren für die Netzinfrastruktur, IT-Systeme und Anwendungen des Auftraggebers ausgehen.
- Änderungen an den IT-Systemen und Anwendungen seitens des Auftragnehmers sind mit dem Auftraggeber abzustimmen und in einem adäquaten, prüffähigen Umfang zu dokumentieren.

2.5 Insbesondere beim Fernzugriff auf das Netzwerk und die IT-Systeme des Auftraggebers gelten die zusätzlichen Bedingungen:

- Das Netz und die für die Fernwartung genutzten IT-Systeme des Auftragnehmers müssen adäquat gegen unberechtigte Zugriffe geschützt sein.
- Der Fernzugriff auf das Netzwerk des Auftraggebers erfolgt ausschließlich über eine nach dem Stand der Technik angemessen sichere, verschlüsselte Verbindung.
- Der Fernzugriff sollte generell nur innerhalb der üblichen Arbeitszeiten des Auftraggebers durchgeführt werden. Ein Fernzugriff außerhalb dieser Zeiten ist mit dem Auftraggeber abzustimmen und zu dokumentieren.
- Der Zugriff ist nach erfolgter Tätigkeit zu beenden und die Verbindung zu schließen.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer hat die Auftragsverarbeitung so durchzuführen, dass sie im Einklang mit den Anforderungen der DSGVO steht und den Schutz der Rechte der betroffenen Personen gewährleistet.

3.2 Der Auftragnehmer verarbeitet personenbezogene Daten nur im Rahmen des Auftrags und der Weisungen des Auftraggebers, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 lit. a DSGVO vor. Auskünfte an Dritte oder Betroffene dürfen ohne eine entsprechende Weisung des Auftraggebers nicht erteilt werden. Der Auftragnehmer darf die Daten für keine anderen Zwecke außerhalb dieser Auftragsverarbeitungsvereinbarung und des Hauptvertrags verwenden und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien/Duplikate dürfen ohne Wissen des Auftraggebers nicht erstellt werden.

3.3 Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die von Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

3.4 Sofern erforderlich, unterstützt der Auftragnehmer den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung seiner Pflichten im Rahmen von Datenschutz-Folgeneinschätzungen im Sinne von Artikel 35 DSGVO und bei der vorherigen Konsultation der Aufsichtsbehörden gem. Artikel 36 DSGVO.

Auf Wunsch wirkt der Auftragnehmer an der Erstellung und Aktualisierung des Verfahrensverzeichnisses des Auftraggebers hinsichtlich der Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen mit. Der Auftraggeber hat ein Einsichtsrecht in die erforderliche Dokumentation des Auftragnehmers. Erforderliche Dokumente sind dem Auftraggeber auf Anfrage offenzulegen.

3.5 Der Auftragnehmer benennt die, für die vorliegende Auftragsverarbeitungsvereinbarung zuständigen Ansprechpartner in **Anhang 2.**

3.6 Mündliche Weisungen des Auftraggebers bestätigt der Auftragnehmer unverzüglich in Textform (z.B. E-Mail, Fax, o.ä.).

3.7 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, eine Weisung verstoße gegen anwendbares Recht. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder abgeändert wird.

3.8 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber heraus. Löschung und/oder Vernichtung sind in geeigneter Weise zu dokumentieren und auf Anfrage des Auftraggebers mitzuteilen.

3.9 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.10 Personenbezogene Daten dürfen nur denjenigen Mitarbeitern zugänglich gemacht werden, die von diesen personenbezogenen Daten für die Durchführung der Auftragsverarbeitungsvereinbarung und des Hauptvertrags Kenntnis haben müssen und nur diese Mitarbeiter haben Zugang zu den personenbezogenen Daten. Personenbezogene Daten dürfen nicht an Dritte weitergegeben werden, sofern nicht ausdrücklich im Hauptvertrag und in dieser Auftragsverarbeitungsvereinbarung gestattet oder dies durch geltendes Recht vorgeschrieben ist; in diesem Fall wird der Auftragnehmer den Auftraggeber über die erzwungene Offenlegung vorher informieren.

3.11 Kommt es bei dem Auftragnehmer zu einer schwerwiegenden Störung des Betriebsablaufs, tritt eine Verletzung des Schutzes personenbezogener Daten ein oder liegt ein begründeter Verdacht vor, dass eine solche Verletzung einzutreten droht, unterrichtet der Auftragnehmer den Auftraggeber unverzüglich. In Abstimmung mit dem Auftraggeber trifft der Auftragnehmer die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen. Im Falle einer eingetretenen Verletzung unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Meldepflicht gem. Artikel 33 und 34 durch Mitteilung mindestens der folgenden Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

3.12 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.

4. Rechte und Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2 Liegt ein schwerwiegender Verstoß gegen die Bestimmungen der DSGVO oder dieser Vereinbarung vor, kann oder will der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen oder verweigert der Auftragsnehmer den Zutritt des Auftraggebers oder dessen Datenschutzbeauftragten vertragswidrig, kann der Auftraggeber die Auftragsverarbeitungsvereinbarung fristlos kündigen.

4.3 Der Auftraggeber benennt nach Zuschlagserteilung die für die vorliegende Auftragsverarbeitungsvereinbarung zuständigen Ansprechpartner.

5. Anfragen betroffener Personen

5.1 Soweit sich eine betroffene Person unmittelbar an den Auftragnehmer mit Anfragen oder Forderungen zur Übertragung, Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und die betroffene Person darüber informieren, dass der Auftraggeber die verantwortliche Stelle im Sinne der DSGVO ist.

5.2 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33-34 DSGVO genannten Pflichten.

5.3 Ist der Auftragnehmer seinen Unterstützungspflichten nachgekommen, haftet er nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Technische und organisatorische Schutzmaßnahmen

6.1 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der DSGVO genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Artikel 32 Abs. 1 DSGVO zu berücksichtigen.

6.2 Der Auftragnehmer stellt dem Auftraggeber bereits im Rahmen des Vergabeverfahrens zusammen mit seinem Angebot aussagekräftige und prüffähige technisch-organisatorische Maßnahmen (Datenschutz- und Datensicherheitskonzept) für diese Auftragsdatenverarbeitung zur Verfügung **(Anhang 3)**. Erfolgt die Vergabe im offenen oder nicht offenen Verfahren wird die von dem Auftragnehmer vorgelegte Dokumentation Bestandteil der vorliegenden Vereinbarung über Auftragsverarbeitung. Erfolgt die Vergabe im Verhandlungsverfahren hat der Auftragnehmer die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu

dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage dieser Auftragsverarbeitungsvereinbarung. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

6.3 Beispiele für die vom Auftragnehmer zu treffenden technisch-organisatorischen Maßnahmen sind in **Anhang 3** aufgeführt.

6.4 Der Auftragnehmer gewährleistet, um seinen Pflichten nach Artikel 32 Abs. 1 lit. d DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sicherzustellen.

6.5 Der Auftragnehmer ermöglicht eine ordnungsgemäße Kontrolle und Überwachung des Datenschutzes durch den Auftraggeber. Der Auftragnehmer wird insbesondere richtige, vollständige und notwendige Informationen zur Verfügung stellen, Überprüfungen und (Kontroll-)Maßnahmen dulden und Anweisungen des Auftraggebers ausführen. Der Auftragnehmer wird den Auftraggeber informieren, falls eine Datenschutzbehörde Überwachungen und Kontrollen durchführt und im Rahmen ihrer Kontrolle und Überwachung des Datenschutzes an den Auftragnehmer hinsichtlich der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrage des Auftraggebers gemäß der Auftragsverarbeitungsvereinbarung herantritt.

6.6 Ungeachtet der Regelung in den vorstehenden Absätzen unterliegen die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragnehmer verpflichtet, adäquate Maßnahmen nach dem Stand der Technik umzusetzen. Weiterhin ist ihm gestattet, bestehende Maßnahmen durch anderweitige adäquate Maßnahmen zu ersetzen. Dabei muss jedoch sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Änderungen sind zu dokumentieren. Wesentliche Änderungen sind dem Auftraggeber in angemessener Zeit, mindestens aber vier (4) Wochen vor deren Einführung mitzuteilen. Ist dies aufgrund der Erforderlichkeit einer sofortigen Umsetzung aus Gründen der Datensicherheit nicht möglich, wird der Auftragnehmer die entsprechenden Informationen unverzüglich zur Verfügung stellen.

Alternativ kann die Einhaltung der vorstehend vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit durch das Vorlegen einer einschlägigen Zertifizierung mit relevantem Scope nachgewiesen werden. Die Zertifizierung wird Bestandteil dieser Vereinbarung (**Anhang 4**). Die Zertifizierung ist regelmäßig gem. ihren jeweiligen Anforderungen zu erneuern.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber ist berechtigt, die in Ziffer 6.5 vorgesehene Kontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

7.2 Nach vorheriger Ankündigung von mindestens sieben (7) Kalendertagen im Voraus darf der Auftraggeber ohne Anlass – bei bestehendem konkreten Anlass nach Ankündigung ohne Einhaltung einer bestimmten Frist – selbst oder durch einen qualifizierten, unabhängigen Prüfer nach Wahl und auf Kosten des Auftraggebers die Verarbeitungsprozesse des Auftragnehmers überprüfen. Sollten im Rahmen dieser Prüfung Verstöße gegen die Vorgaben dieser Auftragsverarbeitungsvereinbarung aufgedeckt werden, hat der Auftragnehmer die für die Durchführung der Prüfung entstandenen Kosten zu tragen.

7.3 Die Prüfungen sind während der üblichen Geschäftszeiten und innerhalb einer angemessenen Dauer vorzunehmen und sollen den täglichen Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigen.

7.4 Für den Fall der Prüfung durch einen unabhängigen Prüfer ist dieser zur Verschwiegenheit gegenüber Dritten zu verpflichten.

7.5 Der Auftragnehmer unterstützt den Auftraggeber in angemessener Weise bei der Durchführung der Prüfung. Insbesondere erklärt sich der Auftragnehmer dazu bereit, dem Auftraggeber hinreichende Beweise und Informationen über seine Datenverarbeitungsanlagen zur Verfügung zu stellen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8. Subunternehmer

8.1 Der Auftragnehmer darf Subunternehmer nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers beauftragen. Die Zustimmung kann nur erfolgen, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt.

8.2 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer Dritte mit der vollständigen oder teilweisen Erfüllung der im Hauptvertrag vereinbarten Leistung beauftragt. Hiervon ausgenommen sind Lieferanten und Dienstleister des Auftragnehmers, welche keine Daten, die Gegenstand dieser Auftragsdatenvereinbarung sind, verarbeiten. Der Verarbeitung von Daten wird die Möglichkeit der Kenntnisnahme gleichgestellt. Wartung und Reparatur von IT-Systemen oder Applikationen stellt daher ein zustimmungspflichtiges Unterauftragsverhältnis und eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO dar, wenn Systeme betroffen sind, die für die die Erbringung von Leistungen für den Auftraggeber genutzt werden und bei deren Wartung auf personenbezogene Daten zugegriffen werden, die für den Auftraggeber verarbeitet werden.

8.3 Subunternehmer, die in **Anhang 5** zu dieser Auftragsverarbeitungsvereinbarung aufgeführt sind („**genehmigte Subunternehmer**"), werden mit Unterzeichnung dieser Auftragsverarbeitungsvereinbarung als Subunternehmer genehmigt. Verarbeitet ein Subunternehmer die persönlichen Daten des Auftraggebers zulässigerweise außerhalb der EU oder des EWR, trägt der Auftragnehmer Sorge für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus.

8.4 Der Auftragnehmer wählt sämtliche Subunternehmer sorgfältig aus, insbesondere unter Berücksichtigung der von ihnen umgesetzten technischen und organisatorischen Schutzmaßnahmen und überprüft vor der Beauftragung sowie regelmäßig während des Vertragsverhältnisses die Einhaltung der gesetzlichen und vertraglichen Datenschutzbestimmungen durch den Subunternehmer.

8.5 Subunternehmer werden vom Auftragnehmer auf Grundlage einer schriftlichen Vereinbarung beauftragt, die Bestimmungen zur Vertraulichkeit, zum Datenschutz und Datensicherheit enthalten muss, welche den jeweiligen Anforderungen dieser Auftragsverarbeitungsvereinbarung genügen. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen den Subunternehmern

8.6 Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Auftragsverarbeitungsvereinbarung gegenüber dem Subunternehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

8.7 Eine weitere Unterbeauftragung durch den Subunternehmer selbst bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers; sämtliche vertraglichen Regelungen dieser Auftragsverarbeitungsvereinbarung sind auch dem weiteren Unterauftragnehmer aufzuerlegen. Eine Weiterleitung von Daten an einen Unterauftragnehmer ist erst zulässig, wenn alle genannten Voraussetzungen für eine Unterbeauftragung vorliegen.

9. Rechte hinsichtlich personenbezogener Daten

9.1 Alle Rechte an den personenbezogenen Daten und an allen Kopien hiervon verbleiben im Verhältnis zum Auftragnehmer beim Auftraggeber.

9.2 Der Auftragnehmer speichert personenbezogene Daten nur solange, wie das Vertragsverhältnis zum Auftraggeber besteht.

9.3 Der Auftragnehmer darf personenbezogene Daten, Datenträger und Unterlagen kopieren, wenn (i) der Auftraggeber vorher ausdrücklich schriftlich zustimmt, (ii) dies ausdrücklich nach dieser Auftragsverarbeitungsvereinbarung erlaubt ist, (iii) dies für die Zwecke dieser Auftragsverarbeitungsvereinbarung oder des Hauptvertrags erforderlich ist oder (iv) dies im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten zwingend erforderlich ist.

9.4 Soweit der Auftraggeber nicht in der Lage ist, personenbezogene Daten zu berichtigen, zu übertragen, zu löschen oder zu sperren, wird der Auftragnehmer einer entsprechenden Aufforderung des Auftraggebers zur Vornahme einer solchen Handlung unentgeltlich nachkommen.

9.5 Nach Beendigung dieser Auftragsverarbeitungsvereinbarung oder nach Aufforderung durch den Auftraggeber wird der Auftragnehmer unverzüglich, spätestens innerhalb von 30 Tagen, und entsprechend den Weisungen des Auftraggebers entweder alle personenbezogenen Daten, die in seinen Besitz sowie an Subunternehmen gelangt sind, gemäß den geltenden Datenschutzbestimmungen zurückgeben oder löschen und/oder alle personenbezogenen Daten vernichten. Die Löschung und/oder Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

10. Haftung und Schadensersatz

10.1 Der Auftraggeber und der Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

10.2 Im Hinblick auf die Haftung des Auftragnehmers gegenüber dem Auftraggeber gelten die im Hauptvertrag getroffenen Regelungen zur Haftung. Verletzt der Auftragnehmer Pflichten nach dem Hauptvertrag oder dieser Auftragsverarbeitungsvereinbarung, stellt der Auftragnehmer den Auftraggeber von etwaigen Ansprüchen Dritter im Umfang der im Hauptvertrag vereinbarten Haftung frei.

11. Schlussbestimmungen

11.1 Werden personenbezogene Daten, die Gegenstand dieser Auftragsverarbeitungsvereinbarung sind, Gegenstand einer Durchsuchung und Beschlagnahme, einer Zwangsvollstreckung, einer Beschlagnahmung im Rahmen eines Konkurs- oder Insolvenzverfahrens oder ähnlicher Ereignisse oder Maßnahmen Dritter, während sie sich in der Kontrolle des Auftragnehmers befinden, so hat der Auftragnehmer den Auftraggeber unverzüglich hiervon in Kenntnis zu setzen. Der Auftragnehmer hat umgehend alle in eine entsprechende Maßnahme involvierten Parteien darüber zu informieren, dass etwaige betroffene personenbezogene Daten alleiniges Eigentum des Auftraggebers sind und in dessen alleinige Verantwortung fallen, dass die personenbezogenen Daten der alleinigen Verfügungsbefugnis des Auftraggebers unterliegen und dass der Auftraggeber der Verantwortliche im Sinne der DSGVO ist.

11.2 Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB an Daten, Unterlagen, erstellten Verarbeitungs- oder Nutzungsergebnissen ist während der Vertragsdauer und danach (gleichgültig, aus welchem Grund das Auftragsverhältnis endet) ausgeschlossen.

11.3 Änderungen an dieser Auftragsverarbeitungsvereinbarung und/oder seinen Bestandteilen – u. a. in Bezug auf etwaige Zusicherungen und Gewährleistungen des Auftragnehmers – sind nur in Schriftform wirksam und bindend und gelten zudem nur dann, wenn aus der Änderung ausdrücklich hervorgeht, dass diese auf die Bedingungen dieser Auftragsverarbeitungsvereinbarung Anwendung findet.

Vorstehendes gilt ebenso für etwaige Verzichtserklärungen oder Änderungen in Bezug auf die vorgeschriebene Schriftform.

11.4 Ist oder wird eine Bestimmung oder Teilbestimmung dieser Auftragsverarbeitungsvereinbarung unwirksam oder von einem Gericht gleich aus welchem Grund für unwirksam, nicht durchsetzbar oder rechtswidrig erklärt, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt und diese Bestimmung oder Teilbestimmung wird nur insoweit gestrichen oder abgeändert, wie dies notwendig ist, um ihre Wirksamkeit, Durchsetzbarkeit oder Rechtmäßigkeit sicherzustellen.

11.5 Diese Auftragsverarbeitungsvereinbarung unterliegt deutschem Recht unter Ausschluss des Kollisionsrechts.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang 1

Details der Datenverarbeitung

Art der Daten	Art und Zweck der Datenverarbeitung	Kreis betroffener Personen

Hinweise:

Art der Daten:

Bitte detaillierte Auflistung der verwendeten Daten erstellen. Z.B.:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, Email)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

etc.

Kreis der Betroffenen:

Z.B.:

- Kunden
- Beschäftigte
- Abonnenten
- Lieferanten
- Handelsvertreter
- Ansprechpartner

etc.

Anhang 2

Benennung von Ansprechpartnern gem. Ziff. 3.4 und 4.3

1. Weisungsberechtigte Personen im Hinblick auf die Datenverarbeitung nach dieser Auftragsverarbeitungsvereinbarung auf Seiten des Auftraggebers sind:

   Vorname, Name: _____

   E-Mail: _____

   Vorname, Name: _____

   E-Mail: _____

2. Hat der Auftragnehmer eine Person bestimmt, welche die Informationssicherheit, einschließlich des Betriebs des Auftragnehmers, überwacht, können Anfragen des Auftraggebers im Hinblick auf Dokumentation zur Informationssicherheit des Auftragnehmers an diese Person gerichtet werden:

   Vorname, Name: _____

   E-Mail: _____

3. Der Datenschutzbeauftragte des Auftragnehmers ist:

   Vorname, Name: _____

   E-Mail: _____

   Hat der Auftragnehmer keinen Datenschutzbeauftragten bestellt, teilt er dem Auftraggeber die Gründe mit, warum dies nach den einschlägigen Regelungen des Datenschutzrechts nicht erforderlich ist.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch Nachfolger bzw. Vertreter mitsamt Kontaktdaten mitzuteilen. Die Weisungen sind für die Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Anhang 3

Technisch-organisatorische Maßnahmen (TOMs)

Die aufgeführten Maßnahmen dienen ausschließlich als Beispiele. **Die vom Auftragnehmer getroffenen Maßnahmen sind entsprechend darzulegen und der Auftragsverarbeitung als Anhang beizulegen.**

1. Vertraulichkeit (Artikel 32 Abs. 1 lit. b DSGVO)

	Anforderung	Beispielhafte Maßnahmen
a)	**Zutrittskontrolle** Kein unbefugter Zutritt zu Datenverarbeitungsanlagen	z.B. durch ▪ Schlüssel, elektronische Schließung ▪ Protokollierung des Zutritts ▪ Verwaltung und Dokumentation von Zutrittsberechtigungen über den gesamten Lebenszyklus ▪ Werkschutz bzw. Pförtner ▪ Alarmanlage ▪ Videoüberwachung etc.
b)	**Zugangskontrolle** Keine unbefugte Systembenutzung	z.B. durch ▪ (sichere) Kennwörter ▪ starke Authentisierung durch Zwei-Faktor-Authentifizierung ▪ automatische zeitabhängige Sperrmechanismen
c)	**Zugriffskontrolle** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems	z.B. durch ▪ Berechtigungskonzept ▪ bedarfsgerechte (kleinstmögliche) Zugriffsrechte ▪ Protokollierung von Zugriffen ▪ regelmäßige Prüfung erteilter Berechtigungen (Audit) etc.
d)	**Trennungskontrolle** Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden	z.B. durch ▪ getrennte Datenbanken ▪ Mandantenfähigkeit ▪ Sandboxing etc.

2. Integrität (Artikel 32 Abs. 1 lit. b DSGVO)

	Anforderung	Beispielhafte Maßnahmen
e)	**Weitergabekontrolle** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.	z.B. durch ▪ (Transport)Verschlüsselung ▪ Virtual Private Network (VPN) ▪ (kryptologische) Hashfunktion etc.
f)	**Eingabekontrolle** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	z.B. durch: ▪ Protokollierung ▪ Dokumentenmanagement etc.

3. Verfügbarkeit und Belastbarkeit (Artikel 32 Abs. 1 lit. b DS-GVO)

	Anforderung	Beispielhafte Maßnahmen
g)	**Verfügbarkeitskontrolle** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust	z.B. durch ▪ Backup-Strategie (online/offline; on-site/off-site) ▪ Unterbrechungsfreie Stromversorgung (USV) ▪ Überwachung/Monitoring-Systeme ▪ Virenschutz ▪ Firewall
h)	**Rasche Wiederherstellbarkeit**	z.B. durch ▪ Redundanz ▪ Meldewege und Notfallpläne etc.

4. Pseudonymisierung (Artikel 32 Abs. 1 lit. a DSGVO; Artikel 25 Abs. 1 DSGVO)

	Anforderung	Beispielhafte Maßnahmen
e)	Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen (Artikel 4 Nr. 5 DSGVO).	z.B. durch ▪ ersetzen von personenbezogenen Daten durch Zufallsdaten, Codes etc. ▪ Umsetzung von TOMs zum Schutz der Zuordnungsinformationen

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Abs. 1 lit. d DSGVO; Artikel 25 Abs. 1 DSGVO)

	Anforderung	Beispielhafte Maßnahmen
e)	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	z.B. durch ▪ Datenschutz-Management ▪ Incident-Response-Management ▪ Datenschutzfreundliche Voreinstellungen (Artikel 25 Abs. 2 DSGVO)

6. Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

	Anforderung	Beispielhafte Maßnahmen
e)	Unter Verschlüsselung versteht man Verfahren und Algorithmen, die Daten und Dateien (Text, Bild, Audio, Video, etc.) oder auch Netzwerkverbindungen mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht einfach lesbare, betrachtbare oder auslesbare Form umwandeln.	z.B. durch ▪ verschlüsselte Übertragung von Zugangsgeheimnissen (Credentials) ▪ Verschlüsselung von Datenträgern etc. ▪ Vgl. auch Weitergabekontrolle

Anhang 4

Zertifizierungen

Anhang 5

Genehmigte Subunternehmer

Name und Anschrift des Unterauftragnehmers	Ort(e) der Datenverarbeitung	Zweck des Unterauftrags

Bei beabsichtigtem Drittlandtransfer:
Das angemessene Schutzniveau in _____ist festgestellt durch

- ☐ einen Angemessenheitsbeschluss der Kommission gemäß Art. 45 Abs. 3 EU-DSGVO;
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften gemäß Art. 46 Abs. 2 lit. b i.V.m. Art. 47 EU-DSGVO;
- ☐ wird hergestellt durch Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c und d EU-DSGV);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln gemäß Art 46 Abs. 2 lit. e i.V.m. Art. 40 EU-DSGVO;
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus gemäß Art. 46 Abs. 2 lit. f i.V.m. Art. 42 EU-DSGVO;
- ☐ wird hergestellt durch sonstige Maßnahmen gemäß Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b EU-DSGVO: _____