

Anlage Nr. 5

Vereinbarung zur Auftragsverarbeitung

Zwischen

dem Land Baden-Württemberg
vertreten durch das Ministerium der Justiz und für Migration Baden-Württemberg
Friedrichstraße 6
70174 Stuttgart

-nachstehend „**Auftraggeber**“ genannt -

und

dem Unternehmen, welches im gegenständlichen Vergabeverfahren zur Beschaffung des Virtual Court den Zuschlag erhalten hat.

- nachstehend „**Auftragnehmer**“ genannt -

- beide nachstehend gemeinsam „**Vertragsparteien**“ genannt -

wird die folgende Vereinbarung zur Auftragsverarbeitung (nachstehend „Vertrag“) als Anlage zum Vertrag / zur Leistungsbeschreibung (nachstehend „**Hauptvertrag**“) geschlossen.

Präambel

Die Vertragsparteien bezwecken mit dem Vertrag ein Auftragsverarbeitungsverhältnis einzugehen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung („**DSGVO**“), des Bundesdatenschutzgesetzes („**BDSG**“) sowie des Datenschutzgesetzes Baden-Württemberg („**LDSG BW**“) in der jeweils gültigen Fassung zu konkretisieren, schließen die Vertragsparteien den nachfolgenden Vertrag.

1 Definitionen

- (1) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.
- (2) Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit der Vertrag eine andere Form ausdrücklich zulässt.

2 Gegenstand und Dauer der Verarbeitung

- (1) Der Auftragnehmer erhält Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend „**Auftraggeberdaten**“) und verarbeitet diese für den Auftraggeber in dessen

Auftrag und nach dessen Weisungen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO. Der Gegenstand des Auftrages ergibt sich aus Ziffer 1.1 des Hauptvertrages.

- (2) Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert. Die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers Änderungen der Festlegungen in **Anlage 1** dieses Vertrags zuzustimmen, soweit er keinen sachlichen Grund zur Verweigerung dieser Zustimmung hat. Die Änderungen sind schriftlich festzulegen.
- (3) Die Dauer der Verarbeitung ergibt sich aus der Dauer des Hauptvertrages.
- (4) Jede von den Festlegungen in **Anlage 1** des Vertrags abweichende oder darüberhinausgehende Verarbeitung von Auftraggeber-Daten ist dem Auftragnehmer untersagt, insbesondere eine Verarbeitung der Auftraggeber-Daten zu eigenen Zwecken. Das gilt auch für den Fall einer Verwendung anonymisierter Daten.
- (5) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet ausschließlich in Mitgliedstaaten der Europäischen Union ("**EU**") oder Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum ("**EW**R") statt. Eine Datenverwendung außerhalb der EU oder des EWR, auch im Wege der Gewährung des Zugriffs auf Auftraggeber-Daten, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Datenverwendungen in Ländern, die weder Mitgliedstaat der EU oder Vertragsstaat des EWR sind (nachfolgend „Drittländer“ genannt) dürfen nur unter der weiteren Voraussetzung erfolgen, dass die Voraussetzungen der Art. 44 ff. DSGVO zur Zufriedenheit des Auftraggebers erfüllt sind.

3 Weisungsbefugnisse des Auftraggebers

- (1) Der Auftragnehmer darf die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- (2) Der Auftraggeber besitzt insoweit gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Umfang, Zweck und Verfahren der Verarbeitung von Auftraggeber-Daten. Die Weisungen des Auftraggebers sollen grundsätzlich in Schrift- oder Textform erfolgen. Bei Bedarf kann der Auftraggeber Weisungen auch mündlich oder telefonisch erteilen. Mündlich oder telefonisch erteilte Weisungen bedürfen jedoch einer unverzüglichen Bestätigung des Auftraggebers in Schrift- oder Textform. Der Auftragnehmer ist verpflichtet, sämtliche Weisungen des Auftraggebers zu dokumentieren.
- (3) Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich auszuführen. Der Auftraggeber ist berechtigt, dem Auftragnehmer hierfür im Einzelfall eine jeweils angemessene Frist zu setzen, die der Auftragnehmer einzuhalten hat.
- (4) Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Bestimmungen dieses Vertrags und den Weisungen des Auftraggebers verarbeitet. Der Auftragnehmer bestätigt, dass ihm und seinen Mitarbeitern, die mit Auftraggeber-Daten umgehen, die Vorschriften der DSGVO und die sonstigen einschlägigen Datenschutzvorschriften bekannt sind. Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist

nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber mit mindestens 14-tägiger Frist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. Bestätigt der Auftraggeber die Weisung, ist der Auftragnehmer verpflichtet, sie zu befolgen.

4 Anforderungen an Personal und Systeme

- (1) Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten in Schriftform zur Vertraulichkeit während und nach Beendigung ihres Beschäftigungsverhältnisses zu verpflichten, soweit diese nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (2) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
- (3) Die Einhaltung dieser Verpflichtung ist dem Auftraggeber auf Anfordern nachzuweisen.
- (4) Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeber-Daten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der EU oder der Mitgliedstaaten zur Verarbeitung verpflichtet.
- (5) Der Auftragnehmer gewährleistet, dass er nur solche Systeme für die Verarbeitung von Auftraggeber-Daten einsetzt, die dafür ausgelegt sind, den Datenschutz durch eine der Verarbeitungssituation angemessene technische Systemgestaltung zu unterstützen.

5 Pflichten des Auftragnehmers

- (1) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutz-Folgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
- (2) Soweit nach Art. 37 Abs. 1 DSGVO oder anderweitig gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenkonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit. Wurde kein Beauftragter bestellt, teilt der Auftragnehmer dem Auftraggeber einen Ansprechpartner für anfallende Datenschutzfragen mit.

6 Technische und organisatorische Maßnahmen

- (1) Der Auftragnehmer gewährleistet, alle nach Art. 32 DSGVO und § 3 Abs. 1 LDSG BW erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen und während der Dauer der Verarbeitung von Auftraggeber-Daten aufrecht zu erhalten, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und

Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten. Die in **Anlage 2** des Vertrags beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die diesem Vertrag oder seiner **Anlage 2** nicht unmittelbar entnommen werden können, ist nicht zulässig.

- (2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Vertragsparteien zu vereinbaren und zu dokumentieren. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- (3) Personenbezogene Daten dürfen lediglich an die befugten Beteiligten weitergegeben werden.
- (4) Die Verarbeitung von Daten in Privatwohnungen (z.B. bei Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird, die nach Art. 32 DSGVO und § 3 Abs. 1 LDSG BW erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.
- (5) Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.
- (6) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

7 Unterauftragsverhältnisse

- (1) Die gegenwärtig vom Auftragnehmer eingesetzten Subunternehmer sind in **Anlage 3** des Vertrags genannt, mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt.
- (2) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

- (3) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.
- (4) Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Subunternehmer informieren. Der Auftraggeber ist berechtigt, gegen jede beabsichtigte Änderung Einspruch zu erheben. Erhebt der Auftraggeber Einspruch, ist dem Auftragnehmer die beabsichtigte Änderung untersagt. Im Falle zugelassener Änderungen wird der Auftragnehmer die Liste der Unterauftragnehmer in **Anlage 3** entsprechend aktualisieren und dem Auftraggeber unverlangt zur Verfügung stellen.
- (5) Die Genehmigung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt und zudem sichergestellt ist, dass dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind und insbesondere die nach Art. 32 DSGVO und § 3 Abs. 1 LDSG BW erforderlichen technischen und organisatorischen Maßnahmen umfassen. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- (6) Der Auftragnehmer wird vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Subunternehmer geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten gemäß dieser Vereinbarung erfolgt.
- (7) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (8) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.
- (9) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DSGVO und § 3 Abs. 1 LDSG BW sorgfältig aus. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Verlangen zur Verfügung zu stellen.
- (10) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
- (11) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich in einem Mitgliedstaat der EU oder eines Vertragsstaates des EWR erbringen, ist nur bei Beachtung der in Ziffer 2 Abs. 5 dieses Vertrages genannten Bedingungen möglich.
- (12) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen.
- (13) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

8 Rechte der Betroffenen

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

- (2) Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
- (3) Der Auftragnehmer wird insbesondere den Auftraggeber unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeber-Daten unmittelbar an den Auftragnehmer wenden sollte und dem Auftraggeber auf Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeber-Daten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt.

9 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a. 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;
 - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (2) Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen (etwa nach Art. 33 oder 34 DSGVO) auf erstes Anfordern im Rahmen des Zumutbaren zu unterstützen. Der Auftragnehmer wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftraggeber-Daten zu minimieren und zu beseitigen, die Auftraggeber-Daten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.
- (3) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragsabwicklung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

10 Nachweise und Überprüfungen

- (1) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die

gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer - soweit erforderlich - Zutritt und Einblick zu ermöglichen. Der Auftragnehmer sichert zu, dass er bei den Kontrollen – soweit erforderlich – unterstützend mitwirkt. Er ist insbesondere verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Ziffer 5 Abs. 8 dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

- (2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (3) Nach Wahl des Auftraggebers kann der Nachweis der Einhaltung der Pflichten nach diesem Verträge anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit - z.B. nach BSI-Grundschutz - („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.
- (4) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers – auch nach Beendigung dieses Vertrages – vertraulich zu behandeln, sofern er nicht aufgrund gesetzlicher Pflichten zur Herausgabe dieser Informationen verpflichtet ist.
- (5) Der Auftragnehmer unterwirft sich der Kontrolle des behördlichen Datenschutzbeauftragten des Ministeriums der Justiz und für Migration Baden-Württemberg. Er gestattet diesem sowie den für ihn tätigen Personen oder vom Auftraggeber beauftragten Personen während der üblichen Geschäftszeiten den Zutritt zu seinen Geschäftsräumen und gewährt Zugang zu den Datenverarbeitungsanlagen und Unterlagen. Der Auftragnehmer ist verpflichtet, Anfragen des Datenschutzbeauftragten oder den zur Kontrolle beauftragten Personen unverzüglich und vollständig zu beantworten.
- (6) Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen des Auftraggebers wird der Auftragnehmer den Auftraggeber im Rahmen von behördlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist. Der Auftragnehmer wird insbesondere auf Verlangen des Auftraggebers ihm selbst oder der Aufsichtsbehörde unmittelbar alle Informationen im Zusammenhang mit diesem Vertrag geben und entsprechende Auskünfte erteilen und der Aufsichtsbehörde die Möglichkeit einräumen, Prüfungen in demselben Umfang durchzuführen, wie sie die Aufsichtsbehörde beim Auftraggeber durchführen darf. Der Auftragnehmer verpflichtet sich, der zuständigen Aufsichtsbehörde auch in diesem Rahmen alle erforderlichen Zugangs-, Auskunft- und Einsichtsrechte zu gewähren. Falls die Aufsichtsbehörde beim Auftragnehmer Kontrollhandlungen, Ermittlungen oder Maßnahmen durchführt, die Auftraggeber-Daten betreffen, hat der Auftragnehmer den Auftraggeber darüber so früh wie möglich und in der Regel unverzüglich nach Erhalt der Ankündigung der Aufsichtsmaßnahme durch die Behörde zu informieren.

11 Pflichten nach Beendigung des Vertrags

- (1) Bei Beendigung des Vertragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder unwiderruflich zu vernichten oder an den Auftraggeber zu übergeben, sofern nicht eine gesetzliche Pflicht zur Speicherung der personenbezogenen Daten besteht. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.

Schutzklasse 1 – normaler Bedarf für interne Daten	Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner Stellung und seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.
--	---

Alternativen, sofern Daten der Schutzklasse 2 oder 3 verarbeitet werden:

Schutzklasse 2 – hoher Bedarf für vertrauliche Daten	Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.
--	--

Schutzklasse 3 – hoher Bedarf für vertrauliche Daten	Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.
--	--

- (2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
- (3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
- (4) Gesetzliche Aufbewahrungspflichten des Auftragnehmers bleiben von den vorstehenden Regelungen unberührt. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12 Haftung

- (1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
- (2) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftraggeber, seine Beschäftigten bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm

eingesetzten Subunternehmer im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

- (3) Die Absätze 2 und 3 der Ziffer 12 gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

13 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln und Geschäftsgeheimnisse durch den Umständen nach angemessene Geheimhaltungsmaßnahmen zu schützen. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform erforderlich.
- (4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.
- (6) Dieser Vertrag unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist XX.

Anlage 1 – Datenkategorien, Zwecke, Betroffene

Der Auftragnehmer verarbeitet die folgenden personenbezogenen Daten:

I. Zwecke

[Hier sind die Zwecke der einzelnen Verarbeitungstätigkeiten einfügen]

II. Betroffene

[Hier sind die Kategorien betroffener Personen einzutragen, z.B.]

- *Mitarbeiter*
- *Beschäftigte*
- *Ansprechpartner*
- *Interessenten*
- *Bewohner des jeweiligen Gebiets*
- *Kooperationspartner]*

III. Datenkategorien

[Hier sind die Datenkategorien zu benennen, z.B.]

- *Personendaten*
- *Mitarbeiterdaten*
- *Kontaktdaten*
- *Kommunikationsdaten*
- *Zahlungsdaten*
- *Projektdaten*
- *Termine]*

Anlage 2 – Technische und organisatorische Maßnahmen (TOM)

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Es müssen Regelungen zu folgenden Punkten getroffen werden:

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse [1, 2 oder 3].

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

>> Zutrittskontrolle

Folgende Maßnahmen sind umzusetzen, um den unbefugten Zutritt zu Datenverarbeitungsanlagen und Daten zu verhindern: [z. B.

- *Verwendung von Sicherheitsschlössern an Zugangstüren*
- *Festlegung einer Schlüsselregelung, durch die ein möglichst kleiner Personenkreis uneingeschränkter Zugang erhält*
- *bei Generalschlüsselanlage Quittierung der Ausgabe des Generalschlüssels*
- *wenn möglich, vom Publikumsverkehr räumlich abgegrenzte PC-Arbeitsplätze, Server und andere Speichermedien sowie Aufbewahrungsorte von Akten]*

>> Zugangskontrolle

Folgende Maßnahmen sind umzusetzen, um eine unbefugte (System-) Benutzung zu verhindern: [z. B.

- *Benutzererkennung mit sicheren Kennwörtern*
 - *unterschiedlichen Zeichenzusammensetzung, Mindestlänge 8 Zeichen, regelmäßiger Wechsel*
 - *Bildschirmsperre bei Pausen mit Passwort-Aktivierung*
 - *Zugangssperre bei mehr als 3 Anmeldeversuchen*
 - *Vermeidung der Verwendung von Gruppen-Passwörter*
- *Firewall inkl. Zugriffs- und Änderungsberechtigungskonzept*
- *Einsatz von Anti-Viren-Software*
- *Regelmäßige Aktualisierung von Sicherheitspaketen bei Programmen, die mit dem Internet verbunden sind*
- *Sicherung und Verschlüsselung von Datenträgern*
- *bei externer Systemadministration Schließung einer Vereinbarung zur Auftragsdatenverarbeitung*
- *sorgfältige Auswahl des Sicherheits- und Reinigungspersonals]*

>> Zugriffskontrolle

Folgende Maßnahmen sind umzusetzen, damit die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind und damit personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können: [z. B.

- *Benutzererkennung mit sicheren Kennwörtern (siehe auch Zugangskontrolle)*

- *Datenträgerverwaltung inkl. Benennung eines Verantwortlichen*
- *bedarfsgerechte Zugriffsrechte (z.B. für Praktikanten und studentische Hilfskräfte)*
- *gesicherte Schnittstellen (insbesondere bei aktiven Netzkomponenten)*
- *Aufbewahrung von sensiblen Akten in verschließbaren Schränken und Einsatz von Aktenvernichtern]*

2. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

>> Verfügbarkeitskontrolle

Folgende Maßnahmen sind zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust umzusetzen: [z. B.

- *Brandschutzmaßnahmen*
 - *Feuerlöscher an/in den PC- Arbeitsräumen und Aktenaufbewahrungsräumen*
 - *Wenn möglich Brandschutztüren*
 - *Rauchverbot an/in den PC- Arbeitsräumen und Aktenaufbewahrungsräumen*
- *Backupkonzept, z.B. Festplattenspiegelung, Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort*
- *Einsatz von Anti-Viren-Software*
- *Schutz vor Diebstahl (siehe auch Zutritts- und Zugangskontrolle)*
- *Testen von Datenwiederherstellung]*

3. Verfahren zur regelmäßigen Überprüfung,

Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

>> Datenschutz-Management

Der Auftragnehmer ist für die Umsetzung der hier genannten technischen und organisatorischen Maßnahmen zuständig und plant, organisiert, steuert und kontrolliert systematisch die gesetzlichen und betrieblichen Anforderungen des Datenschutzes.

>> Incident-Response-Management

Die Verletzung des Schutzes personenbezogener Daten ist gegenüber dem Auftraggeber unverzüglich zu melden. Ferner sind Art. 33 und 34 DSGVO zu beachten.

>> Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Soweit es die Art der zur Verarbeitung vorgesehenen Daten zulässt, ist darauf zu achten, dass diese pseudonymisiert werden.

>> Auftragskontrolle

Folgende Maßnahmen dienen der Verhinderung einer Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers:

- *Beachtung der Weisungsbefugnis*
- *Kontrollen vor Ort*

[Unterschriften folgen auf der nächsten Seite der Vereinbarung zur Auftragsverarbeitung]

[Fortsetzung der Unterschriftenseite zur Vereinbarung zur Auftragsverarbeitung]

Ort, Datum

Ort, Datum

Unterschrift (Auftraggeber)

Unterschrift
(Auftragnehmer)

Name, Vorname, Funktion
des/der
Vertretungsberechtigten

Name, Vorname, Funktion
des/der
Vertretungsberechtigten

Anlage 3 – Liste der genehmigten Subunternehmer

	Name des Subunternehmers	Kontaktperson	Anschrift	Leistung
1				
2				
3				