A n l a g e 1:
Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiter bei der Auftragsdatenverarbeitung
zum Vertrag über eine Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO

1. Pflichten des Auftragsverarbeiters

1.1.

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. So trifft er alle technischen und organisatorischen Maßnahmen zur angemessenen Sicherung der Daten der Auftraggeber vor Missbrauch und Verlust, die den datenschutzrechtlichen Anforderungen (Art. 32 EU-DSGVO) entsprechen.
Art. 32 Abs. 1 EU-DSGVO regelt hierzu:

> *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*
>
> > *a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
> > *b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
> > *c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Der Auftragsverarbeiter unternimmt zudem Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Europäischen Union oder deren Mitgliedstaaten zur Verarbeitung verpflichtet.

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen so gesichert sind, dass diese Daten nicht ohne aktives Eingreifen einer unbestimmten Zahl von natürlichen anderen Personen zugänglich gemacht werden.

1.2

Der Auftragsverarbeiter stellt dem Auftraggeber zu Beginn dieses Vertrages in Anlage 2 ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung zur Verfügung. Dieses Konzept beschreibt nach Art. 32 Abs. 2 EU-DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ferner sind die Voreinstellungen darzustellen, die gewährleisten, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des

geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
Änderungen in diesem Konzept sind dem Auftraggeber vorher so rechtzeitig anzuzeigen, dass diesem genügend Zeit bleibt, um auf Änderungen entsprechend reagieren zu können. Die jeweils aktuelle Fassung des Konzepts wird dem Auftraggeber zur Kenntnisnahme und Zustimmung übersandt.

1.3.
Der Auftragsverarbeiter stellt dem Auftraggeber die für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO programmspezifischen notwendigen Angaben zur Verfügung (Anlage 2). Die Auftraggeber sollten in ihrem Verzeichnis von Verarbeitungstätigkeiten auf das gesamte Vertragswerk zur Auftragsdatenverarbeitung verweisen.
Ferner führt der Auftragsverarbeiter selbst ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung nach Art. 30 Abs. 2 EU-DSGVO. Dieses Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Auftragsverarbeiter stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

1.4
Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

1.5.
Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktdaten des betrieblichen oder behördlichen Datenschutzbeauftragten mit.

1.6.
Der Auftragsverarbeiter unterrichtet die Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes (z. B. technischer Art), im Falle einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (Art. 33 Abs. 2 EU-DSGVO).

1.7.
Datensicherungen sind vom Auftragsverarbeiter sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Datensicherungen übernimmt der Auftragsverarbeiter in regelmäßigen Abständen, mindestens alle 5 Jahre ab Vertragsbeginn.

1.8.
Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Die Verarbeitung der Daten in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum bedarf der vorherigen Zustimmung des Auftraggebers.

1.9
Nach Ende des Vertragsverhältnisses sind vom Auftragsverarbeiter alle Daten spätestens innerhalb eines Monats zu löschen. Der Auftragsverarbeiter hat dem Auftraggeber die Löschung umgehend schriftlich zu bestätigen.
Der Auftragsverarbeiter muss auf Wunsch des Auftraggebers diesem alle personenbezogenen Daten zurückgeben.

2. Pflichten des Auftraggebers

2.1.
Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei Nutzung der Dienste Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

2.2.
Der Auftraggeber, als für den Datenschutz Verantwortlicher, ist für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO zuständig.

2.3.
Dem Auftraggeber obliegt die Einhaltung der in den Art. 32 bis 36 EU-DSGVO genannten Pflichten. Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 genannten Pflichten unterstützen.

Ferner obliegen dem Auftraggeber die aus den Art. 15 bis 21 EU-DSGVO resultierenden Pflichten gegenüber den Betroffenen, insbesondere über Auskunft, Berichtigung und Löschung. Der Auftragsverarbeiter wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III EU-DSGVO genannten Rechte der betroffenen Person nachzukommen.

3. Kontrollpflichten

Der Auftraggeber überzeugt sich in regelmäßigen Abständen von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und kann sich dazu vom Auftragsverarbeiter deren Einhaltung schriftlich bestätigen lassen. Der Auftraggeber oder dessen Beauftragter kann sich hierüber auch vor Ort selbst überzeugen. Der Auftragsverarbeiter räumt dem Auftraggeber oder dessen Beauftragten insofern ein Zutrittsrecht während der üblichen Arbeitszeit für die Räumlichkeiten und Einrichtungen des Auftragsverarbeiters ein.

Der Nachweis dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Vorgaben der EU-DSGVO erfolgt, kann der Auftragsverarbeiter auch durch Vorlage einer Bestätigung eines anerkannten lizenzierten Auditors, dass genehmigte Verhaltensregeln gemäß Art. 40 EU-DSGVO oder ein genehmigtes Zertifizierungsverfahrens gemäß Art. 42 EU-DSGVO durch den Auftragsverarbeiter eingehalten werden, erbringen.

Der Auftragsverarbeiter muss dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Ver-

fügung stellen sowie Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die EU-DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

Der Auftraggeber hat gegenüber dem Auftragsverarbeiter Weisungsbefugnis hinsichtlich der Verarbeitung der personenbezogenen Daten. Der Auftragsverarbeiter erteilt dem Auftraggeber die hierfür notwendigen Auskünfte und ermöglicht die Überprüfung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen in geeigneter Weise. Im Falle einer Überprüfung durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg gilt dies entsprechend. Der Auftragsverarbeiter gestattet dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit gemäß Art. 58 Abs. 1 lit. e EU-DSGVO jederzeit Zutritt zu den Räumen, in denen er Daten des Auftraggebers im Auftrag verarbeitet, und Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung dessen Aufgaben notwendig sind.

4. Unterauftragsverhältnisse

4.1.
Der Auftragsverarbeiter und dessen Unterauftragnehmer nehmen keine weiteren Unterauftragsverarbeiter als Subunternehmer ohne vorherige gesonderte schriftliche Genehmigung des Auftraggebers in Anspruch. Mit dem Subunternehmer ist durch den Auftragsverarbeiter eine Vereinbarung nach Maßgaben des Art. 28 Abs. 2 bis 4 EU-DSGVO abzuschließen.

4.2.
Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder

eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Auftraggeber und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 EU-DSGVO festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

5. Informationspflicht

Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortliche Stelle“ im Sinne der EU-DSGVO liegen.

6. Sonstiges

Die Vertragspartner vereinbaren, die datenschutzrechtlichen Bestimmungen einzuhalten und ihre Mitarbeiterinnen und Mitarbeiter hierzu zu verpflichten.