

AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV)

der

GIZZImedia GmbH, Glärnischstr. 8, D-78464 Konstanz
Geschäftsführerin: Christine Böck, Alice Boßmann

- nachstehend **Auftragnehmer** genannt -

Präambel

Im Rahmen der Leistungserbringung nach dem mündlichen Vertrag (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich oder zumindest nicht auszuschließen, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert.

Diese Auftragsverarbeitungsvereinbarung (AVV) bildet die vertragliche Basis für die Auftragsvereinbarung im Sinne des Artikels 28 Absatz 3 DSGVO und die Verpflichtungen der Parteien im Hinblick auf die Auftragsverarbeitung.

Dieser AVV liegt sämtlichen Vertragsbeziehungen zwischen dem Auftraggeber und dem Auftragnehmer zugrunde, sofern der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet. Diese AVV ist Teil der AGB des Auftragnehmers und gilt auch dann als vereinbart, wenn in der Vertragsdokumentation nicht ausdrücklich darauf Bezug genommen wird.

Diese Vereinbarung ergänzt den Vertrag ausschließlich zur Erfüllung regulatorischer Voraussetzungen im Bereich des Datenschutzes und der Datensicherheit. In diesen Bereichen ist die AVV vorrangig vor anderen Vertragsdokumenten und ist geltungserhaltend im Sinne der DSGVO und der begleitenden Datenschutzgesetze auszulegen.

§ 1 Anwendungsbereich, Gegenstand und Dauer der Verarbeitung

(1) Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(2) Der Gegenstand und die Dauer des Auftrages sowie Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Hauptvertrag.

(3) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer

Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der hier vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

(4) Gegenstand Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten (z.B. Name, Vorname, Anschrift, Geburtsdatum)
- Kommunikationsdaten (z.B. Telefonnummern, E-Mail-Adressen)
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(5) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Bewerber

(6) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 f. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§ 2 Definitionen

(1) Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).

(2) Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Sinne des Art. 28 DSGVO.

(3) Weisung

Eine Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Berichtigung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag und diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 3 Verantwortlichkeit für die Datenverarbeitung

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Der Auftragnehmer ist für die Einhaltung der auf seinen Verantwortungsbereich bezogenen datenschutzrechtlichen Vorgaben der Artt. 28ff. und Art. 32 DSGVO verantwortlich.

(3) Unbeschadet der Artt. 82, 83 und 84 DSGVO gilt ein Auftragsverarbeiter, der unter Verstoß gegen die Vorschriften der DSGVO die Zwecke und Mittel der Verarbeitung bestimmt und damit insbesondere die Weisungen des Auftraggebers überschreitet, in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 4 Technische und organisatorische Maßnahmen

(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 und deren Einhaltung sicherstellen, die den Anforderungen der Artt. 28 Abs. 3 lit. c, 32 DSGVO in Verbindung mit Art. 5 DSGVO genügen.

(2) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren.

(3) Die Darstellung der technischen und organisatorischen Maßnahmen ist Bestandteil dieser Vereinbarung (siehe Anlage 3: Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen) und Grundlage des Vertrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind zu dokumentieren und dem Auftraggeber mitzuteilen.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten. Der Auftragnehmer hat ausschließlich nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer 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 Person gewährleistet wird. Der Auftragnehmer wird dem Auftraggeber auf Anfrage geeignete Nachweise der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 9 dieser Vereinbarung zur Verfügung stellen.

(3) Der Auftragnehmer stellt sicher und gewährleistet, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO zur Vertraulichkeit verpflichtet wurden. Ferner stellt der Auftragnehmer sicher, dass das von ihm eingesetzte Personal ausreichend in die Schutzbestimmungen des Datenschutzrechts eingewiesen worden ist und darüber hinaus über die sich aus dieser Vereinbarung ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt wird.

(4) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit (sofern ein solcher vom Auftragnehmer nach den gesetzlichen Bestimmungen zu bestellen ist) und den Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen.

(5) Der Auftragnehmer unterrichtet den Auftraggeber insbesondere im Hinblick auf Artt. 33, 34 DSGVO unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Verletzungen des Schutzes personenbezogener Daten gem. Art. 4 Nr. 12 DSGVO oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers, insbesondere über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde beim Auftragnehmer ermittelt. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Artt. 33, 34 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen. Meldungen nach Art. 3 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

(6) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(7) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(8) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

§ 6 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von betroffenen Personen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus Artt. 33, 34 DSGVO resultierenden Meldepflichten.

§ 7 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(2) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 S. 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 8 Unterstützungspflichten

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Informationen oder Auskünfte zur Verarbeitung von Daten dieser Person zu geben oder die Rechte von betroffenen Personen nach Kapitel III (Artt. 12 bis 23) der DSGVO zu gewährleisten, wird der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Pflichten mit geeigneten technischen und organisatorischen Maßnahmen entsprechend Art. 28 Abs. 3 lit. e DSGVO unterstützen.

(2) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten entsprechend Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung der in den Artt. 32 bis 36 DSGVO genannten Pflichten und bei der Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DSGVO).

(3) Im Falle einer Inanspruchnahme einer Vertragspartei durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich die in Anspruch genommene Vertragspartei, die andere Vertragspartei unverzüglich zu informieren. Die Vertragsparteien werden sich bei der Abwehr des Anspruchs gegenseitig unterstützen.

§ 9 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung der in den Artt. 28, 29 DSGVO und dieser Vereinbarung festgelegten Pflichten des Auftragnehmers zu überprüfen. Dieser Nachweis kann durch den Auftragnehmer durch Vorlage einer Bestätigung der Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO erbracht werden, wenn diese dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung zu überzeugen. Alternativ kann der Auftraggeber nach seiner Wahl

entweder Selbstauskünfte des Auftragnehmers einholen oder sich vor Ort persönlich (oder vertreten durch einen hierzu beauftragten Dritten) überzeugen. Bestehen Zweifel, ob technische und organisatorische Maßnahmen des Auftragnehmers die Ausführung der Artt. 28, 29 DSGVO gewährleisten können, steht es dem Auftraggeber frei, sich ein Testat eines Sachverständigen vorlegen zu lassen.

(2) Der Auftragnehmer verpflichtet sich im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Abs. 1 vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags, dem Auftraggeber auf schriftliche Anforderung und eigene Kosten innerhalb einer angemessenen Frist alle Auskünfte zu geben und entsprechende Nachweise verfügbar zu machen, die zur Durchführung einer Kontrolle erforderlich sind. Ferner stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

§ 10 Unterauftragnehmer (weiterer Auftragsverarbeiter nach Art. 28 Abs. 2 und 4 DSGVO).

(1) Der Auftraggeber stimmt hiermit zu, dass der Auftragnehmer andere Auftragsverarbeiter, Subunternehmer oder Unterauftragnehmer (im Folgenden einheitlich: Unterauftragnehmer) beauftragen kann. Gleiches gilt für die Ersetzung eines bestehenden Unterauftragnehmers.

(2) Erteilt der Auftragnehmer unter Beachtung von Abs. 1 Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Der Auftragnehmer versichert, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend § 9 einzuräumen. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(3) Die vom Auftragnehmer eingesetzten Unterauftragnehmer sind in Anlage 2 aufgeführt. Der Auftraggeber genehmigt hiermit die Beauftragung der in Anlage 2 genannten Unterauftragnehmer. Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von

Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen diese Änderung Einspruch zu erheben (Art. 28 Abs. 2 DSGVO).

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen nach Artt. 44 ff. DSGVO sicher.

(5) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber (Art. 28 Abs. 4 S. 2 DSGVO).

(6) Keiner Zustimmung bedarf die Einschaltung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem Hauptvertrag in Anspruch nimmt, auch wenn dabei ein Zugriff auf die Daten des Auftraggebers nicht ausgeschlossen werden kann; dazu zählen insbesondere Telekommunikationsleistungen, Post- oder Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

§ 11 Haftung

Eine zwischen den Vertragsparteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, es sei denn, die Vertragsparteien haben ausdrücklich etwas anderes vereinbart.

§ 12 Schlussvorschriften

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne des Art. 4 Nr. 7 DSGVO liegen.

(2) Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen dieser Vereinbarung und Regelungen aus sonstigen vertraglichen Abreden, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus dieser Vereinbarung vor.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Ausschließlicher Gerichtsstand für alle aus diesem Vertrag sich ergebenden Streitigkeiten ist der Sitz des Auftraggebers. Es gilt deutsches Recht.

Fassung 10.01.2025

Anlagen:

Anlage 1: Spezifikation der personenbezogenen Daten

Anlage 2: Übersicht über die vom Auftragnehmer eingesetzten Unterauftragnehmer

Anlage 3: Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Anlage 1: Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

Spezifikation der personenbezogenen Daten

Bewerberdaten

- Vorname
- Nachname
- Adresse
- Geburtsdatum
- Staatsangehörigkeit
- E-Mail-Adresse
- Telefonnummer
- Mobilnummer
- Erreichbarkeit
- Schulabschluss
- Ausbildung
- Letzte Tätigkeit
- Bewerbungstext
- Job Präferenzen

Die konkrete **Verarbeitung** der Daten besteht in deren:

- Erhebung
- Speicherung
- Organisation
- Übermittlung/ Offenlegung/ Verbreitung
- Abgleich/ Verknüpfung
- Löschung/ Vernichtung

zu folgenden Zwecken

- Bereitstellung der Bewerberdaten für den Auftraggeber
- Statistische Auswertung

Anlage 2: Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

Übersicht über die vom Auftragnehmer eingesetzten Unterauftragnehmer gem. § 10 Abs. 3

UNTERAUFTRAGNEHMER

w3 GmbH

Anschrift

w3 GmbH
Lägelerstr. 31
88250 Weingarten

Baden-Württemberg

Deutschland

Beschreibung der übernommenen Teilleistung

Hosting und Programmier-Partner des Bewerberportals www.zustellerkom.de. Die Daten liegen bei der w3 GmbH auf dem Server in Weingarten, Deutschland.

Anlage 3: Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß (Art. 30 Abs. 1 lit. g i.V.m. Art 32 Abs. 1 DSGVO)

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Informationen zum Standort von Datenverarbeitungsanlagen und Rechenzentren

Die Zustellerkom-Bewerberdatenbank wird vom IT-Unternehmen w3 in Weingarten betreut und gehostet. Der Server steht in Deutschland, in Weingarten.

Es findet eine Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen) statt. Dies umfasst folgende Maßnahmen:

- Schlüssel / Schlüsselvergabe

Es findet eine Zugangskontrolle (keine unbefugte Systembenutzung) statt. Dies umfasst die folgenden Maßnahmen:

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Pausenschaltung)
- Verschlüsselung von Datenträgern und Datensätzen
- Software Firewall
- Hardware Firewall
- Anti-Viren Software

Es findet eine Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems) statt. Dies umfasst folgende Maßnahmen:

- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte)
- Benutzererkennung mit Passwort
- Virenschutz / Firewall
- Regelmäßige Updates der Systeme

Es findet eine Trennungskontrolle / Verwendungszweckkontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden) statt. Dies umfasst die folgenden Maßnahmen:

- „Interne Mandantenfähigkeit“ ist hergestellt
- Separierung von Datenbanken
- Separierung von Tables in Datenbanken

Es findet eine Pseudonymisierung von Datensätzen statt. Dies umfasst die folgenden Maßnahmen:

- Identifizierung von Datensätzen mit IDs anstatt Klarnamen und andere persönlichen Daten

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Weitergabekontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport) statt. Dies umfasst die folgenden Maßnahmen:

- Verschlüsselung / Tunnelverbindung
- Prüfung der Rechtmäßigkeit der Weitergabe von Daten
- Protokollierung

Es findet eine Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind) statt. Dies umfasst folgende Maßnahmen:

- Dokumentenmanagement, Dokumentenlenkung
- Protokollierungs- und Protokollauswertungssysteme
- Sicherung von Protokolldaten gegen Verlust oder Veränderung

Verfügbarkeit oder Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) statt. Dies umfasst die folgenden Maßnahmen:

- Backup-Strategie (offline)
- Schutz vor Diebstahl
- Virenschutz / Firewall

Es ist eine rasche Wiederherstellbarkeit gegeben. Dies wird durch folgende Maßnahmen gewährleistet:

- Szenarioübungen (incl. worst-case)

Technische und organisatorische Umsetzung des Rechts auf Löschung, „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)

Folgende Maßnahmen wurden getroffen:

- Einfache Datenlöschung (ohne Überschreiben)
- Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern
- Automatische Löschung von Datensätzen nach einem festgelegten Ablaufdatum
- Protokollierung von Löschvorgängen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die technischen und organisatorischen Maßnahmen werden in regelmäßigen Abständen evaluiert.

Die dokumentierten Maßnahmen sind unter Berücksichtigung des aktuellen Standes der Technik, angemessener Implementierungs- und Wartungskosten, der Art, des Umfangs und der Zwecke der Verarbeitung, sowie unter Abwägung der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind im Einsatz. Dies wird durch folgende Maßnahmen unterstützt:

- Datenschutz-Management
- Regelmäßige Datenschulungen
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle für Auftragsverarbeiter (AV)
- Eindeutige Vertragsgestaltung

Es liegen folgende Anweisungen, Regeln oder Analysen schriftlich vor:

- Interne Verhaltensregeln
- Risikoanalyse
- Datensicherheitskonzept
- Auftragskontrolle durch Auftragsverarbeiter (AV)