Vertrag zur Auftragsverarbeitung (AV) gemäß Art. 28 Abs. 3 DS-GVO

Zwischen

concept4work GmbH, Friedenstraße 49 -51, 40219 Düsseldorf – nachfolgend Auftragnehmer genannt –

und

_____ – nachfolgend Auftraggeber/Verantwortlicher genannt –

Übersicht der Inhalte

I. Allgemeines

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

Diese Vereinbarung zur Auftragsverarbeitung (nachfolgend „AV") regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Hinblick auf die Erfüllung und Einhaltung gesetzlicher Bestimmungen zum Datenschutz. Die gesetzlichen Grundlagen bilden die Regelungen der Europäischen Datenschutzgrundverordnung (nachfolgend „DS-GVO") und des Bundesdatenschutzgesetzes (nachfolgend „BDSG", n.F. vom 25. Mai 2018).

II. Umfang und Art der vorgesehenen Verarbeitung von Daten

(1) Gegenstand des Auftrags ist nicht die originäre Nutzung oder Verarbeitung personenbezogener Daten des Verantwortlichen durch den Auftragsverarbeiter. Im Rahmen der Leistungserbringung durch den Auftragsverarbeiter kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden. Im Rahmen der Leistungserbringung werden die folgenden Daten von betroffenen Personengruppen Bestandteil der Datenverarbeitung:

Kreis der Betroffenen

☒ Mitarbeiter, Bewerber, Praktikanten, Azubis
☒ Mitglieder (z. B. von Vereinen)
☐ Sonstige (bitte benennen):_____
☒ Kunden /Interessenten
☒ Lieferanten /Dienstleister

Art der personenbezogenen Daten

☒ Name, Vorname, Anrede
☒ Informationen zum Familienstand
☒ Vertragsdaten
☒ Abrechnungsdaten
☒ Protokolldateien mit Personenbezug
☒ Kommunikations- / Verbindungsdaten
☒ Persönliche Informationen wie Hobbies, Interessen (Bewerbungen)
☒ Geburtsdaten
☒ Kontaktdaten
☒ Bank-, Finanz-, Konto-,Transaktionsdaten
☒ Leistungsdaten
☒ Auswertungen

(2) Die Datenverarbeitung findet ausschließlich 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 schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS- GVO erfüllt sind.

III. Verantwortlichkeit und Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher" i. S. v. Art. 4 Nr. 7 DS-GVO).

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihr Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DS-GVO, § 15a TMG oder § 109a TKG besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

(4) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen sind schriftlich zu erteilen.

Regelungen über eine etwaige Vergütung von Mehraufwänden, die in Folge ergänzender Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

IV. Kontrollrecht des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich vor Beginn der Datenverarbeitung und sodann regelmäßig durch Stichprobenkontrollen, die mit einer angemessenen Vorlaufzeit beim Auftragnehmer bzw. dessen Unterauftragnehmer anzumelden sind, von der Einhaltung der gesetzlich und in dieser Vereinbarung übernommenen Verpflichtungen des Auftragnehmers bzw. von dessen Unterauftragnehmer in dessen

Geschäftsbetrieb zu dessen Geschäftszeiten zu überzeugen (Kontrollrecht). Er kann diese Überprüfung selbst durchführen oder durch von ihm zu benennende, auf Vertraulichkeit verpflichtete, Dritte auf seine Kosten durchführen lassen. Dritte in diesem Sinne dürfen keine Vertreter von Wettbewerbern des Auftragnehmers sein. Der Auftragnehmer kann der Überprüfung durch externe Prüfer widersprechen, wenn der vom Auftraggeber ausgewählte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmenachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen,

- Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS- GVO
- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Datenschutzauditoren, Qualitätsauditoren)
- Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z. B. nach BSI-Grundschutz)

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

V. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Auftrages und der Weisung des Auftraggebers. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen unverzüglich nach Kenntnisnahme mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Weiterhin ausgenommen sind separat getroffene Vereinbarungen zur Verarbeitung der Buchhaltungsrelevanten Unterlagen.

(2) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen sowie bei der Einhaltung und Durchführung von Melde- und Informationspflichten gemäß DS-GVO. Des Weiteren unterstützt der Auftragnehmer den Auftraggeber bei der Erstellung von Verzeichnissen von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO und teilt ihm die jeweils erforderlichen Angaben in geeigneter Weise mit.

(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten.

(4) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

(6) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen oder die erteilten Weisungen des Auftraggebers, der im Rahmen der Verarbeitung durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglichmitzuteilen.

Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DS-GVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

Stellt der Auftragnehmer fest oder begründen Tatsachen die Annahme, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, unterrichtet er den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls in Schriftform. Die Information hat eine Darlegung der Art der unrechtmäßigen Kenntniserlangung sowie mögliche nachteilige Folgen der unrechtmäßigen Kenntniserlangung zu beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung oder Kenntnisnahme durch Dritte künftig zu verhindern.

(7) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DS-GVO bestellt hat. Die Kontaktdaten des für den Auftragnehmer bestellten Datenschutzbeauftragten sind auf der Homepage der Auftragnehmerin veröffentlicht und leicht zugänglich: www.concept4work.de

(8) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftraggebers oder genehmigter Subunternehmer ist nur mit schriftlicher Zustimmung des Auftraggebers in Schriftform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform zulässig.

VI. Technische- und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer hat die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung zu überwachen. Er versichert, dass er die gesetzlichen Bestimmungen zur Sicherheit bei der Auftragsverarbeitung gemäß Art. 28 Abs 3 c i.V.m. Art. 32 DS-GVO einhält. Hierzu hat er angemessene Maßnahmen der Datensicherheit (technisch-organisatorische Maßnahmen; TOM) getroffen und gewährleistet unter fortlaufender Vornahme gegebenenfalls erforderlicher Anpassungen ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Datenverarbeitungssysteme. Hierbei wird dem Stand der Technik, der Verhältnismäßigkeit und die Art, der Umfang und die Zwecke der Datenverarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen Rechnung getragen.

(2) Der Auftragnehmer hat die technisch-organisatorischen Maßnahmen vor Beginn der Datenverarbeitung zu dokumentieren und stellt sie dem Auftraggeber im Anhang dieser Vereinbarung zur Prüfung zur Verfügung. Mit Abschluss dieser Vereinbarung werden die dokumentierten Maßnahmen Grundlage der Auftragsverarbeitung.

(3) Die technisch-organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Dem Auftragnehmer ist es insoweit gestattet, alternative adäquate Maßnahmen umzusetzen. Das Sicherheitsniveau der in dieser Vereinbarung festgelegten Maßnahmen darf dabei jedoch nicht unterschritten werden.

VII. Unterauftragsverhältnisse

(1) Der Einsatz von Unterauftragnehmer (Subunternehmer) als weitere Auftragsverarbeiter ist nur nach vorheriger Zustimmung durch den Auftraggeber zulässig.

(2) Ein zustimmungspflichtiges Unterauftragsverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistungserbringung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutzmaßnahmen zu gewährleisten.

Nicht zu den Unterauftragsverhältnissen gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsdienstleistungen, Post- oder Transportdienstleistungen, Wartung oder Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und rechtskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Der Auftraggeber stimmt zu, dass der Auftragnehmer Unterauftragnehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Unterauftragnehmer informiert der Auftragnehmer den Auftraggeber frühzeitig. Der Auftraggeber kann der Änderung innerhalb einer angemessenen Frist aus wichtigem Grund gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung oder Ergänzung als gegeben.

(4) Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(5) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt ihm die Pflicht, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen.

(6) Erbringt ein Unterauftragnehmer die vereinbarte Leistung nicht innerhalb eines Mitgliedsstaates der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt auch, wenn Dienstleister lediglich zur Erbringung von Nebenleistungen i.S.d. Abs. 2 eingesetzt werden sollen.

VIII. Beendigung und Rückgabe von Daten

(1) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grundlage einer Einzelbeauftragung durch den Auftraggeber oder gibt die Daten an den Auftraggeber zurück.

(2) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(3) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

(4)

IX. Schlussbestimmung

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z. B. durch Pfändung oder Beschlagnahmung), durch Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache unverzüglich informieren, dass es sich um Daten handelt, die im Auftrag verarbeitet werden.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen einer schriftlichen Vereinbarung.

(3) Bei etwaigen Widersprüchen zum Hauptvertrag gehen die in diesem Auftragsverarbeitungsvertrag getroffenen Regelungen vor. Sollten einzelne Teile dieser Regelung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen nicht.

(4) Es gilt deutsches Recht. Als Gerichtsstand wird der Sitz des Auftraggebers vereinbart.

Düsseldorf, den _____

Unterschrift Auftraggeber	Unterschrift Auftragnehmer