Vereinbarung über Auftragsverarbeitung

z w i s c h e n

Kunde mit Anschrift

- nachstehend Auftraggeber genannt -

u n d

PitchYou GmbH, vertreten durch den Geschäftsführer Robin Sudermann, Campusallee 9, D-51379 Leverkusen

- nachstehend Auftragnehmer genannt -

§ 1 Gegenstand des Auftrages

(1) Gegenstand des Auftrages ist dem jeweiligen Leistungsvertrag der Parteien zu entnehmen. Der Leistungsvertrag besteht aus Angebot und AGB des Auftragnehmers.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers sowie personenbezogene Daten von Bewerbern im Auftrag des Auftragsgebers. Die Parteien sind sich darin einig, dass auf den Vertrag über die Verarbeitung von personenbezogenen Daten im Auftrag des Auftraggebers die Vorschriften der EU-Datenschutzgrundverordnung (DSGVO), insbesondere die Vorschriften über die Datenverarbeitung im Auftrag, anzuwenden sind. Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Leistungen nach Maßgabe des Art. 28 DSGVO ordnungsgemäß durchzuführen.

(3) Der Vertrag regelt die datenschutzrechtlichen Maßnahmen im Sinne von Art. 28 DSGVO und die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der datenschutzrechtlichen Anforderungen.

§ 2 Dauer, Laufzeit des Auftrages

Die Laufzeit dieses Vertrages ist an die Laufzeit des Leistungsvertrages geknüpft.

§ 3 Kategorien von betroffenen Personen

Die Auftragserfüllung und Datenverarbeitung durch den Auftragnehmer kann folgende Kategorien von natürlichen Personen des Auftraggebers betreffen:

☒Beschäftigte
☒Bewerber

§ 4 Arten der personenbezogenen Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien:

Bewerberdaten (Name, Anschrift, Kontaktdaten, Geburtsdatum, beruflicher Werdegang, berufliche Qualifikationen, persönliche Qualifikationen, zeitliche und örtliche Verfügbarkeit, persönlicher Werdegang, Profilbild, Profilvideo), Namen und Kontaktmöglichkeiten von eigenen Mitarbeitern.

§ 5 Ort der Verarbeitung

(1) Die Datenverarbeitung findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland oder innerhalb der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes statt. Eine Verarbeitung in anderen Staaten ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Der Auftragnehmer führt auf Wunsch des Auftraggebers den Nachweis für das Bestehen eines Angemessenheitsbeschlusses der EU-Kommission gem. Art. 45 Abs. 3 DSGVO und/oder der Garantien und eines angemessenen Schutzniveaus. Der Nachweis kann **durch Vorlage eines entsprechenden Zertifikates einer akkreditierten Zertifizierungsstelle nach Art. 43 DSGVO geführt werden. Der Auftragnehmer verpflichtet sich, die Einhaltung der Garantien und eines angemessenen Schutzniveaus sicherzustellen. Der Auftraggeber behält sich vor, das Vorliegen des Angemessenheitsbeschlusses der EU-Kommission sowie der Garantien und die Einhaltung eines angemessenen Schutzniveaus im Rahmen seiner Audit- und Kontrollrechte jederzeit zu überprüfen.**

§ 6 Kontroll- und Auditrechte des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung der personenbezogenen Daten sowie für die Ausführung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Bei einer Datenverarbeitung im Auftrag arbeitet der Auftraggeber gem. Art. 28 Abs. 1 Satz 1 DSGVO nur mit Auftragsverarbeitern zusammen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen zur Erfüllung der Anforderungen der DSGVO eingerichtet sind.

(2) Der Auftraggeber ist danach verpflichtet und befugt, vor Beginn der Datenverarbeitung und nach seinem Ermessen auch wiederholt nach vorheriger Abstimmung während der üblichen Geschäftszeiten im erforderlichen Umfang die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, zu kontrollieren.

Hierzu ist der Auftraggeber befugt, schriftliche Auskünfte und die Vorlage von Nachweisen über die eingerichteten Datenschutzmaßnahmen sowie über die Art und Weise ihrer technischen und organisatorischen Umsetzung zu verlangen, das Grundstück und die Betriebsstätten des Auftragnehmers zu betreten, nach seinem Ermessen Prüfungen und Besichtigungen vorzunehmen und im erforderlichen Umfang in verarbeitungsrelevante Unterlagen, Verarbeitungs- und Ablaufprotokolle, Systeme und gespeicherte Daten und in Regelungen, Richtlinien und Handbücher zur Regelung der beauftragten Datenverarbeitung einzusehen. Dazu gehören auch Nachweise über die Bestellung eines Datenschutzbeauftragten (sofern notwendig), die Verpflichtung der Mitarbeiter auf die Wahrung der Vertraulichkeit und technische und

organisatorische Konzepte, z.B. Verträge mit Unterauftragnehmern. Die gleichen Rechte besitzen auch Beauftragte des Auftraggebers, z. B. Gutachter oder Sachverständige, soweit sie besonders zur Verschwiegenheit verpflichtet sind oder strafbewehrten berufsständischen Schweigepflichten unterliegen.

(3) Die Rechte des Auftraggebers bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus diesem Vertrag, mindestens jedoch solange der Auftraggeber personenbezogene Daten aus den beauftragten Verarbeitungen speichert.

(4) Die Prüfung erfolgt nach vorheriger Anmeldung. In besonderen Fällen, insbesondere wenn Verarbeitungsprobleme bestehen, meldepflichtige Vorfälle aufgetreten sind oder aufsichtsrechtliche Maßnahmen anstehen oder eingeleitet worden sind, kann die Prüfung auch ohne vorherige Anmeldung erfolgen.

§ 7 Weisungsbefugnisse des Auftraggebers

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Leistungsvereinbarungen und dieser Vereinbarung über Auftragsverarbeitung nur auf dokumentierte Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über einzelne datenverarbeitende Prozesse des Auftragnehmers vor. Die Weisungen werden schriftlich, in Schriftform oder in einem anderen geeigneten elektronischen Format erteilt. Mündliche Weisungen werden unverzüglich in Schriftform, schriftlich oder in einem elektronischen Format bestätigt. Die Weisungen werden über die Dauer des Auftragsverhältnisses, mindestens jedoch für die Dauer ihrer Gültigkeit, aufbewahrt.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften verstößt. Der Auftragnehmer kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Der Auftraggeber haftet für rechtswidrige Weisungen und stellt den Auftragnehmer insoweit von Schadensersatzansprüchen und sonstigen Forderungen frei.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

§ 8 Pflichten des Auftragnehmers

(1) Verarbeitungspflichten

Der Auftragnehmer führt den Auftrag ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.

Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Auftraggebers nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrages oder zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich ist oder eine gesetzliche oder sonstige Aufbewahrungspflicht besteht. Eventuell hergestellte Auszüge, Kopien oder Duplikate sind nach Abschluss der Verarbeitung oder Nutzung vom Auftragnehmer unverzüglich sicher zu löschen bzw. datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.

Der Auftragnehmer verpflichtet sich, nur solche Software, Daten oder Datenträger einzusetzen, die zuverlässig auf Freiheit von schädlicher Software geprüft sind, um ein Einschleusen von Viren etc. zu vermeiden.

(2) Duldungspflichten bei Kontrollen

Der Auftragnehmer verpflichtet sich, in Prüfungen durch den Auftraggeber die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nachzuweisen, Auskünfte zu erteilen und die entsprechenden Unterlagen vorzulegen bzw. Einsicht in die erforderlichen Unterlagen und Systeme zu gewähren und nach vorheriger Abstimmung entsprechende Prüfungen des Auftraggebers vor Ort zu dulden und zu unterstützen. Er verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.

Der Nachweis angemessener technischer und organisatorischer Maßnahmen kann auch durch Vorlage von Testaten oder Zertifikaten oder durch eine Zertifizierung bzw. ein Datenschutzaudit einer unabhängigen Einrichtung bzw. eines autorisierten Sachverständigen geführt werden. Unabhängig von diesen Nachweisen ist der Auftragnehmer verpflichtet, Kontrollen durch den Auftraggeber gem. § 6 dieser Vereinbarung zu dulden.

(3) Informationspflichten

Der Auftragnehmer ist verpflichtet, wesentliche Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmäßigkeit der Durchführung der Auftragsleistungen herabsetzen, unaufgefordert dem Auftraggeber zu melden.

Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen der Aufsichtsbehörde für den Datenschutz, insbesondere gem. Art. 58 DSGVO, und über eventuelle Maßnahmen und Auflagen zum Schutz der personenbezogenen Daten.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Er informiert den Auftraggeber unverzüglich über das Erlöschen oder den Widerruf von Zertifikaten oder von Maßnahmen gem. Art. 41 Abs. 4 DSGVO.

Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten und Änderungen in der Person des betrieblichen Datenschutzbeauftragten oder, wenn keine Bestellpflicht besteht, den Namen und die Kontaktdaten der sonstigen zuständigen Stelle mit.

(4) Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. e und f DSGVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu

stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

(5) Organisationspflichten

Der Auftragnehmer verpflichtet sich zur Einrichtung von Maßnahmen und Dokumentationen, die eine Kontrolle und Nachvollziehbarkeit aller mit der Auftragsverarbeitung zusammenhängenden Tätigkeiten und Verarbeitungsprozesse im Sinne einer Auftragskontrolle und der Ordnungsmäßigkeit der Datenverarbeitung ermöglichen. Datenschutzvorfälle und sonstige sicherheitsrelevante Störungen der Verarbeitung sind einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren und dem Auftraggeber zu melden. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.

Wird die Verarbeitung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, verpflichtet sich der Auftragnehmer, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Verarbeitung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung vom Ort des Auftragnehmers aus der Fall ist.

§ 9 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

(1) Personenbezogene und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der personenbezogenen Daten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrages bekannt werdenden personenbezogenen Daten und sonstige unternehmensinterne Umstände, Daten und Informationen (Betriebsgeheimnisse) vertraulich zu behandeln sowie die im Rahmen dieses Vertrages tätig werdenden Mitarbeiter auch über die Beendigung des Beschäftigungsverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Verarbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er für die Durchführung der Arbeiten nur eigenes Personal einsetzt und die mit der Auftragsdurchführung beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und einer regelmäßigen Schulung unterzieht.

(3) Der Auftragnehmer verpflichtet sich zur Beachtung aller sonstigen Geheimnisse, soweit diese für die Verarbeitung einschlägig sind, wie des Sozialgeheimnisses, des Fernmeldegeheimnisses und sonstiger Berufsgeheimnisse gem. § 203 StGB sowie zur Verpflichtung und Belehrung der Beschäftigten zur Sicherstellung der Wahrung dieser Geheimnisse.

(4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über administrative Zugangsdaten und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen. Von den ihm eingeräumten Zugriffsrechten darf der Auftragnehmer nur in dem Umfang Gebrauch machen, der für die Durchführung der Datenverarbeitung erforderlich ist. Die Verpflichtung zur Wahrung der Vertraulichkeit und der sonstigen Geheimnisse gilt auch über die Beendigung dieses Vertrages

hinaus.

§ 10 Unterauftragsverhältnisse

(1) Mit Unterzeichnung dieses Vertrages stimmt der Auftraggeber der Einschaltung der in der Anlage 2 im Einzelnen aufgeführten Unterauftragnehmer zu.

(2) Im Fall der Einschaltung von weiteren Unterauftragnehmern, wird Auftragnehmer die Unterauftragnehmer nach deren Eignung sorgfältig auswählen. Für die Einschaltung von Unterauftragnehmern, welche eine Datenverarbeitung ausschließlich innerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR) garantieren und auch sämtliche Voraussetzungen für eine rechtskonforme Datenverarbeitung erfüllen, erteilt der Auftraggeber hiermit bereits jetzt ausdrücklich seine Zustimmung. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter rechtzeitig informieren, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Hinzuziehungen bzw. Änderungen bei Vorliegen eines wichtigen Grundes Einspruch zu erheben. Die Einschaltung von Unterauftragnehmern außerhalb der EU und des EWR (auch im Falle von verbundenen Unternehmen) bedarf der ausdrücklichen schriftlichen Einwilligung des Auftraggebers.

(3) Der Auftraggeber kann bei Vorliegen eines von ihm nachzuweisenden wichtigen Grundes, insbesondere bei einer Gesetzes- oder Vertragsverletzung, seine Zustimmung zur Unterbeauftragung widerrufen. Die Unterbeauftragung ist dann unverzüglich einzustellen.

(4) Der Auftragnehmer hat die vertraglichen Vereinbarungen mit jedem Unterauftragnehmer so zu gestalten, dass sie mit den Datenschutzbestimmungen dieses Vertrages vergleichbar sind. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten an einen Unterauftragnehmer ist erst zulässig, wenn eine entsprechende Vereinbarung über eine Auftragsverarbeitung abgeschlossen worden ist und der Unterauftragnehmer alle Anforderungen dieses Vertrages erfüllt hat. Auf schriftliche Anforderung hat der Auftragnehmer dem Auftraggeber Auskunft über die wesentlichen Vertragsinhalte und die Umsetzung der datenschutzrelevanten Verpflichtungen der Unterauftragsverhältnisse, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erteilen.

(5) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind auch solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. sonstige Telekommunikationsleistungen, Wartung und Benutzerservices, Reinigungskräfte oder Prüfer. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(6) Eine Beauftragung von Unterauftragnehmern außerhalb des Gebiets der Bundesrepublik Deutschland oder der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Im Übrigen gelten die Regelungen zu § 5 dieses Vertrages auch für die Beauftragung von Unterauftragnehmern.

§ 11 Mitteilungspflichten bei Störungen und Datenschutzverletzungen

(1) Bei einer Störung der Verarbeitung oder einer Datenschutzverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und für den Auftraggeber ein.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der personenbezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können. Zu den Datenschutzverstößen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne dieses Vertrages.

(3) Die Meldung an den Auftraggeber umfasst alle Informationen, die für den Auftraggeber erforderlich sind, um den Vorfall und seine Meldepflicht an die Aufsichtsbehörde und die Informationspflicht der Betroffenen gem. Art. 33 und 34 DSGVO beurteilen und ggf. fristgerecht die Meldung an die Aufsichtsbehörde und ggf. die Information der Betroffenen vornehmen zu können. Die Meldung an den Auftraggeber umfasst insbesondere Angaben zur Art des Vorfalls und der Verletzung des Schutzes von personenbezogenen Daten, eine Beschreibung der wahrscheinlichen Risiken für die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen und eine Beschreibung der bereits eingeleiteten Maßnahmen zur Behebung bzw. Reduzierung eines möglichen Schadens oder sonstiger Risiken für die Betroffenen und den Auftraggeber.

(4) Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 33 und 34 DSGVO und unternimmt alle in seinen Verantwortungsbereich fallenden Maßnahmen zur Minderung nachteiliger Folgen für die Betroffenen sowie zur Aufklärung des Vorfalls und dessen Folgen. Dies gilt auch nach Beendigung des Vertragsverhältnisses.

§ 12 Rechte der Betroffenen

(1) Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zuständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen im notwendigen Umfang.

(2) Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarten Kontaktpersonen erteilt werden.

§ 13 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert ein dem Risiko für die Rechte und Freiheiten der Betroffenen adäquates Schutzniveau der personenbezogenen Daten zu. Zu diesem Zweck verpflichtet sich der Auftragnehmer, seine innerbetriebliche Organisation und die erforderlichen technischen und organisatorischen Maßnahmen unter Berücksichtigung des jeweiligen Stands der Technik, der

Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen so zu gestalten und laufend zu aktualisieren, dass diese den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten.

Die technischen und organisatorischen Maßnahmen umfassen insbesondere

a) die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten,
b) die rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls und
c) die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Der Auftragnehmer sichert die Einhaltung der in der Anlage 1 genannten technischen und organisatorischen Maßnahmen zu. Diese Maßnahmen gelten als vereinbart und die Beschreibung der Maßnahmen in der Anlage 1 wird Bestandteil dieses Vertrages.

(3) 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 sind zu dokumentieren.

(4) Der Auftragnehmer kann die Eignung der nach Art. 32 DSGVO zu treffenden technisch-organisatorischen Maßnahmen gegebenenfalls durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder eines Datenschutzsiegels oder Prüfzeichen nach Art. 42 DSGVO nachweisen, das für die vertragsgegenständlichen Verarbeitungsverfahren und Orte erteilt und für die unter diese Vereinbarung fallenden Verarbeitungsverfahren relevant ist. Der Auftragnehmer hat Veränderungen am Zertifikat oder dessen Ablauf dem Auftraggeber unverzüglich mitzuteilen. Die Kontroll- und Auditrechte des Auftraggebers bleiben unberührt.

§ 14 Verfahren nach Beendigung des Auftrages

(1) Nach Abschluss der Verarbeitung, spätestens nach Beendigung dieses Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten personenbezogenen oder sonstige vertrauliche Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder in Abstimmung mit dem Auftraggeber datenschutzgerecht zu vernichten oder sicher zu löschen. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen. Diese Verpflichtung gilt in gleichem Maße auch für eventuell beauftragte Unterauftragnehmer. Unberührt bleiben Kopien, die zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.

(2) Für diese Daten ist die Verarbeitung gem. Art. 18 DSGVO einzuschränken. Die Daten dürfen durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden und sind nach Ablauf der Aufbewahrungsfrist unverzüglich sicher zu löschen. Der Auftraggeber ist auf Anforderung über Art und Umfang dieser gespeicherten Daten zu unterrichten.

(3) Der Auftragnehmer hat dem Auftraggeber nach Beendigung dieses Vertrages die sichere Löschung bzw. die sichere Vernichtung aller in seinem Besitz befindlichen Unterlagen der Daten des Auftraggebers bzw. die Einschränkung der Verarbeitung an Daten des Auftraggebers gem. Art. 18 DSGVO schriftlich zu bestätigen.

§ 15 Vertragsdauer, Kündigung

(1) Die Vertragsdauer richtet sich nach der Laufzeit des Leistungsvertrages.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers oder eines Unterauftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen diese Vereinbarung vorliegt, der Auftragnehmer oder ein Unterauftragnehmer einer rechtmäßigen Weisung des Auftraggebers nicht nachkommt oder ein Auftragnehmer oder der Unterauftragnehmer sich einer angemessenen Datenschutzkontrolle entzieht.

(3) Eine Kündigung des Vertrags kann nur schriftlich erfolgen.

§ 16 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

§ 17 Haftung

Für die Haftung gelten die Regelungen des Art. 82 DSGVO.

§ 18 Namen und Kontaktdaten der zuständigen Stelle beim Auftragnehmer

Zuständige Stelle:
PitchYou GmbH, Campusallee 9, 51379 Leverkusen,
E-Mail: info@pitchyou.de

Datenschutzbeauftragter:
Sebastian Herting
Vertreter: Philipp Lehmann
Herting Oberbeck Datenschutz GmbH
Hallerstraße 76
20146 Hamburg
https://www.datenschutzkanzlei.de
E-Mail: datenschutz@talentsconnect.com

§ 19 Anwendbares Recht und Gerichtsstand

(1) Das anwendbare Recht und der Gerichtsstand richten sich nach den Regelungen des jeweiligen Leistungsvertrages.

(2) Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

Datum

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Anlage 1
Beschreibung der vereinbarten technischen und organisatorischen Maßnahmen

Folgende technische und organisatorische Maßnahmen sind eingerichtet und gelten als vereinbart:

1. Zugangskontrolle:

Der Auftragnehmer hat folgende Zugangskontrollen eingerichtet, die es verhindern, dass Datenverarbeitungssysteme von Unbefugten verarbeitet und genutzt werden können:

- Sicherheitsschloss für Büroräume
- Sämtliche Daten werden auf einem Server in einem Rechenzentrum der Firma Hetzner (Serverstandort Deutschland) gespeichert.
- Lokale Rechner unserer Mitarbeiter mit der jeweils aktuellen stabilen Betriebssystem-Version. Sämtliche eingesetzten Programme werden ebenfalls auf dem aktuellen Stand gehalten.
- Sämtliche lokalen Rechner sind per Passwort geschützt. Zusätzlich ist die Festplatte verschlüsselt.
- Mitarbeiter dürfen außerhalb der Büroräume an Projekten arbeiten. Es ist vorgeschrieben, dass keine öffentlichen WLANs genutzt werden dürfen.
- Sämtliche Mitarbeiter sind auf das Datengeheimnis verpflichtet.

2. Datenträgerkontrolle:

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern:

- Kennwortverfahren für alle Ebenen (lokales Netzwerk, Server, Anwendungen) u.a. mit Sonderzeichen, Mindestlänge.
- Automatische Sperrung bei mehrfacher Falscheingabe von Kennwörtern
- Zugriff auf Server nur über SSH und zertifikatsbasiertes Login.

3. Speicherkontrolle:

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten:

- Kennwortverfahren für alle Ebenen (lokales Netzwerk, Server, Anwendungen) u.a. mit Sonderzeichen, Mindestlänge.
- Automatische Sperrung bei mehrfacher Falscheingabe von Kennwörtern
- Zugriff auf Server nur über SSH und zertifikatsbasiertes Login

4. Benutzerkontrolle:

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

- Kennwortverfahren für alle Ebenen (lokales Netzwerk, Server, Anwendungen) u.a. mit Sonderzeichen, Mindestlänge.
- Automatische Sperrung bei mehrfacher Falscheingabe von Kennwörtern
- Zugriff auf Server nur über SSH und zertifikatsbasiertes Login

5. Zugriffskontrolle:

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogene Daten Zugang haben.

- Es wird sichergestellt, dass nur die Zugriffsrechte vergeben werden, die zur Erfüllung der jeweiligen Aufgabenstellung erforderlich sind.
- Die Vergabe und Freigabe von Zugriffsrechten ist nachvollziehbar dokumentiert, sodass festgestellt werden kann, wer auf die Daten Zugriff hat.
- Das Vergabeverfahren und die Zugriffrechte werden regelmäßig geprüft und bestätigt. Zugriffsrechte werden unverzüglich entzogen, sofern sie nicht mehr erforderlich sind.
- Für alle Daten ist jeweils ein Verantwortlicher festgelegt, der entscheidet, wer welchen Zugriff erhalten darf.
- Zugriffsrechte werden angepasst, wenn sich die Aufgabenstellungen in den Geschäftsabläufen ändern.
- In den Applikationen ist sichergestellt, dass die zugeteilten Zugriffsrechte technisch umgesetzt sind.
- In allen Umgebungen, die Produktionsdaten enthalten (auch Entwicklung, Test etc.), wird der unbefugte Zugriff ausgeschlossen.
- Benutzerberechtigungen für Mitarbeiter werden zentral vergeben und sind ausschließlich personenbezogen
- Benutzerberechtigungen werden ausschließlich rollenbezogen (bei Eintritt oder Positionsänderung) vergeben: Development, Application Support, Infrastructure Support, Management.
- (Virtuelle) Server-Rechner sind durch 2-Faktor-Authentifzierung geschützt. Der Zugriff ist über eine zentrale Hardware-Firewall limitiert.
- Angriffsversuche von außen werden durch installierte Tools (Prometheus und Grafana) detektiert.

6. Übertragungskontrolle:

Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung, ihrer Speicherung auf Datenträger oder während ihres Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- Die Daten werden bei Transport, Speicherung, Übertragung und Verarbeitung außerhalb des geschützten Bereiches des Unternehmens mit Verfahren wie starker Verschlüsselung, Zwei-Faktor-Authentifizierung gesichert (z. B. Festplattenverschlüsselung).
- Es sind Anweisungen für die Handhabung von Informationen festgelegt und die Mitarbeiter werden geschult, um den Missbrauch der Daten zu verhindern (z.B. zertifizierte Entsorgung von Papier und Datenträger, Auswahl der Übermittlungsverfahren).
- Kryptografische Schlüssel zum Schutz der Daten werden sicher in einem entsprechenden Managementsystem verwaltet.

7. Transportkontrolle:

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- Elektronische Signatur durch SSL-Zertifikat
- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- SSH

8. Wiederherstellbarkeit:

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können:

- Eine Backup-Routine sichert die Daten auf einem extra Backup-Space unseres Providers (derzeit die Firma Hetzner – siehe Anlage 2).

9. Zuverlässigkeit:

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

- Service Desk zur Fehlermeldung

10. Datenintegrität:

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können:

- Ausgiebige Tests von produktiver Inbetriebnahme neuer IT-Systeme
- Eine Backup-Routine sichert die Daten auf einem extra Backup-Space unseres Providers (derzeit die Firma Hetzner – siehe Anlage 2).

11. Auftragskontrolle:

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Eindeutige Vertragsgestaltung
- Kontrolle der Vertragsausführung

12. Verfügbarkeitskontrolle:

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- Eine Backup-Routine sichert die Daten auf einem extra Backup-Space unseres Rechenzentrum-Providers (Unterauftragnehmer Hetzner – siehe Anlage 2).
- Aktueller Virenschutz / Aktuelle Firewall
- Alle Datenbackups erfolgen täglich und können innerhalb eines halben Tages wieder hergestellt werden.
- Backup-Daten sind physikalisch von den Daten des laufenden Betriebs getrennt

13. Trennbarkeit:

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können:

- Die Verarbeitung von Daten erfolgt auf Serversystemen, die durch ein System von verschiedenen Zugriffskontrollen und Zugriffsrechten getrennt sind (vergleiche hierzu die Regelungen in Ziffern 1. und 4. dieser TOMs).
- Das Regelwerk für Informationssicherheit und Datenschutz sowie die Sicherheitsmaßnahmen werden regelmäßig auf Einhaltung und Wirksamkeit geprüft.
- Es gibt eine System- und Softwareentwicklungsrichtlinie, die die Aspekte des Datenschutzes beinhaltet.

14. Eingabekontrolle:

Anlegen, Ändern und Löschen von Daten durch die Software ist nur unter einem Benutzernamen erlaubt. Benutzernamen sind immer einzel-personenbezogen. Alle Datenänderungen und -löschungen werden unter dem entsprechenden Benutzernamen protokolliert. Das Berechtigungskonzept der Software sieht nur Berechtigungen für einzelne Personen (nie für Gruppen) vor.

Anlage 2
Unterauftragnehmer

Unterauftragnehmer, Name, Adresse	**Beauftragte Leistungen**	**Datenschutzkontakt**
Amazon Web Services EMEA SARL 28 Avenue John F. Kennedy L-1855 Luxemburg	Server, Cloud Hosting Nur bei Nutzung der KI-Komponente: Amazon Bedrock	aus-EU-privacy@amazon.com
360dialog GmbH Torstraße 61 D-10119 Berlin	Zugang zur WhatsApp Business API	René Rautenberg +49 89 55294870 info@er-secure.de
Nur bei Nutzung der automatisierten Übersetzung: DeepL SE Maarweg 165 D-50825 Köln	Übersetzung von Messages	Dr. Christian Lenz +49 2261 81950 datenschutz@dhgp.de
Nur bei Nutzung der p78 Schnittstelle zu SAP SuccessFactors: Projekt0708 GmbH Leopoldstraße 37 a D-80802 München	Übertragung von Bewerberdaten in das SAP SuccessFactors-System des Auftraggebers	Katja Hauser +49 40790 2350 datenschutz@projekt0708.com