Vertrag
über die Auftragsverarbeitung

zwischen

(nachfolgend der „**Auftraggeber**“)

und

talentsconnect operations GmbH
Niehler Straße 104
50733 Köln
(nachfolgend „**Auftragnehmer**“)

(nachfolgend einzeln oder gemeinsam "**Partei**" oder "**Parteien**")

1. Auftrag und Festlegungen zur Verarbeitung

1.1. Dieser Vertrag über die Auftragsverarbeitung (nachfolgend „**AVV**“) konkretisiert für alle Verarbeitungen die datenschutzrechtlichen Rechte und Pflichten der Parteien, welche sich aus den zwischen den Parteien bereits bestehenden oder künftig abzuschließenden Verträgen (nachfolgend „**Hauptvertrag**“) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers kommt. Dieser AVV erfasst nicht diejenigen Verarbeitungen, die im eigenen Verantwortlichkeitsbereich des Auftragnehmers gemäß Hauptvertrag erfolgen. Anlage 2 – Technische und organisatorische Maßnahmen gilt jedoch entsprechend auch für Datenverarbeitungen in eigener Verantwortlichkeit des Auftragnehmers.

1.2. Dieser AVV kommt mit all seinen Bestandteilen zur Anwendung, wenn der Auftraggeber den Auftragnehmer zur Verarbeitung personenbezogener Daten (nachfolgend „**Daten**“) im Auftrag gemäß Art. 28 DSGVO verpflichtet hat. Dabei bildet dieser AVV den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

1.3. Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV mit all seinen Bestandteilen den Regelungen des zugehörigen Hauptvertrages vor.

1.4. Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (nachfolgend „**Festlegungen**“) werden vor Beginn der Verarbeitung in Anlagen zum AVV (nachfolgend „**Anlagen**“) geregelt. Dies sind insbesondere

Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorien von Daten und die Kategorien betroffener Personen („**Anlage 1 – Festlegungen**") sowie die technischen und organisatorischen Maßnahmen (nachfolgend „**TOM**").

1.5. Die Anlagen sind Teil des AVV. Bei etwaigen Widersprüchen gehen die Anlagen der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den Anlagen auf den AVV Bezug genommen, so ist der AVV mit all seinen Bestandteilen gemeint.

2. Verantwortlichkeit und Verarbeitung auf Weisung

2.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („**Verantwortlicher**" gemäß Art. 4 Nr. 7 DSGVO).

2.2. Der Auftragnehmer handelt wegen der Verarbeitung der Daten ausschließlich weisungsgebunden, es sei denn es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Wird der Auftraggeber als Auftragsverarbeiter für einen Dritten tätig, gelten die Verpflichtungen des Auftraggebers aus dieser Auftragsverarbeitung für den Dritten unmittelbar als Weisungen des Auftraggebers im Verhältnis zum Auftragnehmer, sofern diese Verpflichtungen strenger sein sollten als diejenigen aus diesem AVV. Der Auftraggeber wird den Auftragnehmer über solche Anforderungen Dritter an die Auftragsverarbeitung in Textform in Kenntnis setzen.

2.3. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (nachfolgend „**Sperrung**"), wenn der Auftraggeber dies anweist und dies sonst vom Weisungsrahmen umfasst ist.

2.4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz oder diesen AVV verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Auftragnehmer ablehnen.

2.5. Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen (a) die Weisungen des Auftraggebers kennen und diese beachten, sowie (b) sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

3. Sicherheit der Verarbeitung

3.1. Die Parteien vereinbaren TOM gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten in einer Anlage zu diesem AVV (nachfolgend „**Anlage 2 – Technische und organisatorische Maßnahmen**").

3.2. Änderung der TOM bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber als neue Fassung der Anlage 2 - Technische und organisatorische Maßnahmen in Textform mitzuteilen.

Änderungen zum Nachteil des Auftraggebers bedürfen dessen vorheriger Zustimmung in Textform.

4. Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

4.1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der ihm vom Auftraggeber anvertrauten Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht.

4.2. Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu unterrichten.

4.3. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß 4.1 oder der Fehler gemäß 4.2 sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für die betroffenen Personen. Hierüber stimmt er sich mit dem Auftraggeber ab. Mündliche Unterrichtungen sind unverzüglich in Textform nachzureichen.

5. Übermittlung von Daten an einen Empfänger in einem Drittland oder in einer internationalen Organisation

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter Einhaltung der in Art. 44 ff. DSGVO festgelegten Bedingungen und nach vorheriger Zustimmung des Auftraggebers in Textform zulässig. Einzelheiten werden in einer oder mehreren Anlagen geregelt.

6. Unterbeauftragungen durch den Auftragnehmer

6.1. Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „**Unterauftragnehmer**“) erbringen lassen.

6.2. Bei Unterzeichnung des AVV setzt der Auftragnehmer die in „**Anlage 3 – Unterauftragnehmer**“ genannten Unterauftragnehmer ein. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt.

6.3. Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

6.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

7. Rechte betroffener Personen und Unterstützung des Auftraggebers

Macht eine betroffene Person Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

8. Kontroll- und Informationsrechte des Auftraggebers

8.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

8.2. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit kann der Auftragnehmer auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Verhaltensregeln nach Art. 40 DSGVO oder Zertifizierungen nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Auftragnehmer hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Weitere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) können zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden. Das Inspektionsrecht des Auftraggebers aus Ziff. 8.3 bleibt hiervon unberührt.

8.3. Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen TOM abhängig machen.

8.4. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien die umzusetzenden Maßnahmen ab.

8.5. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

9. Haftung und Schadenersatz

9.1. Macht eine betroffene Person gegenüber einer Partei Schadensersatzansprüche wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

9.2. Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

9.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei, zur Aufsichtsbehörde oder gegenüber Dritten gefährden.

10. Laufzeit

10.1. Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit einer Anlage wird in der jeweiligen Anlage geregelt; ohne eine solche Regelung läuft die Anlage auf unbestimmte Zeit.

10.2. Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor alle Anlagen beendet wurden.

10.3. Eine Anlage endet mit Beendigung des zugehörigen Hauptvertrags, ohne dass es einer gesonderten Kündigung dieser Anlage bedarf. Der Auftragnehmer hat in diesem Fall nach Wahl des Auftraggebers unverzüglich die nach der Anlage verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform zu bestätigen. Sofern der Auftragnehmer eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen.

11. Kosten

Jede Partei trägt die ihr im Zusammenhang mit diesem AVV anfallenden Kosten selbst.

12. Schlussbestimmungen

12.1. 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 in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

12.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen, Ergänzungen oder Kündigung dieses Vertrags bedürfen zu ihrer Wirksamkeit der Textform. Dies gilt auch für eine Änderung dieser Formklausel. Abweichende mündliche Abreden der Parteien sind unwirksam.

12.3. Sollte eine der Bestimmungen ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, oder eine von den Parteien bei Abschluss nicht bedachte Lücke enthalten, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. An Stelle der rechtsunwirksamen, nichtigen oder fehlenden Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133,

157 BGB geschlossen werden kann. Beide Parteien sind jedoch verpflichtet, unverzüglich Verhandlungen aufzunehmen mit dem Ziel einer Vereinbarung an Stelle der rechtsunwirksamen, nichtigen oder fehlenden Bestimmung, die deren Sinn und Zweck in rechtlicher und wirtschaftlicher Hinsicht am nächsten kommt.

12.4. Auf die von den Parteien hierunter erbrachten Leistungen und sonstigen Handlungen findet ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und des Kollisionsrechts Anwendung; Art. 3 Abs. 3, Abs. 4 Rom-I VO bleiben unberührt.

Unterschriften:

,	Köln,
_____	_____
	John Shiles
	CPO
Auftraggeber	**Auftragnehmer**

Anlagen:

- Anlage 1 – Festlegungen
- Anlage 2 – Technische und organisatorische Maßnahmen
- Anlage 3 – Unterauftragnehmer
- Anlage 4 – Kontaktdaten

Anlage 1

Festlegungen

Die Parteien treffen zum Vertrag über die Auftragsverarbeitung ergänzend folgende Festlegungen zur Spezifizierung der Produkte **JobShop, ChatAgent,** und **talentsconnect Home**:

1. Gegenstand und Zweck der Datenverarbeitung

A. JobShop (Fast Application) Gegenstand der Verarbeitung ist die Bereitstellung einer Bewerbungsschnittstelle (Fast Application) für einen optimierten Bewerbungsprozess auf unserer cloudbasierten Karriereseite (JobShop).

- **Zweck:** Ermöglichung von Online-Bewerbungen, Übermittlung von Bewerberdaten an das Bewerbermanagementsystem (ATS) des Auftraggebers, sowie (optional) interne Bewerbungen durch einen internen JobShop.

B. talentsconnect Home (ManagementKonsole für JobShop) Gegenstand der Verarbeitung ist die Bereitstellung einer zentralen Administrationsoberfläche für Mitarbeiter des Auftraggebers (insb. Recruiter, HR-Manager, Administratoren).

- **Zweck:** Verwaltung der JobShop-Inhalte, Konfiguration der Recruiting-Kampagnen, Nutzerverwaltung für das System sowie Auswertung von Recruiting-Kennzahlen (Analytics & Reporting) und Auswertung der Nutzung.

C. ChatAgent und Webchat Gegenstand ist die Ermöglichung einer Kommunikation zwischen Bewerbern und dem Auftraggeber via Chat-Schnittstellen (z.B. WhatsApp Business API).

- **Zweck:** Automatisierte Erstansprache, Beantwortung von Rückfragen und Erfassung von Bewerbungen über Messenger-Dienste.

2. Kategorien betroffener Personen

- **Bewerber:** Personen, die sich über die Fast Application oder Chat-Schnittstellen für Stellen interessieren oder bewerben.
- **Beschäftigte (Administrativ):** Mitarbeiter des Auftraggebers (z.B. Recruiter, Administratoren), die **talentsconnect Home** zur Steuerung und Analyse nutzen.
- **Beschäftigte (Nutzer):** Mitarbeiter des Auftraggebers, die den **internen JobShop** zur internen Bewerbung nutzen.

3. Kategorien personenbezogener Daten

Bewerberdaten:

- **Stammdaten:** Name, Vorname, Anschrift, E-Mail-Adresse, Telefonnummer.
- **Bewerbungsunterlagen:** Lebenslauf, Zeugnisse, Qualifikationen, Anschreiben, Foto (sofern vom Bewerber bereitgestellt).
- **Präferenzen:** Interessen an Fachbereichen, Standorten oder Beschäftigungsarten.
- **Kommunikationsdaten:** Chat-Inhalte, E-Mail-Korrespondenz, Zeitstempel der Interaktion.

Beschäftigtendaten (talentsconnect Home & Internal JobShop):

- **Identifikationsdaten:** Name, geschäftliche E-Mail-Adresse, Abteilung, Position.
- **Zugangsdaten:** Benutzername, (gehashte) Passwörter, Berechtigungsrollen.
- **Log- und Nutzungsdaten:** IP-Adresse, Zeitpunkte der Logins, vorgenommene Systemänderungen (Audit Logs), Interaktionen mit der Management-Konsole.

Anlage 2

Technische und organisatorische Maßnahmen

Gültig für die Produkte JobShop, ChatAgent und talentsconnect Home:

Diese Anlage beschreibt die gemäß Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen. Sie berücksichtigen den Einsatz einer hybriden Infrastruktur (AWS und Dembach Goo Informatik) sowie die Integration von KI-Diensten über Amazon Bedrock.

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

1.1 Zutrittskontrolle

Verhinderung des unbefugten Zutritts zu Datenverarbeitungsanlagen:

1. **Rechenzentren (AWS):** Die physische Sicherheit der AWS-Rechenzentren (Region: Europa/EWR, primär Frankfurt) wird durch AWS gemäß ISO 27001 und SOC 1/2/3 Standards gewährleistet (Zutritt nur für autorisiertes Fachpersonal, Videoüberwachung, biometrische Scanner).
2. **Rechenzentren (DGi - JobShop):** Betrieb in zugangsgesicherten Räumen an Standorten in Deutschland (DUS1, DUS5). Maßnahmen umfassen Chipkarten mit PIN, Handscanner, Vereinzelungsschleusen und 24/7 personelle Besetzung.
3. **Büroräume (talentsconnect):** Zutritt zu Büroflächen ist über individuelle elektronische Dongles geschützt. Serverschränke befinden sich in einem extra gesicherten Raum.

1.2 Zugangskontrolle

Verhinderung der unbefugten Systemnutzung:

1. **Identitätsmanagement:** Streng personenbezogene Benutzeraccounts mit verpflichtender Passwort-Richtlinie (z.B. Mindestlänge, Anzahl Sonderzeichen, vorherige Passwörter); verpflichtende MFA (Multi-Faktor-Authentifizierung) für alle administrativen Zugänge. Rechteverwaltung nur über abteilungs-/positionsabhängige Benutzergruppen.
2. **Verschlüsselung der Endgeräte:** Sämtliche Mitarbeiter-Laptops verfügen über eine vollständige Festplattenverschlüsselung.
3. **Mobiles Arbeiten:** Zugriff auf die Infrastruktur ist nur über ein verschlüsseltes VPN oder den AWS Systems Manager Session Manager gestattet.

1.3 Zugriffskontrolle

Gewährleistung, dass Berechtigte nur auf die ihrer Berechtigung unterliegenden Daten zugreifen:

1. **Need-to-Know-Prinzip:** Rollenbasierte Berechtigungsvergabe (RBAC) nach dem Prinzip der minimalen Rechtevergabe.
2. **Authentifizierung:** Authentifizierung an Servern nur über passwortgeschützte private Schlüsseldatei (“Private Key”).
3. **KI-Datenisolation (Bedrock):**
    - **VPC-Endpunkte:** Die Kommunikation mit KI-Modellen erfolgt ausschließlich über private VPC-Endpunkte innerhalb des AWS-Netzwerks. Daten verlassen das gesicherte Netzwerk des Auftragsverarbeiters zu keinem Zeitpunkt über das öffentliche Internet.
    - **Logische Isolation:** Datenströme innerhalb von Amazon Bedrock sind logisch von anderen AWS-Kunden und den Modellanbietern (z. B. Anthropic) isoliert. Modellanbieter haben keinen Zugriff auf Eingabedaten (Prompts) oder Ausgaben.
4. **Review-Prozesse:** Regelmäßige Prüfung der Zugriffsrechte.

1.4 Trennungskontrolle

Gewährleistung der getrennten Verarbeitung zu unterschiedlichen Zwecken:

- **Logische Mandantentrennung:** Strikte Trennung der Kundendaten auf Datenbankebene (VPC).
- **Systemtrennung:** Trennung von Entwicklungs-, Test- und Produktivsystem
- **KI-Zweckbindung & Trainingsverbot:**
    - **Kein Modell-Training:** Es besteht eine technisch-vertragliche Garantie, dass weder Kunden-Prompts noch generierte Antworten zum Training oder zur Verbesserung der Basis-Modelle (Foundation Models) von AWS oder Drittanbietern verwendet werden.
    - **Datenhaltung:** Eingabedaten werden von Amazon Bedrock nicht dauerhaft gespeichert, sondern lediglich für die Dauer der Inferenz (Verarbeitung) im flüchtigen Speicher gehalten.

1.5 Auftragskontrolle

- **AWS:** Die Daten werden physisch in Europa gespeichert und nicht an Drittländer übertragen.
- **Datenschutzbeauftragter:** Alle eingesetzten Dienstleister haben einen Datenschutzbeauftragten bestellt und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.

1.6 Pseudonymisierung

- **Pseudonymisierung**: Sobald Daten vom Server heruntergeladen und lokal gespeichert werden, wird der Personenbezug der Daten gelöscht und die Daten pseudonymisiert.
- **Datenbankverschlüsselung**: Die Datenbank wird “at-rest” verschlüsselt.

- **AWS**: Zusätzlich zu den genannten Punkten, werden die Daten bei AWS EU mittels sog. “Customer Managed Keys” (AES-256, gespeichert in einem FIPS-140-2 HSM) auf dem Transportweg sowie im Ruhezustand verschlüsselt. Mitarbeiter von AWS EU haben somit keinen Zugriff auf das kryptographische Material und sind damit nicht in der Lage, die gespeicherten Daten zu entschlüsseln.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Schutz der Daten bei der elektronischen Übertragung oder beim Transport:

13. **Transportverschlüsselung:** Sämtliche Kommunikation erfolgt über TLS 1.2 oder höher. Zugriffe auf Server sind nur mittels VPN möglich.
14. **Encryption-at-rest:** Einsatz von AES-256 Verschlüsselung. Bei Nutzung von Amazon Bedrock werden Daten (z. B. temporäre Caches) mit AWS KMS Schlüsseln verschlüsselt, die unter der direkten Kontrolle des Auftragsverarbeiters stehen.

2.2 Eingabekontrolle

Feststellung, ob und von wem Daten eingegeben, verändert oder entfernt wurden:

- **Protokollierung:** Revisionssichere Protokollierung zur Fehlerbeseitigung aller administrativen Aktionen über zentrale Logging-Systeme.
- **Personenbezogene Daten**: Die Eingabe, Änderung, Löschung sowie Übertragungen von personenbezogenen Daten werden gesondert protokolliert.

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

3.1 Verfügbarkeitskontrolle & Wiederherstellbarkeit

- **Backup-Konzept:** Tägliche automatisierte Snapshots mit Multi-Availability-Zone-Strategie über 30 Tage.
- **Disaster Recovery:** Zielwert für die Wiederherstellung (RTO) von maximal einem halben Arbeitstag.
- **Redundanz:** Strikte redundante Auslegung kritischer Komponenten (z.B. Speicher, Switches, Firewalls, Load Balancer, Internetanbindung, Stromversorgung, Klimatisierung), USV-Anlagen und redundante Netzwerkanbindungen in allen genutzten Rechenzentren (AWS & DGi).
- **Software:** Der aktuelle Stand der Softwareentwicklung ist über vollständige sowie inkrementelle Backups (offsite) sowie durch ein Versionskontrollsystem gesichert.

3.2 Löschkonzept

- Anweisung: Der Auftragnehmer löscht nur Daten, wenn eine entsprechende Anweisung des Auftraggebers vorliegt

- Backup: Die Backup-Daten werden für einen begrenzten Zeitraum vorgehalten und dann durch entsprechende automatisierte Routinen gelöscht.
- Personenbezogene Daten: Der Auftragnehmer hat ein Löschkonzept erstellt, in dem die Maßnahmen für das richtige Löschen der personenbezogenen Daten beschrieben sind.

4. Verfahren zur regelmäßigen Überprüfung und Bewertung

4.1 Datenschutz-Management & Incident Response

- **Datenschutzbeauftragter:** Ein externer DSB ist bestellt.
- Datenschutzmanagement: Es wird ein Verzeichnis über Verarbeitungstätigkeiten geführt und, wenn nötig, Datenschutzfolgeabschätzungen durchgeführt. Schulungs- und Sensibilisierungsmaßnahmen werden in regelmäßigen Abständen durchgeführt.
- **Incident Management:** Definierte Prozesse zur Erkennung und Behebung von Sicherheitsvorfällen. Ein Reflexionsprozess (“Post Mortem”) ist etabliert.
- **Datenschutzfreundliche Voreinstellungen:** Prozess zur Sicherstellung von “Privacy by Design” sowie "Privacy by Default" bei Änderungen wird eingehalten.

4.2 KI-Governance

- **Bedrock Guardrails:** Einsatz automatisierter Filter zur Erkennung und Maskierung von personenbezogenen Daten (PII), um zu verhindern, dass sensible Informationen unbeabsichtigt von Frontier-Modellen verarbeitet werden.
- **Human-in-the-loop:** Menschliche Überprüfung von KI-generierten Entwürfen vor der finalen Verwendung oder Veröffentlichung.
- **Transparenz:** Information der Nutzer über die Interaktion mit KI-Systemen.

talents connect

Anlage 3

Unterauftragnehmer

Der Auftragnehmer setzt zum Zeitpunkt des Abschluss des AVV folgende Unterauftragnehmer ein und hat im Falle von Drittland-Transfers die nachfolgend beschriebenen Schutzmaßnahmen implementiert:

Name des Unterauftragnehmers	**Adresse**	**Zweck der Verarbeitung**	**Ort der Verarbeitung**	**Schutzmaßnahmen im Fall von Drittland-Transfers**	**Weitere Schutzmaßnahmen zur Absicherung der Datenübertragung**
Gilt für alle Produkte					
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855, Luxemburg	Server, Hosting	EU	EU-U.S. Data Privacy Framework Zertifizierung; EU-Standardvertragsklauseln ((EU) 2021/915, 4.6.2021, Module 2)	AWS ist Träger einer Vielzahl international anerkannter Zertifizierungen und Akkreditierungen. Die Compliance wird mit strengen Standards wie ISO 27017 für Cloud-Sicherheit, ISO 27701 für Datenschutzmanagement und ISO 27018 für Cloud-Datenschutz gewährleistet. **Verschlüsselung:** Daten werden während des Transports sowie während der Speicherung in der Cloud gemäß Stand der Technik (AES-256, FIPS 140/2) mit einem durch talentsconnect verwalteten Schlüssel verschlüsselt, bevor diese AWS-Server erreichen.
Google Ireland Ltd. - Workspace	Gordon House Barrow Street	Zurverfügungstellung einer E-Mail-Server-Infrastruktur	EU	EU-U.S. Data Privacy Framework Zertifizierung	**Verschlüsselung**

	Dublin 4 Ireland	zur Kundenkommunikation im Supportfall			Alle Daten werden bei der Übertragung (*data in transit*) und im Ruhezustand (*data at rest*) verschlüsselt. *Data in transit* Verschlüsselung: Google erzwingt standardmäßig die Verschlüsselung bei der Übertragung, indem es FIPS 140-2-validierte kryptografische Module zur Verschlüsselung des gesamten Datenverkehrs zwischen den Regionen verwendet. Application Layer Transport Security (ALTS) von Google ist ein von Google entwickeltes System zur gegenseitigen Authentifizierung und Transportverschlüsselung, das zur Sicherung der Remote Procedure Call (RPC)-Kommunikation innerhalb der Google-Infrastruktur verwendet wird. ALTS ist vom Konzept her ähnlich wie TLS mit gegenseitiger Authentifizierung, wurde jedoch für die Anforderungen der Rechenzentrumsumgebungen von Google entwickelt und optimiert. *Data at rest* Verschlüsselung:

					Wenn Daten im Ruhezustand gespeichert werden, wendet Google standardmäßig auf der Speicherebene eine Verschlüsselung mit AES256 an Wenn Daten im Ruhezustand gespeichert werden, wendet Google standardmäßig auf der Speicherebene eine Verschlüsselung mit AES256 an.
KeyCDN - proinity LLC	Reichenauweg 1, 8272 Ermatingen, Schweiz	Content Delivery Network, Bereitstellung von Medieninhalten	EU	Angemessenheitsbeschluss der Europäischen Kommission	Wir haben bei dem Anbieter die Verteilung der Inhalte auf Server innerhalb der EU beschränkt. Es werden umfangreiche Sicherheitsmaßnahmen getroffen, wie TLS-Verschlüsselung, DDoS-Protection.
Kombo Technologies GmbH	Lohmühlenstraße 65 12435 Berlin, Deutschland	Integration und Betrieb der Schnittstelle zwischen der Fast Application und dem Bewerbermanagementsystem des Auftraggebers	EU		Die Kombo Technologies GmbH ist nach ISO27001 zertifiziert. Weitere Informationen zu technischen und organisatorischen Sicherheitsmaßnahmen: security.kombo.dev. **Encryption-at-rest:** AES-256-Verschlüsselung **Encryption-in-transit:** Der gesamte ausgehende Datenverkehr verwendet die höchste TLS-Version, die in der API der jeweiligen Integration verfügbar ist. Der gesamte eingehende Verkehr über die

					Kombo-API wird zwingend mit TLS 1.3 abgewickelt.
Gilt nur für JobShop					
Dembach Goo Informatik GmbH & Co. KG	Hohenzollernring 72, 50672 Köln, Deutschland	Server, Hosting (Wird in der Übergangszeit bis zur vollständigen Umstellung auf AWS noch verwendet)	Deutschland Serverstandorte siehe Anlage 2 (TOMs): DUS1, DUS5 und FAL		
Amplitude, Inc.	201 3rd Street, Suite 200, San Francisco, CA 94103	Web-Analyse	EU	EU-U.S. Data Privacy Framework Zertifizierung; EU-Standardvertragsklauseln ((EU) 2021/915, 4.6.2021, Module 2)	**Verschlüsselung**: Amplitude unterhält eine sichere Umgebung für die Übertragung der persönlichen Daten seiner Kunden, Verschlüsselung, die den Industriestandards entspricht, wie z.B. den Federal Information Processing Standards FIPS 140-2 und/oder NIST SP800-52 und unter Verwendung branchenüblicher Verschlüsselungstechnologien wie z.B. Serverzertifikat-basierte Authentifizierung innerhalb der Amplitude Umgebung. Amplitude unterhält eine sichere Umgebung für die Speicherung der persönlichen Daten seiner Kunden, Verschlüsselung, die dem Industriestandard entspricht, wie zum Beispiel den Federal Information Processing Standards FIPS 140-2 und/oder NIST

					SP800-52 und Daten im Ruhezustand mit AES-256.
MailJet (Global HQ)	13-13 bis, rue de l'Aubrac, 75012 Paris, France	Transaktionsmails	EU		
Gilt nur für ChatAgent und WebChat					
360dialog GmbH	Torstraße 61 D-10119 Berlin René Rautenberg +49 89 55294870 info@er-secure.de	Zugang zur WhatsApp Business API	EU		
Nur bei Nutzung der automatisierten Übersetzung: DeepL SE	Maarweg 165 D-50825 Köln Dr. Christian Lenz +49 2261 81950 datenschutz@dhgp.de	Übersetzung von Messages	EU		
Nur bei Nutzung der p78 Schnittstelle zu SAP SuccessFactors: Projekt0708 GmbH	Leopoldstraße 37 a D-80802 München Katja Hauser +49 40790 2350 datenschutz@projekt0708.com	Übertragung von Bewerberdaten in das SAP SuccessFactors-System des Auftraggebers			
Multiposting-Tool: Wenn gewünscht					
VONQ B.V.	Beursplein 37 (3011 AA), Rotterdam, Niederlande	Job-Advertising/Distribution; Multi-Channel-Posting; technische Bereitstellung von Jobboard-Integrationen. Dafür werden Beschäftigtendaten verarbeitet.	EU/EWR		Die VONQ B.V. ist nach ISO27001 zertifiziert. Weitere Informationen zu technischen und organisatorischen Sicherheitsmaßnahmen: https://hapisupport.vonq.com/hc/en-us/articles/15494642476316-DATA-PROCESSING-ADDENDUM.

Anlage 4

Kontaktdaten

4. Weisungsberechtigte Personen

4.1. Auftraggeber

Name, Titel:

E-Mail:

Telefonnummer:

4.2. Auftragnehmer

Name, Titel: Andreas Buchholz, Managing Director Technology, CISO

E-Mail: andreas.buchholz@talentsconnect.com

Telefonnummer: +49 (0)221 82 00 69 - 0

5. Datenschutzbeauftragte/r

5.1. Auftraggeber

Name, Titel:

E-Mail:

Telefonnummer:

Auftragnehmer

Herr Sebastian Herting, Herting Oberbeck Rechtsanwälte Partnerschaft, Hallerstraße 76, 20146 Hamburg

E-Mail: herting@datenschutzkanzlei.de

Telefonnummer: +49 (0) 40 228 691 140