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:

1. Gegenstand und Zweck der Datenverarbeitung

Gegenstand der Verarbeitung ist die Übermittlung der Bewerbungsdaten der Bewerber über die Fast Application an das Bewerbungsmanagementsystem des Auftraggebers. Dabei erfolgt eine Zwischenspeicherung der Bewerbungen auf den Servern von talentsconnect. Im Falle einer Bewerbung über WhatsApp werden Bewerbungen aus der WhatsApp Business API an das Bewerbungsmanagementsystem des Auftraggebers geschickt. Die Verarbeitung der Mitarbeiterdaten des Auftraggebers im Recruiting Home ist ebenfalls Gegenstand der Auftragsverarbeitung. Zweck der Datenverarbeitungen ist die Erbringung der Dienste Fast Application und Recruiting Home.

2. Kategorien betroffener Personen

a. Bewerber, Interessenten
b. Im Rahmen des Recruiting Home: betriebliche Nutzer/Mitarbeiter

3. Kategorien personenbezogener Daten

- Stammdaten (Name, Adresse, Kontaktdaten einschl. E-Mail)
- Interessen, Kommunikationsdaten
- Bewerbungsdaten (Lebenslauf, Zeugnisse, Präferenzen, Bildnis, etc.)
- Im Rahmen des Recruiting Home: Nutzer-/Mitarbeiterdaten (Zugangsdaten)

Anlage 2

Technische und organisatorische Maßnahmen

Terminologie

Dieses Dokument verwendet die Terminologie und die Definitionen gemäß der Datenschutz-Grundverordnung (im folgenden „DSGVO“ bezeichnet). Darüber hinaus bezeichnet

- „Auftragnehmer“ den Auftragsverarbeiter gemäß den Angaben oben in diesem Dokument;
- „Auftraggeber“ den Verantwortlichen gemäß DSGVO, der mit dem Auftragsverarbeiter einen Vertrag zur Auftragsverarbeitung vereinbart hat.
- „Software“, “JobShop” bzw. "talentsconnect" die SaaS-Lösung, die der Auftragnehmer zur Nutzung für den Auftraggeber bereitstellt, um die Verarbeitung der Daten durchzuführen.

Zur Absicherung der Daten des Auftraggebers werden folgende technischen und organisatorischen Maßnahmen für die Systeme des Auftragnehmers verbindlich festgelegt:

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

Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.	Rechenzentren (RZ) Die Datenverarbeitungssysteme, mit denen die personenbezogenen Daten des Kunden verarbeitet werden, werden von zwei Anbietern betrieben, Dembach Goo Informatik GmbH & Co. KG und Amazon Web Services EMEA SARL. Dembach Goo Informatik GmbH & Co. KG bietet umfassende Sicherheitskonzepte für das Hosting der Produkte. Die Server der talentsconnect-Produkte (betrieben von der talentsconnect AG) werden daher ausschließlich in entsprechend zugangsgesicherten Rechenzentrumsräumen an verschiedenen Standorten in Deutschland betrieben. Folgende technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten, werden an den RZ-Standorten von Dembach Goo Informatik GmbH & Co. KG eingesetzt. Standort DUS1 ● Zugang zu den RZ-Flächen mit persönlicher Chipkarte mit PIN, Handscanner, Serverschränke befinden sich innerhalb des RZ in einer „Private Suite“ (gesondert geschützte Stahlwandumbauung), deren Türen PIN-Code gesichert sind. ● PIN-Code gesicherter Schlüsselkasten innerhalb der Private Suite.

	• Zentrale Videoüberwachung und -aufzeichnung durch den örtlichen RZ-Betreiber. • Externe Personen (z. B. Service-Techniker) haben nur in ständiger Begleitung einer autorisierten Person Zugang zu RZ-Flächen und Server-Schränken. Standort DUS5 • Zugang zu den RZ-Flächen mit persönlicher Chipkarte; Wachpersonal gibt an autorisierte Personen (Liste hinterlegt, Prüfung des Personalausweises) ggf. Zugangskarte und Schlüssel für Serverschränke aus. Zugang zum RZ-Bereich durch eine Vereinzelungsschleuse mit Handscanner bzw. Freischaltung durch Wachpersonal. • Schlüsselverwahrung durch Wachpersonal. • Zentrale Videoüberwachung und -aufzeichnung durch den örtlichen RZ-Betreiber. • Externe Personen (z. B. Service-Techniker) haben nur in ständiger Begleitung einer autorisierten Person Zugang zu RZ-Flächen und Server-Schränken. Standort FAL • Elektronisches Zutrittskontrollsystem mit Protokollierung • Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden • Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude • 24/7 personelle Besetzung der Rechenzentren • Videoüberwachung an den Ein- und Ausgängen Detaillierte Informationen zu den Zutrittskontrollen kann der Auftraggeber bei Dembach Goo Informatik GmbH & Co. KG erfragen. Die Datenverarbeitungssysteme, mit denen die personenbezogenen Daten des Kunden verarbeitet werden, werden von Amazon Web Services EMEA SARL (nachfolgend AWS oder AWS EU genannt) betrieben. AWS EU • Das primäre Rechenzentrum befindet sich in Frankfurt am Main, es können aber auch andere europäische Rechenzentren des Anbieters zu Ausfallsicherungszwecken genutzt werden. • Das genutzte Rechenzentrum von AWS erfüllt EU adäquate Standard- und Datenschutzbedingungen. Unter anderem die DIN ISO/IEC 27001 und 27018 Zertifizierung und ermöglicht Zutritt nur für autorisiertes Fachpersonal des Rechenzentrums. • Der Zugang zur Datenverarbeitungsanlage ist durch das Rechenzentrum von AWS geregelt. Weitere Informationen zu den Sicherheitsprozessen des AWS Rechenzentrums finden Sie hier:

	○ Data Center - Our Data Centers ○ Data Center - Our Controls talentsconnect AG – Verwaltung ● Zutritt zu den Büro-Flächen mit persönlichem Dongle. ● Serverschränke befinden sich innerhalb des Büros in einem abgeschlossenen Bereich, deren Türen Dongle gesichert sind. ● Die personenbezogenen Daten des Auftraggebers werden auf den oben genannten Servern im Rechenzentrum der Hosting Anbieters verarbeitet. In den Büroräumen des Auftragnehmers werden die personenbezogenen Daten nicht dauerhaft gespeichert oder verarbeitet. Der Zugriff auf die personenbezogenen Daten erfolgt über die Arbeitsplatzrechner des Auftragnehmers. ● Die Ausgabe und Rücknahme von Dongles erfolgt durch die Abteilung HR.
Zugangskontrolle Keine unbefugte Systembenutzung.	**Rechenzentren (RZ)** Folgende technische bzw. organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, werden an den Standorten DUS1, DUS5 sowie FAL eingesetzt. ● Für jeden Benutzer des Systems ist ein eigener Benutzerstammsatz („Account“) erforderlich. Die Authentifizierung erfolgt über den Benutzernamen und ein nur dem Benutzer vollständig bekanntes Passwort. ● Beim Anlegeverfahren in der Benutzerverwaltung werden Verfahren zur Erstellung sicherer Kennwörter eingesetzt (z. B. Erzwingen von Sonderzeichen und Mindestlänge). ● Ein regelmäßiger Wechsel des Kennworts wird nicht erzwungen, wird aber für jeden Benutzer über eine bereitgestellte Maske ermöglicht. ● Für alle Zugriffswege auf das System werden verschlüsselte Datenprotokolle angeboten; eine Authentifizierung der Serverdienste ist für jeden Benutzer durch den Einsatz serverseitiger Zertifikate möglich. ● Administratoren unseres Dienstleisters (DUS1 und DUS5) erhalten nur über besonders geschützte Zugänge (VPN, Mitgliedschaft in der Administrator-Gruppe und Besitz eines individuellen privaten Schlüssels) Zugriff auf die Konsolen der Serversysteme. ● Dem RZ-Betreiber (FAL) sind Passwörter, welche nur von der talentsconnect AG nach erstmaliger Inbetriebnahme selbst geändert wurden nicht bekannt. ● Der Zugang auf die einzelnen Maschinen (FAL) ist nur über eine Keyauthentifizierung möglich. Folgende technische bzw. organisatorische Maßnahmen

	hinsichtlich der Benutzeridentifikation und Authentifizierung, werden an den AWS-Standorten eingesetzt. ● Für jeden Benutzer des Systems ist ein eigener Benutzerstammsatz („Account“) erforderlich. Die Authentifizierung erfolgt über den Benutzernamen und ein nur dem Benutzer vollständig bekanntes Passwort. ● Beim Anlegeverfahren in der Benutzerverwaltung werden Verfahren zur Erstellung sicherer Kennwörter eingesetzt (z. B. Erzwingen von Sonderzeichen und Mindestlänge). ● Für alle Zugriffswege auf das System werden verschlüsselte Datenprotokolle angeboten; eine Authentifizierung der Serverdienste ist für jeden Benutzer durch den Einsatz serverseitiger Zertifikate möglich. ● Für das AWS-Rechenzentrum gilt, dass auch dort alle Berechtigungen nach dem Prinzip der Minimalberechtigung erteilt und Berechtigungen regelmäßig überprüft werden. Die Vergabe und der Entzug von Berechtigungen wird protokolliert. Die Verwendung von Passwörtern ist ebenfalls geregelt und sieht die Verwendung von komplexen Passwörtern, einen Passwortwechsel nach spätestens 90 Tagen sowie eine Passworthistorie vor. **talentsconnect AG – Verwaltung** ● Passwörter, welche nur vom Mitarbeiter nach erstmaliger Inbetriebnahme von ihm selbst geändert werden. ● Auf die Systeme des Hosting-Anbieters kann darüber hinaus auch nur unter Kenntnis des Benutzernamens und Passwortes sowie einer aktiven VPN Verbindung zum Hosting-Anbieter zugegriffen werden. ● Abteilungs- bzw. positionsabhängige Zuordnung von Benutzerrechten. ● Einsatz einer Hardware-Firewall. ● Einsatz von VPN Technologie. ● Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet. **JobShop** ● Je nach Auftragsbeschreibung mit dem Auftraggeber, ist es möglich die "Merken"-Funktion, sowie die FastTrack Application zu nutzen, durch die personenbezogene Daten an den Auftraggeber übermittelt werden. Die Daten werden während der Übertragung verschlüsselt. Welche Daten übergeben werden, ist der Auftragsbeschreibung des Auftraggebers dokumentiert. ● Der Zugang zu einem Personaler-Account erfolgt jeweils durch Abfrage der Zugangsdaten bestehend aus E-Mail und einem eindeutigen, ausschließlich dem Personaler

	bekannten, Passwort.
	Rechenzentren (RZ) <u>Standort DUS1 und DUS5:</u> ● Zum einen müssen Benutzer mit Systemadministrator-Rechten auf den Servern im betriebenen Verzeichnisdienst angelegt werden. Benutzer sind stets eindeutig einer Verwaltungsdomäne zugeordnet, die wiederum nur von Administratoren seitens unseres technischen Dienstleisters verändert werden kann. Einzelne Benutzer einer Verwaltungsdomäne können als deren Verwalter ausgezeichnet werden. Der Verwalter einer Verwaltungsdomäne kann Benutzer anlegen, löschen und sperren und Kennwörter zurücksetzen. Die Aktionen des Verwalters werden protokolliert und sind für 30 Tage nachvollziehbar. ● Ein Passwort-Reset wird entweder durch den Benutzer selbst oder den Verwalter ausgelöst. Bei dem Reset wird dem Benutzer die erste Hälfte des Passworts per E-Mail und die zweite Hälfte an eine vorher definierte Mobilfunknummer per SMS verschickt. <u>Standort FAL:</u> ● Der Zugang auf die einzelnen Maschinen (FAL) ist nur über eine Keyauthentifizierung über verschlüsselte Wege möglich. ● Angebotene Services, soweit datenschutzrechtlich relevant, sind zusätzlich durch Benutzername und Passwort geschützt. <u>AWS EU:</u> ● Der Zugriff auf die AWS IT-Infrastruktur erfolgt via verschlüsselte SSH- und VPN-Verbindung und ist ausschließlich Mitarbeitern des Auftragsverarbeiters vorbehalten. ● Der Zugriff auf den Server erfolgt über eine passwortgeschützte private Schlüsseldatei (Private Key File). ● Die zuständigen Mitarbeiter des Auftragsverarbeiters erhalten jeweils einen eigenen Key. ● Der Zugriff auf Daten und Dienste der AWS IT-Infrastruktur wird über eine differenzierte Zugriffsregelung, basierend auf Gruppen, geregelt. ● Zwei-Faktor-Authentifizierung (2FA), Anmeldeprozess (Authentifikation) mit Benutzerkennung und Passwort plus dynamisch erzeugten Einmal-Code der bspw. per SMS

	verschickt wird. **talentsconnect AG – Verwaltung** ● Verwaltung der Rechte durch Systemadministrator sowie Security Owner. ● Die Anzahl der Administratoren ist auf das „Notwendigste“ reduziert. ● Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten. ● Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet. **JobShop** ● Je nach Auftragsbeschreibung mit dem Auftraggeber, ist es möglich, dass dem Kunde ein Zugang eingerichtet wird. Die Rechte für Personaler werden zentral durch die Mitarbeiter der talentsconnect AG verwaltet. ● Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.	**Rechenzentren (RZ)** <u>Standort DUS1 und DUS5:</u> ● Das verwendete System, wird in einem Serververbund für mehrere Kunden gemeinsam betrieben. Das System ist mandantenfähig, das heißt, die Daten des Kunden sind von Daten anderer Personen logisch getrennt. Benutzer und deren Daten sind dabei immer eindeutig einem Mandanten zugeordnet. Ein interner Austausch oder gemeinsame Nutzung von Benutzern/Daten zwischen Mandanten ist nicht möglich. <u>Standort FAL:</u> ● Die Datentrennung erfolgt durch physikalische und logische Trennung. <u>AWS EU:</u> ● Die Datentrennung erfolgt durch physikalische und logische Trennung. Auf dem vom Auftraggeber genutzten Systemen werden keine Daten anderer Kunden des Auftragnehmers verarbeitet.

	talentsconnect AG – Verwaltung ● Berechtigungskonzept **JobShop** Der Auftragnehmer führt in der Regel keine Änderungen an den personenbezogenen Daten des Auftraggebers durch. Der Auftragnehmer stellt dem Auftraggeber mit der Software Funktionalitäten zur Verfügung. ● Berechtigungskonzept ● Festlegung von Datenbankrechten ● Logische Mandantentrennung (datenbankseitig): Eine Einsichtnahme von Benutzern anderer Nutzerkreise ist aufgrund der Architektur nicht möglich und wurde während der Programmierung der Software sichergestellt. ● Trennung von Produktiv- und Testsystem
Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.	**Rechenzentren (RZ)** Der Hosting Anbieter führt keine Änderungen an den personenbezogenen Daten des Auftraggebers durch, sondern stellt lediglich die Infrastruktur für den technischen Betrieb der Server zur Verfügung. <u>Standort DUS1 und DUS5:</u> ● Im Regelbetrieb (keine Störung am System) greift der Dienstleister nicht auf Systeme zu. Die Behebung von Störungen kann dies erforderlich machen. Störungen werden den Betriebsmitarbeitern durch Zuweisung eines Tickets in einem Trouble-Ticket-System angezeigt. Tickets können per E-Mail oder Telefon auch vom talentsconnect AG erstellt werden. Im Ticket werden die ausgeführten Aktionen und Problemlösungen festgehalten. ● Der Rechenzentrumsbetreiber hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betriebliche Prozesse. <u>Standort FAL:</u> ● Mitarbeiter des RZ Betreibers werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des

	Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers. ● Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers. ● Der Rechenzentrumsbetreiber hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betriebliche Prozesse. <u>AWS EU:</u> ● Allgemeine Geschäftsbedingungen & Vereinbarung zur Auftragsverarbeitung. ● Die Daten werden physisch in Europe gespeichert und nicht in Drittländer übertragen. ● AWS hat sich dem Auftragsverarbeiter gegenüber innerhalb einer Datenverarbeitungsvereinbarung zur Wahrung von Datenschutzstandards nach EU-Recht verpflichtet. ● Diese Verpflichtung unterliegt allerdings der Geheimhaltung. ● Die Rechte an den gehaltenen Daten liegen beim Auftragsverarbeiter und nicht bei AWS. **talentsconnect AG – Verwaltung** ● Die Auswahl der Auftragnehmer erfolgt unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit). ● Die talentsconnect AG hat einen Datenschutzbeauftragten bestellt. ● Vorherige Prüfung und Dokumentation der bei der talentsconnect AG getroffenen Sicherheitsmaßnahmen. ● Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet. **JobShop** ● Die Mitarbeiter der talentsconnect AG dokumentieren die gebuchten Leistungen der Kunden im CRM-System und stellen im laufenden Betrieb sicher, dass genau diese erbracht werden.
Pseudonymisierung	**JobShop**

(Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) *Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern* *diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.*	Pseudonymisierung ● Sobald Daten vom Server heruntergeladen und lokal gespeichert werden, wird der Personenbezug der Daten gelöscht und die Daten pseudoymisiert. Verschlüsselung auf den Systemen des Auftragnehmers ● Die persönlichen Daten werden in der Datenbank der Software in Klartext gespeichert mit Ausnahme des Passwortes. Das Passwort wird nur verschlüsselt gespeichert ohne die Möglichkeit, das ursprüngliche Passwort zu berechnen. Somit ist es auch dem Auftragnehmer nicht möglich, die Passwörter einzusehen. Der Auftragnehmer sieht das als zwingende Notwendigkeit an, da zum einen die Kenntnis über das Passwort für den Betrieb und die Verfügbarkeit der Software nicht notwendig ist, zum anderen manche Nutzer das gleiche Passwort für verschiedene Internetdienste nutzen. Neben der Datenbank werden die Daten in einem Backup gespeichert. Auch dort bleibt die Verschlüsselung des Passwortes erhalten. Das Backup wird auf einem gesicherten Backup-Server gespeichert, auf das ohne Kenntnis des Benutzers und Passworts kein Zugriff möglich ist. ● Die Datenbank wird “at-rest” verschlüsselt. ● Der für den Zugriff erforderliche Benutzername und das Passwort sind lediglich den befugten Mitarbeitern des Auftragnehmers bekannt. ● Die Mitarbeiter wurden zur Vertraulichkeit verpflichtet. Zusätzliche Verschlüsselung auf den Systemen von AWS EU ● Zusätzlich zu den oben 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 keinen Zugriff auf das kryptographische Material und sind somit nicht in der Lage, die gespeicherten Daten zu entschlüsseln. Verschlüsselung bei der Kommunikation der beteiligten Systeme bei Verwendung der Software ● Bei der Verwendung der Software sind die Internet-Browser des Auftraggebers, der Server der Software, und die Arbeitsplatzrechner oder Endgeräten der Mitarbeiter des Auftragnehmers beteiligt, zusammen mit den Systemen, die den Transport der Informationen über das Internet gewährleisten. Damit die Daten nicht von dritten beteiligten Systemen außer den Systemen des

	Auftragnehmers und des Auftraggebers ausgelesen werden können, und die Informationen fälschungssicher zugestellt werden, stellt der Auftragnehmer sicher, dass die Software sämtliche Kommunikation per SSL/TLS (Secure Socket Layer / Transport Layer Security) verschlüsselt. Sollte eines der genannten Systeme des Auftraggebers eine ungesicherte Verbindung aufbauen wollen, wird die Software die Anfrage mit einem Verweis auf Verwendung einer gesicherten Verbindung quittieren, ohne dabei persönliche Daten zu übermitteln. Die Antwort mit Verweis auf die gesicherte Verbindung ist dabei so gestaltet, dass das anfragende System die Möglichkeit hat, automatisch auf die gesicherte Verbindung zu wechseln und die Anfrage zu wiederholen. Verschlüsselung bei der Kommunikation per elektronischer Email oder Schnittstelle ● Je nach Auftragsbeschreibung mit dem Auftraggeber, ist es möglich die personenbezogene Daten an den Auftraggeber zu übermitteln. Die Daten werden während der Übertragung verschlüsselt. Welche Daten übergeben werden, ist den Auftragsbeschreibung des Auftraggebers dokumentiert. JobShop ● Je nach Auftragsbeschreibung mit dem Auftraggeber, ist es möglich die "Merken"-Funktion, sowie die FastTrack Application zu nutzen, durch die personenbezogene Daten an den Auftraggeber übermittelt werden. Die Daten werden während der Übertragung verschlüsselt. Welche Daten übergeben werden, ist der Auftragsbeschreibung des Auftraggebers dokumentiert.

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

Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.	**Rechenzentren (RZ)** ● Interner Datentransport findet ausschließlich über Datenverbindungen unter Kontrolle des Dienstleisters statt (eigene Leitungen oder VPN). Das gilt insbesondere auch für Datenbackups. ● Alle Mitarbeiter haben sich auf die Vertraulichkeit der Daten verpflichtet. ● Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung. **talentsconnect AG – Verwaltung**

	• Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet. • Der Zugriff zwischen den Arbeitsplatzrechnern des Auftragnehmers und den Systemen, auf dem die Software betrieben wird und dem Backup-Server erfolgt stets über SSL gesicherte Kommunikation. • Nutzung von VPN-Tunneln und verschlüsselten Verbindungen wie bspw. HTTPS. • Einsatz von Aktenvernichtern. **JobShop** • Weitergabe der Daten an den Auftraggeber gemäß Auftragsbeschreibung. • Die für die Verarbeitung der vom Auftraggeber bereitgestellten Daten zuständige Software ist über das Internet erreichbar. Die Software stellt dabei sicher, dass die Kommunikation stets über eine SSL gesicherte Verbindung mit aktuellen Sicherheitsstandards erfolgt.
Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	**Rechenzentren (RZ)** Folgende Administratorenaktionen sind durch nachträgliche Logfile-Auswertungen prüfbar: • Anmeldung am System • Benutzerverwaltung: Anlegen, Verändern und Löschen von Benutzern (Uhrzeit, ausführender Benutzer, veränderter Benutzer) **talentsconnect AG – Verwaltung** • Protokollierung der Eingabe, Änderung und Löschung von Daten. • Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts. • Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. **JobShop** • Logdateien werden zur Fehlerbeseitigung und zum Nachweis der ordnungsgemäßen Leistungserbringung verwendet und ansonsten nicht weiter ausgewertet. • Die Eingabe, Änderung und Löschung von personenbezogenen Daten wird protokolliert

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

Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.	**Rechenzentren (RZ)** Folgende technische bzw. organisatorische Maßnahmen zur Verfügbarkeitskontrolle, werden an den RZ-Standorten von Dembach Goo Informatik GmbH & Co. KG eingesetzt. <u>Standort DUS1 und DUS5:</u> ● Backup-Verfahren (tägliche Gesamtsicherung der EMail-Datenbanken zur Disaster Recovery). Vorhalten von mindestens zwei Versionen über 30 Tage, Spiegelung der Backup-Daten über zwei Standorte, zusätzliche Sicherung einer Kopie auf Band. ● Spiegelung der Datenspeichersysteme über zwei Standorte, Einsatz von RAID ● Redundante, unterbrechungsfreie Stromversorgung (USV); Dieselgenerator ● Strikt redundante Auslegung aller zur Serviceerbringung benötigter Komponenten (Server, Speicher, Switches, Firewalls, Load-Balancer, Internet-Anbindung, Stromversorgung, Klimatisierung) ● Verteilung wichtiger Komponenten über zwei gekoppelte RZ-Standorte **Standort FAL:** ● Verschlüsseltes off-site Backup durch talentsconnect AG ● Sicherung des laufenden Betriebs durch Festplatten im RAID-Verbund ● Einsatz unterbrechungsfreier Stromversorgung. **AWS EU:** ● Backups zur Disaster Recovery sowie Just-In-Time Snapshot für Datenbanken ● Redundante, unterbrechungsfreie Stromversorgung ● Überwachung von Temperatur und Feuchtigkeitsparameter ● Verteilung von wichtigen Systemkomponenten über mehrere Standorte (Availability Zones) ● Weitere Informationen zu den Sicherheitsprozessen des AWS Rechenzentrums finden Sie hier: ○ Data Center - Our Data Centers ○ Data Center - Our Controls **talentsconnect AG – Verwaltung**

	• Unterbrechungsfreie Stromversorgung (USV). • Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen. • Feuer- und Rauchmeldeanlagen. • Klimaanlage in Serverräumen. • Backup- & Recoverykonzept. **JobShop** • Die Produkte werden ausschließlich in den Rechenzentren betrieben. Entsprechend gelten die o.g. Rahmenbedingungen. • Der aktuelle Stand der Softwareentwicklung ist über vollständiges und inkrementelles Backup (offsite) sowie durch die verwendete Software zur Versionskontrolle gesichert. Es ist jederzeit möglich den aktuellen oder auch einen “last known good” Zustand der Produkte wiederherzustellen.
Wiederherstellbarkeit Wiederherstellung bei einem bei einem physischen oder technischen Zwischenfall	**Rechenzentren (RZ)** Folgende technische bzw. organisatorische Maßnahmen zur Wiederherstellbarkeit, werden an den RZ-Standorten von Dembach Goo Informatik GmbH & Co. KG eingesetzt. <u>Standort DUS1 und DUS5:</u> • Backup-Verfahren (tägliche Gesamtsicherung der EMail-Datenbanken zur Disaster Recovery). Vorhalten von mindestens zwei Versionen über 30 Tage, Spiegelung der Backup-Daten über zwei Standorte, zusätzliche Sicherung einer Kopie auf Band. • Spiegelung der Datenspeichersysteme über zwei Standorte, Einsatz von RAID • Redundante, unterbrechungsfreie Stromversorgung (USV); Dieselgenerator • Strikt redundante Auslegung aller zur Serviceerbringung benötigter Komponenten (Server, Speicher, Switches, Firewalls, Load-Balancer, Internet-Anbindung, Stromversorgung, Klimatisierung) • Verteilung wichtiger Komponenten über zwei gekoppelte RZ-Standorte <u>Standort FAL:</u> • Verschlüsseltes off-site Backup durch talentsconnect AG • Sicherung des laufenden Betriebs durch Festplatten im RAID-Verbund • Einsatz unterbrechungsfreier Stromversorgung. <u>AWS EU:</u>

	● Backups zur Disaster Recovery sowie Just-In-Time Snapshot für Datenbanken ● Redundante, unterbrechungsfreie Stromversorgung ● Überwachung von Temperatur und Feuchtigkeitsparameter ● Verteilung von wichtigen Systemkomponenten über mehrere Standorte (Availability Zones) ● Weitere Informationen zu den Sicherheitsprozessen des AWS Rechenzentrums finden Sie hier: ○ https://aws.amazon.com/compliance/data-center/data-centers/ ○ https://aws.amazon.com/compliance/data-center/controls/ **JobShop** ● Der Auftragnehmer setzt ein technisches Verfahren ein, mit dem der Datenbestand automatisiert und regelmäßig einem von der Laufzeitumgebung physisch und logisch getrennten System (Offsitesicherung) gesichert wird. ● Im Falle eines physischen oder technischen Zwischenfalls auf dem System der Laufzeitumgebung können die Daten aus dem Backup-Server wiederhergestellt werden und dem Auftraggeber wieder zur Verfügung gestellt werden.
Löschkonzept Löschung der richtigen Daten zum richtigen Zeitpunkt	● Daten in der Software werden nur vom Auftraggeber gelöscht. Der Auftragnehmer löscht keine Daten, außer in dem Fall, wenn der Auftraggeber den Auftragnehmer entsprechende Anweisung erteilt. ● Die Backup-Daten werden für einen begrenzten Zeitraum vorgehalten und dann durch entsprechende automatisierte Routinen, deren Funktionalität der Auftragnehmer gewährleisten muss, gelöscht. ● Der Auftragnehmer hat ein Löschkonzept erstellt, in dem die Maßnahmen für das richtige Löschen der personenbezogenen Daten beschrieben sind.

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

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.

Datenschutz-Management	● Die talentsconnect AG hat einen externen Datenschutzbeauftragten bestellt. ● Es wird ein Verzeichnis von Verarbeitungstätigkeiten

	geführt und es werden Datenschutzfolgeabschätzungen durchgeführt. ● Schulungsmaßnahmen bzw. Sensiblisierungsmaßnahmen von allen Mitarbeitern werden in regelmäßigen Abstände durchgeführt. ● Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet. ● Arbeitsanweisungen bzw. Policies mit Datenschutzhintergrund liegen vor.
Incident Response Management	● Zuständigkeiten und Verantwortlichkeiten für Vorfälle sind definiert. ● Maßnahmen für relevant und denkbare Vorfälle sind definiert, sowie vorbereitete Reaktionen auf den Vorfall. ● Um aus Vorfällen zu lernen erfolgt Reflexion und ein Nachbereitungsprozess.
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	● Prozess zur Sicherstellung von Privacy by Design bei Änderungen wird eingehalten. ● Prozess zur Sicherstellung von Privacy by Default bei Änderungen wird eingehalten.

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**
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		
Google Ireland Ltd. - Workspace	Gordon House Barrow Street Dublin 4 Ireland	Zurverfügungstellung einer E-Mail-Server-Infrastruktur zur Kundenkommunikation im Supportfall	EU	EU-U.S. Data Privacy Framework Zertifizierung	**Verschlüsselung** 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.
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		
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.
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.
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.
PitchYou GmbH	Campusallee 9, D-51379 Leverkusen	Technische Implementierung und Abwicklung der Bewerbung über Whatsapp über die WhatsApp Business API, wenn diese Funktion eingebunden ist und vom Bewerber auf Basis einer Einwilligung genutzt wird.	Deutschland		
Chat-Tool: Wenn gewünscht					
Userlike UG (haftungsbeschränkt)	Probsteigasse 44-46, 50670 Köln, Deutschland	Chat	Deutschland		

Anlage 4

Kontaktdaten

1. Weisungsberechtigte Personen

1.1. Auftraggeber

Name, Titel:

E-Mail:

Telefonnummer:

1.2. Auftragnehmer

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

E-Mail: andreas.buchholz@talentsconnect.com

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

2. Datenschutzbeauftragte/r

2.1. 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