

# **Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO**

(der "Vertrag")

## **Präambel**

Die Jobkey GmbH ("Auftragnehmer") erbringt für Unternehmen ("Auftraggeber"), einzeln die "Partei" und beide zusammen die "Parteien", auf der Jobkey-Plattform, die über <https://jobkey.eu> zu erreichen ist, Leistungen im Bereich der Beschaffung und der Verwaltung von externem Personal (z. B. Arbeitnehmerüberlassung) gemäß Zustimmung der Allgemeinen Geschäftsbestimmungen (der "Hauptvertrag"). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung (die "DSGVO"). Zur Erfüllung der Anforderungen der DSGVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

**Dies vorausgeschickt, vereinbaren die Parteien, was folgt:**

## **1. Gegenstand und Umfang der Beauftragung**

- 1.1 Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer und seine Beschäftigten Zugriff auf personenbezogene Daten von Mitarbeitern des Auftraggebers erhält (nachfolgend "Auftraggeberdaten") und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO verarbeitet.
- 1.2 Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag sowie aus der Anlage 1 zu diesem Vertrag. Der Kreis der von der Datenverarbeitung betroffenen Personen und der Datenarten ist in Anlage 2 zu diesem Vertrag dargestellt. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung. Dem Auftragnehmer ist eine abweichende oder über die Festlegungen in Anlage 1 und Anlage 2 hinausgehende Verarbeitung von Auftraggeberdaten untersagt.

- 1.3 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien den vorliegenden Vertrag. Seine Regelungen gehen im Zweifel den Regelungen des Hauptvertrags vor.
- 1.4 Der vorliegende Vertrag wird für den Zeitraum des Bestehens des Hauptvertrages geschlossen.
- 1.5 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

## **2. Weisungsrechte des Auftraggebers**

- 2.1 Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers verarbeiten. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.
- 2.2 Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen insbesondere im Hinblick auf die Berichtigung und Löschung von Daten sowie auf die Einschränkung der Verarbeitung. Die weisungsberechtigten Personen ergeben sich aus Anlage 3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.
- 2.3 Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die im Hauptvertrag vereinbarten Leistungen hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

- 2.4 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.
- 2.5 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

### **3. Schutzmaßnahmen des Auftragnehmers**

- 3.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
- 3.2 Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden ("Mitarbeiter"), in Schriftform zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen.
- 3.3 Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gemäß Art. 32 DSGVO, insbesondere die in Anlage 4 zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrechtzuerhalten.
- 3.4 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß Anlage 4 nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

3.5 Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in Anlage 4 bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen.

#### **4. Informations- und Unterstützungspflichten des Auftragnehmers**

4.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens aber innerhalb von 48 Stunden in Schrift- oder elektronischer Form über

- Störungen bzw. Verdacht auf Datenschutzverletzungen,
- Verletzungen vertraglicher Verpflichtungen des Auftragnehmers,
- Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer.

Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen haben jeweils zumindest die in Art. 33 Abs. 3 DSGVO genannten Angaben zu enthalten.

4.2 Der Auftragnehmer wird den Auftraggeber im vorgenannten Falle bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

4.3 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle gemäß Ziffer 6 Abs. 1 dieses Vertrages erforderlich sind. Ferner wird der Auftragnehmer dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung stellen.

4.4 Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung des Verarbeitungsverzeichnisses nach Art. 30 Abs. 1 DSGVO, bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO

unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen in angemessenem Umfang zu unterstützen. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen. Kosten, die dem Auftragnehmer durch seine Unterstützungshandlungen entstehen, sind ihm im angemessenen Umfang zu erstatten, soweit die Unterstützung nicht wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde.

## **5. Sonstige Pflichten des Auftragnehmers**

- 5.1 Der Auftragnehmer ist verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gemäß Art. 30 Abs. 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.
- 5.2 Der Auftragnehmer bestätigt, dass er, soweit eine gesetzliche Verpflichtung hierzu besteht, einen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten, oder – sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DSGVO bzw. § 38 BDSG bzw. einem Landesdatenschutzgesetz nicht bestellt werden muss – des Ansprechpartners für den Datenschutz beim Auftragnehmer, ist Antonio Zill, Pettenkoflerstr. 33, 80336 München, [info@jobkey.eu](mailto:info@jobkey.eu). Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten bzw. Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.
- 5.3 Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegt.

## **6. Kontrollrechte des Auftraggebers**

- 6.1 Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß Ziffer 3.3 dieses

Vertrages, zu überzeugen. Hierfür wird der Auftragnehmer dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem Dritten, sofern dieser nicht in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer steht, ermöglichen und dazu beitragen.

- 6.2 Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig, mindestens aber vier Wochen im Voraus, sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint.
- 6.3 Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

## **7. Einsatz von Subunternehmern**

- 7.1 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 5 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern ("Subunternehmerverhältnis") befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser nicht innerhalb einer Frist von zwei Wochen widersprochen hat.
- 7.2 Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Bei der Einschaltung von Subunternehmern hat der Auftragnehmer diese entsprechend den Regelungen dieses Vertrages zu verpflichten.
- 7.3 Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist.

7.4 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen Subunternehmerverhältnisse i. S. d. Abs. 1 dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

## **8. Rechte Betroffener**

8.1 Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des Auftraggebers nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO.

8.2 Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

## **9. Laufzeit und Kündigung**

9.1 Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

9.2 Der Auftraggeber ist jederzeit zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO im Rahmen der Auftragsverarbeitung vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will, es sei denn, eine Weisung verletzt Datenschutzbestimmungen. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer

zunächst eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht dem Auftraggeber sodann das Recht zur außerordentlichen Kündigung zu.

## **10. Löschung und Rückgabe nach Vertragsende**

10.1 Der Auftragnehmer wird dem Auftraggeber nach Abschluss der Erbringung der Verarbeitungsleistung oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen.

10.2 Der Auftragnehmer wird dem Auftraggeber die Löschung schriftlich bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig, es sei denn eine Kontrolle ohne vorherige Anmeldung erscheint erforderlich.

10.3 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

## **11. Haftung**

11.1 Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

11.2 Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Der vorstehende Satz gilt im Falle einer gegen eine Partei verhängten Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.



11.3 Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

## **12. Schlussbestimmungen**

12.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

12.2 Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Die digitale Form einer Unterschrift (z. B. Scan als PDF oder DocuSign) genügt.

12.3 Sollten sich einzelne Bestimmungen dieses Vertrages ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

12.4 Dieser Vertrag unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist München, Deutschland.

Stand: November 2024

## **Anlage 1**

### **Art, Umfang und Zweck der Datenverarbeitung**

- 1.1 Gegenstand dieses Auftrages ist der Hauptvertrag.
- 1.2 Umfang, Art (Art. 4 Nr. 2 DSGVO) und Zweck der Datenverarbeitung ist das Erfassen, Speichern, Verändern, Abfragen und Löschen von personenbezogenen Daten für das Management von Arbeitskräften im Rahmen der Arbeitnehmerüberlassung, die über die vom Auftragnehmer bereitgestellte Plattform vermittelt wurden.
- 1.3 Neben der Vermittlung von Mitarbeitern ermöglicht die Plattform die Einsatzplanung und das Management von Mitarbeitern, einschließlich Schichtplanung und Abwesenheitsverwaltung.
- 1.4 Nach Abschluss des Personaleinsatzes bietet die Plattform zudem die Möglichkeit, Feedback zum Einsatz des vermittelten Mitarbeiters zu erfassen.

## Anlage 2

### Beschreibung der Datenarten und der Kategorien betroffener Personen

#### 2.1 Art der Daten

Datenkategorie	Beispiele
Berufliche Kontakt- und (Arbeits-)Organisationsdaten	<ul style="list-style-type: none"> <li>- Vorname, Nachname, Anschrift, Geburtsdatum, E-Mail-Adresse, Mobil-Telefonnummer, Personalnummer</li> <li>- Lebenslauf (im Fall von Zeitarbeitnehmern),</li> <li>- Profilfoto</li> </ul>
Daten zu beruflichen Verhältnissen	<ul style="list-style-type: none"> <li>- Verfügbarkeiten, Schichtzeiten und Schichtinhalte</li> <li>- Abwesenheiten (z. B. Urlaub, Krankheit, Ruhetage)</li> <li>- Einsatzpräferenzen</li> <li>- Qualifikationen</li> <li>- Einsatzbewertung</li> </ul>
Private Kontakt- und Identifikationsdaten	<ul style="list-style-type: none"> <li>- Vorname, Nachname, Anschrift, Geburtsdatum, Geschlecht, Staatsbürgerschaft, Sozialversicherungsnummer, anonymisierte Personalausweiskopie, Identitätsnachweise</li> </ul>
Vertragsdaten	<ul style="list-style-type: none"> <li>- Persönliche Zuordnung von Tarif- und Arbeitszeitregelungen, sowie (AÜ-)Verträgen</li> <li>- Abrechnungsinformationen</li> </ul>
Sonstige Daten	<ul style="list-style-type: none"> <li>- Kommentare (Nutzer mit der gleichen Firmenzuordnung können Kommentare zu Bewerbungsvorgängen hinterlassen)</li> <li>- System-/Leistungsdaten über die Bereitstellung der Leistungen des Auftragnehmers</li> </ul>

#### 2.2 Kategorien betroffener Personen

Betroffenengruppe	Beschreibung	Beispiele
Mitarbeiter des Auftraggebers / Entleiher (Aktive User)	User von Jobkey, d.h. verantwortliche HR-Manager oder Niederlassungsleiter, die den Bewerbungsprozess der Zeitarbeitnehmer verwalten.	<ul style="list-style-type: none"> <li>- HR-Manager,</li> <li>- Niederlassungsleiter,</li> <li>- Produktionsleiter,</li> <li>- Geschäftsführer</li> </ul>
Mitarbeiter des Auftragnehmers / Verleiher (Aktive User)	User von Jobkey, d.h. verantwortliche Niederlassungsleiter, die Bewerber in Jobkey einspielen.	<ul style="list-style-type: none"> <li>- Niederlassungsleiter,</li> <li>- Key-Account Manager,</li> <li>- Geschäftsführer</li> </ul>
Zeitarbeitnehmer		<ul style="list-style-type: none"> <li>- Bewerber,</li> <li>- Zeitarbeiter</li> </ul>

### **Anlage 3**

#### **Weisungsberechtigte Personen des Auftraggebers**

Darüber hinaus nimmt der Auftragsverarbeiter an, dass alle vom Auftraggeber als "Nutzer" benannten Personen weisungsberechtigte Personen des Auftraggebers sind. Es liegt in der Verantwortung des Auftraggebers, Abweichungen davon mitzuteilen.

## Anlage 4

### **Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO)**

#### **4.1 Zutrittskontrolle** (Maßnahmen, die verhindern, dass Unbefugte Zutritt zu Gebäuden und Räumen bekommen, in denen sich Datenverarbeitungsanlagen befinden)

- Perimetersicherung
  - Zaun
  - Flutlicht
  - Videoüberwachung
  - Zutrittskontrollsystem
- Gebäudesicherung
  - Manuelles Schließsystem
- Innenraumsicherung
  - Zutrittskontrollsystem
- Organisatorische Maßnahmen
  - Zutrittskonzept
  - Schlüsselregelung
  - Dokumentierte Schlüsselausgabe
  - Besucherprozess

#### **4.2 Zugangskontrolle** (Maßnahmen, die sicherstellen, dass Unbefugten kein Zugang zu Datenverarbeitungssystemen haben)

- Technische Maßnahmen
  - Authentifikation mittels Passworteingabe, zentrale Passwortvergabe, Benutzerkennung mit Passwortrichtlinie
  - Verschlüsselung von Datenträgern und mobilen Endgeräten (z. B. SSL-Verbindungen)
  - Sichere WLAN-Verschlüsselung für drahtlose Netzwerke
  - Clean-Desk-Richtlinie
  - Automatische Desktopsperre
  - Mehr-Faktor-Authentifizierung (MFA)
  - Firewall
  - Anti-Viren-Software
  - Bildschirmschutzfilter bei Reisen zur Verhinderung von Einsicht durch Unbefugte
- Organisatorische Maßnahmen
  - Berechtigungskonzept sowie regelmäßige Überprüfung und Aktualisierung
  - Vertraulichkeitsvereinbarungen mit externen Dienstleistern
  - Definierte On- und Offboarding-Prozesse

- Mitarbeiterschulungen für Mitarbeiter zum Sicherheitsbewusstsein

#### 4.3 **Zugriffskontrolle** (Maßnahmen, die sicherstellen, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben)

- Technische Maßnahmen
  - Rollenbasierte Zugriffskontrolle durch Zuweisung von Zugriffsrechten basierend auf der Rolle des Mitarbeiters im Unternehmen
  - Berechtigungsmanagement-Systeme durch Einsatz von Software zur Verwaltung und Kontrolle von Benutzerrechten
  - Automatische Konto-Sperrung
- Organisatorische Maßnahmen
  - Berechtigungskonzept
  - Regelmäßige Prüfung von Zugriffsrechten sowie Verfahren bei Vergabe/Entziehung von Rechten
  - Verwaltung der Benutzerrechte durch IT-Administrator bzw. Geschäftsführung
  - Mitarbeiterschulungen zur Datensicherheit

#### 4.4 **Weitergabekontrolle** (Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, wer personenbezogene Daten erhalten haben)

- Technische Maßnahme
  - Der Auftraggeber übermittelt personenbezogene Daten nur auf eigene Veranlassung und ausschließlich remote auf das System des Auftragnehmers.
  - Sollte im Ausnahmefall kein Remote-Zugriff möglich sein: Elektronische Signatur und/oder E-Mail-Verschlüsselung

Penetrationstests

#### 4.5 **Eingabekontrolle** (Maßnahmen, die sicherstellen, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat)

- Technische Maßnahme
  - Ständige Überwachung und Protokollierung durch den Auftragnehmer für die Dauer des Remotezugriffs (ggf. auch durch Aufzeichnung)
  - Aufzeichnung von Nutzeraktivitäten (z. B. Log-ins) durch Unterauftragnehmer für die Dauer von grundsätzlich 30 Tagen
- Organisatorische Maßnahme

- Dokumentation der Verarbeitungsprozesse einschließlich der eingesetzten Software und der damit jeweils verarbeiteten Daten (Verarbeitungsübersicht)

**4.6 Auftragskontrolle** (Maßnahmen, die sicherstellen, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden)

- Technische Maßnahme
  - Protokollierung von Systemzugriffen
  - Automatisierte Meldung zum Status der Verarbeitung
- Organisatorische Maßnahme
  - Live-Monitoring von Systemzugriffen
  - Sorgfältige Auswahl von Unterauftragnehmern, ggf. inkl. regelmäßiger Prüfung der getroffenen Sicherheitsmaßnahmen und deren Dokumentation
  - Abschluss der notwendigen Vereinbarungen, darunter
    - Schriftliche Weisungen für Auftragnehmer (AV-Vertrag),
    - Rechtliche Prüfung auf Verpflichtung der Mitarbeiter des Auftragnehmers,
    - Rechtliche Prüfung der Verpflichtung zur Bestellung eines Datenschutzbeauftragten,
    - Vereinbarung wirksamer Kontrollrechte gegenüber dem Unterauftragnehmer,
  - Festlegung der Regelungen zum Einsatz weiterer Unterauftragnehmer.
  - Schriftliche Weisungen für Auftragnehmer (AV-Vertrag)
  - Rechtliche Sicherstellung der datenschutzkonformen Vernichtung von Daten nach Beendigung des Auftrages

**4.7 Verfügbarkeitskontrolle** (Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Verantwortlichen stets verfügbar sind)

- Technische Maßnahme
  - Unterbrechungsfreie Stromversorgung (USV)
  - Notstromversorgung
  - Spiegelung von Daten
- Organisatorische Maßnahme
  - Service Level Agreements

**4.8 Pseudonymisierung und Verschlüsselung**

- Technische Maßnahme
  - Verschlüsselung von Daten, nämlich: TLS-Verbindungen

**4.9 Belastbarkeit der Systeme und Dienste** (Maßnahmen, die sicherstellen, dass die eingesetzten Systeme und Dienste fehlertolerant sind und bei Störungen und Teilausfällen die wesentlichen Funktionen aufrechterhalten)

- Technische Maßnahme
  - Server-Cluster für Datenbanken, Webservices und sonstige Dienste
- Organisatorische Maßnahme
  - Monitoring der Systemverfügbarkeiten
  - Vereinbarungen angemessener Service-Level, Reaktions- und Wiederherstellungszeiten mit Dienstleistern

**4.10 Rasche Wiederherstellung** (Maßnahmen, die sicherstellen, dass die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann)

- Technische Maßnahme
  - Keine Übertragung ins eigene System des Auftragnehmers
  - Regelmäßige Datensicherungen

**4.11 Regelmäßige Überprüfung** (Maßnahmen zur Bewertung und Evaluierung der Wirksamkeit technisch-organisatorischer Maßnahmen)

- Technische Maßnahme
  - Protokollierung von sicherheitsrelevanten Vorgängen
  - Protokollierung von Benutzeraktivitäten
  - Regelmäßige Software-Updates
- Organisatorische Maßnahme
  - Auswertung von Sicherheitsvorfällen
  - Regelmäßige interne Audits
  - Aktualisierung von Sicherheitsrichtlinien
  - Risikobewertungen
  - Mitarbeiterschulungen zur Sensibilisierung von Mitarbeitern zum Thema Datenschutz
  - Mitarbeiterschulungen zu Cybersecurity/IT-Sicherheit



## Anlage 5

### Subunternehmer des Auftragnehmers

Zum Kreis der genehmigten Unterauftragnehmer bei Abschluss dieses Vertrages gehören die im folgenden Abschnitt genannten Dienstleister:

	Subunternehmer	Weitere Informationen
1.	Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	<ul style="list-style-type: none"><li>- <u>Dienstleistung:</u> Nutzung cloudbasierter Dienstleistungen</li><li>- <u>Rechtsgrundlage für Drittlandtransfer:</u><ul style="list-style-type: none"><li>- Zertifizierung unter Data Privacy Framework (Art. 45 Abs. 1 DSGVO)</li><li>- Standardvertragsklauseln der EU Kommission, Art. 46 Abs. 2 lit. c) DSGVO</li></ul></li><li>-</li></ul>
2.	Celonis, Inc. One World Trade Center 87th Floor New York, NY 10007, U.S.	<ul style="list-style-type: none"><li>- <u>Dienstleistung:</u> Senden von E-Mail-Benachrichtigungen</li><li>- <u>Rechtsgrundlage für Drittlandtransfer:</u><ul style="list-style-type: none"><li>- Zertifizierung unter Data Privacy Framework (Art. 45 Abs. 1 DSGVO)</li><li>- Standardvertragsklauseln der EU Kommission, Art. 46 Abs. 2 lit. c) DSGVO</li></ul></li></ul>
3.	Formagrid Inc 799 Market St., 8th Floor, San Francisco, California 94103, U.S.	<ul style="list-style-type: none"><li>- <u>Dienstleistung:</u> Bereitstellung der Datenbank</li><li>- <u>Serverstandort:</u> Die Daten werden grundsätzlich auf Servern in der EU verarbeitet.</li><li>- <u>Rechtsgrundlage für Drittlandtransfer:</u><ul style="list-style-type: none"><li>- Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c) DSGVO zu.</li></ul></li></ul>
4.	typeguard Inc., 1 Blackfield Drive, Suite 2, #346 Tiburon, CA 94920, U.S.	<ul style="list-style-type: none"><li>- <u>Dienstleistung:</u> Bereitstellung des Frontends und der User Datenbank</li><li>- <u>Rechtsgrundlage für Drittlandtransfer:</u><ul style="list-style-type: none"><li>- Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c) DSGVO zu.</li></ul></li></ul>

5.	Yousign SAS, Rue De Suède Av Pierre Berthelot 1400 - Caen, Frankreich	- <u>Dienstleistung:</u> Erstellen von rechtsgültigen AÜV-Verträgen mittels qualifizierter elektronischer Signatur (QES)
6.	Intercom R&D Unlimited Company, Stephen Court 18-21 Saint Stephen's Green, Dublin 2, Irland	- <u>Dienstleistung:</u> Kommunikationsplattform
7.	Heyflow GmbH, Jungfernstieg 49, 20354 Hamburg	- <u>Dienstleistung:</u> Einbindung von Formularen und Upload von Dokumenten