Vereinbarung über Auftragsverarbeitung gemäß Art. 28 DS-GVO

Präambel:

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Vertragsparteien bezüglich der Auftragsverarbeitung durch Recruit United (im Folgenden „Auftragnehmer“) im Rahmen des Hauptvertrags zur Nutzung der Recruit United-Plattform. Sie gilt für alle Aktivitäten, bei denen Mitarbeiter des Auftragnehmers oder beauftragte Dritte des Auftragnehmers mit personenbezogenen Daten des Kunden (im Folgenden „Auftraggeber“) in Kontakt kommen könnten.

§ 1 Definitionen:

- Personenbezogene Daten: Informationen, die sich auf identifizierbare natürliche Personen beziehen.
- Personenbezogene Daten des Auftraggebers: Daten, die der Auftragnehmer für den Auftraggeber erhebt oder erhält.
- Datenverarbeitung: Alle Vorgänge im Zusammenhang mit personenbezogenen Daten.
- Datenverarbeitung im Auftrag: Verarbeitung durch den Auftragnehmer im Namen des Auftraggebers.
- Weisung: Anweisungen gemäß Hauptvertrag oder zusätzlichen schriftlichen Weisungen.
- Datenschutzvorschriften: Gesetze und Vorschriften zum Datenschutz.
- EU: Mitgliedstaaten der Europäischen Union.

§ 2 Gegenstand und Dauer des Auftrags; Umfang, Art und Zweck der Datenverarbeitung; Art der Daten und Kreis der Betroffenen:

Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers gemäß den Vorgaben des Hauptvertrags und etwaigen zusätzlichen Weisungen. Dies umfasst Tätigkeiten gemäß der Leistungsbeschreibung des Hauptvertrags.

Die Dauer und der Umfang der Datenverarbeitung richten sich nach den Regelungen des Hauptvertrags sowie den Weisungen des Auftraggebers.

Der Zweck der Datenverarbeitung besteht darin, die im Hauptvertrag festgelegten Tätigkeiten zu erfüllen. Die betroffenen Personen umfassen Mitarbeiter des Auftraggebers sowie deren Nutzungsdaten und potenzielle Kandidaten.

§ 3 Technisch-organisatorische Maßnahmen:

- Der Auftragnehmer verpflichtet sich zur Umsetzung und Einhaltung technisch-organisatorischer Maßnahmen gemäß den geltenden Datenschutzvorschriften, insbesondere Art. 32 DS-GVO. Diese Maßnahmen gewährleisten ein angemessenes Datenschutzniveau und die Sicherheit der Datenverarbeitung. Dazu zählen:
- Zutrittskontrolle, um unbefugten Zugriff zu verhindern.
- Zugangskontrolle, um die Nutzung von Datenverarbeitungssystemen zu regeln.
- Zugriffskontrolle, um sicherzustellen, dass autorisierte Personen nur auf relevante Daten zugreifen.
- Weitergabekontrolle, um Datenübertragung und -speicherung zu sichern.
- Eingabekontrolle, um Veränderungen an Daten nachvollziehbar zu machen.
- Auftragskontrolle, um die Verarbeitung nach Weisung des Auftraggebers zu gewährleisten.
- Verfügbarkeitskontrolle, um Daten vor Zerstörung oder Verlust zu schützen.
- Trennungskontrolle, um Daten getrennt zu verarbeiten.
- Pseudonymisierung und Verschlüsselung von Daten.
- Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit der Systeme.
- Wiederherstellungsverfahren bei Zwischenfällen.
- Regelmäßige Überprüfung und Evaluierung der Sicherheitsmaßnahmen.

Der Auftragnehmer hat dem Auftraggeber ein Datenschutz- und Datensicherheitskonzept vorgelegt, das alle technischen und organisatorischen Maßnahmen beschreibt. Dieses Konzept wird regelmäßig überprüft, bewertet und aktualisiert. Der Auftraggeber kann auf Anfrage Einblick in diese Maßnahmen erhalten, die auch durch Testate, Berichte oder Zertifizierungen belegt werden können.

§ 4 Berichtigung, Sperrung und Löschung / Betroffenenrechte:

Der Auftragnehmer darf Daten nur gemäß den Weisungen des Auftraggebers berichtigen, sperren oder löschen. Anfragen von Betroffenen zur Berichtigung, Sperrung oder Löschung ihrer Daten werden umgehend an den Auftraggeber weitergeleitet. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Betroffenenrechte gemäß den Datenschutzvorschriften.

§ 5 Kontrollen und sonstige Pflichten des Auftragnehmers:

- Mitarbeiter des Auftragnehmers sind zur Einhaltung des Datengeheimnisses verpflichtet.
- Der Auftragnehmer informiert den Auftraggeber über Kontrollen und Ermittlungen der Datenschutzbehörden.
- Die Einhaltung der Datenschutzbestimmungen wird regelmäßig kontrolliert und angepasst.
- Auf Anfrage des Auftraggebers werden umfassende Informationen zur Datenverarbeitung bereitgestellt.
- Ein Verzeichnis von Verarbeitungstätigkeiten wird geführt und bei Bedarf der Aufsichtsbehörde vorgelegt.
- Der Auftragnehmer unterstützt den Auftraggeber bei Datenschutz-Folgenabschätzungen und Konsultationen mit den Aufsichtsbehörden.

§ 6 Subunternehmer (Unterauftragsverhältnisse):

Der Auftragnehmer kann Subunternehmer für spezifizierte Leistungen einschalten, wie z. B. Amazon Web Services für die Bereitstellung der Datenbank zur Nutzerverwaltung.

Änderungen bezüglich der Hinzuziehung oder des Austauschs von Subunternehmern werden dem Auftraggeber mitgeteilt, der Einspruch erheben kann.

Subunternehmer müssen vertraglich den Datenschutzanforderungen entsprechen, und dem Auftraggeber werden Kontrollrechte eingeräumt.

§ 7 Kontrollrechte des Auftraggebers:

Der Auftraggeber kann die Einhaltung der Datenschutzmaßnahmen durch den Auftragnehmer in dessen Betriebsstätten prüfen.
Der Auftragnehmer stellt auf Anforderung alle relevanten Auskünfte und Nachweise zur Verfügung, die für eine umfassende Kontrolle erforderlich sind.

§ 8 Mitteilung bei Verstößen des Auftragnehmers:

Der Auftragnehmer meldet Verstöße gegen Datenschutzvorschriften oder vertragliche Festlegungen dem Auftraggeber unverzüglich.

Bei Verstößen unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung von Melde- und Benachrichtigungspflichten und dokumentiert die Vorfälle entsprechend den Datenschutzvorschriften.

§ 9 Weisungsbefugnis des Auftraggebers:

Die Datenverarbeitung erfolgt gemäß den Weisungen des Auftraggebers, der ein umfassendes Weisungsrecht hat.

Der Auftragnehmer informiert den Auftraggeber über etwaige Bedenken bezüglich der Weisungen, und die Ausführung einer Weisung wird ausgesetzt, bis sie bestätigt oder geändert wird.

§ 10 Löschung von Daten und Rückgabe von Datenträgern:

Nach Abschluss der vertraglichen Arbeiten oder auf Aufforderung des Auftraggebers müssen sämtliche im Zusammenhang mit dem Auftragsverhältnis stehenden Unterlagen, Datenbestände und erstellte Verarbeitungsergebnisse datenschutzgerecht an den Auftraggeber übergeben oder vernichtet werden.

Dokumentationen zur Nachweisführung der Datenverarbeitung sind entsprechend der Aufbewahrungsfristen auch über das Vertragsende hinaus aufzubewahren.

§ 11 Auftragnehmer außerhalb der EU:

Der Auftragnehmer garantiert, dass die Verarbeitung personenbezogener Daten außerhalb der EU den geltenden Datenschutzvorschriften entspricht.

Es wird sichergestellt, dass auch Subunternehmer angemessene Datenschutzstandards einhalten, beispielsweise durch den Abschluss von EU-Standardvertragsklauseln.

Der Auftragnehmer informiert den Auftraggeber unverzüglich schriftlich, wenn die datenschutzrechtliche Rechtfertigung nicht mehr gegeben ist oder erkennbar wird.

Der Auftragnehmer stellt den Auftraggeber von etwaigen Ansprüchen Dritter frei, die auf einem Verstoß gegen Datenschutzbestimmungen beruhen.

Bei Wegfall der datenschutzrechtlichen Rechtfertigung kann der Auftraggeber den Hauptvertrag außerordentlich kündigen oder den Auftragnehmer zur Vorlage alternativer datenschutzrechtlicher Rechtfertigungen auffordern.

§ 12 Kosten:

Alle Kosten, die aus der Erfüllung der Vereinbarung entstehen, trägt der Auftragnehmer.

Die im Hauptvertrag vereinbarte Vergütung des Auftragnehmers deckt auch die Kosten gemäß dieser Vereinbarung ab.

§ 14 Sonstiges, Allgemeines:

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn die personenbezogenen Daten des Auftraggebers durch Dritte gefährdet werden.

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform und expliziter Zustimmung.

Die Bestimmungen der Vereinbarung gelten auch nach Vertragsende bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten an den Auftraggeber.

Die Regelungen des Hauptvertrages finden eine entsprechende Anwendung.

Anlage 1: Datenschutz- und Datensicherheitskonzept / Technische und organisatorische Maßnahmen / Recruit United

Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO:

Maßnahmen zur Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:

Recruit United implementiert geeignete technische und organisatorische Maßnahmen, um den Anforderungen der DS-GVO zu genügen. Dies umfasst auch datenschutzfreundliche Voreinstellungen, die sicherstellen, dass nur die für den jeweiligen Verarbeitungszweck erforderlichen personenbezogenen Daten verarbeitet werden.

Maßnahmen zur Sicherstellung der Vertraulichkeit:

Recruit United gewährleistet, dass vertrauliche Daten und Informationen nur befugten Personen in zulässiger Weise zugänglich sind. Dies wird unter anderem durch klare Organisationsstrukturen und Anweisungen sichergestellt.

Organisationskontrolle:

Recruit United stellt sicher, dass die interne Organisation den besonderen Anforderungen des Datenschutzes gerecht wird. Dazu gehören unter anderem klare Richtlinien, die Bestellung eines Datenschutzbeauftragten sowie Schulungen und Sensibilisierungsmaßnahmen für die Mitarbeiter.

Verschlüsselung und Pseudonymisierung personenbezogener Daten:

Um die Vertraulichkeit personenbezogener Daten zu gewährleisten, setzt Recruit United auf Verschlüsselungsmethoden und Pseudonymisierungstechniken. Dies umfasst unter anderem die Übermittlung von Daten über verschlüsselte Netzwerke und die Verschlüsselung von mobilen Datenträgern.

Zutrittskontrolle:

Der Zugang zu IT-Systemen und Verarbeitungsanlagen wird streng kontrolliert und Unbefugten verwehrt. Dies wird durch elektronische Türsicherungen, kontrollierte Schlüsselvergabe und die Beaufsichtigung von Fremdpersonen sichergestellt.

Weitere Sicherheitsmaßnahmen:

Recruit United implementiert auch weitere Sicherheitsmaßnahmen wie die Einschränkung der Privatnutzung von Kommunikationsmitteln, Schulungen zum Datenschutz für Mitarbeiter und Maßnahmen zur Personalsicherheit.

Diese Maßnahmen dienen dazu, die Anforderungen der DS-GVO zu erfüllen und die Sicherheit und Vertraulichkeit der verarbeiteten Daten zu gewährleisten.

Physische Sicherheit der Server-Systeme:

Recruit United setzt Server-Systeme ein, die in zertifizierten Rechenzentren mit umfassenden physischen Sicherheitsmaßnahmen untergebracht sind.

Zugangskontrolle:

a) Authentifizierung: Der Zugriff auf Daten erfolgt über sichere Protokolle und erfordert eine eindeutige Authentifizierung.

b) Verwendung sicherer Passwörter: Mitarbeiter verwenden sichere Passwörter gemäß bewährten Sicherheitsstandards.

c) Automatische Sperrung: Bei Inaktivität werden Geräte automatisch gesperrt, um unbefugten Zugriff zu verhindern.

d) Einsatz von Anti-Viren-Software: Alle betrieblichen IT-Systeme sind mit aktueller Anti-Viren-Software ausgestattet.

e) "Clean Desk Policy": Mitarbeiter werden angehalten, Arbeitsmaterialien ordentlich zu verwahren und sensible Daten sicher zu entsorgen.

Zugriffskontrolle:

a) Rollen- und Berechtigungskonzept: Der Zugriff auf Systeme erfolgt nach einem klaren Rollen- und Berechtigungskonzept, das sicherstellt, dass Mitarbeiter nur auf die Daten zugreifen können, die für ihre Aufgaben erforderlich sind.

b) Dokumentation und Überprüfung: Zugriffsrechte werden dokumentiert und regelmäßig überprüft, um sicherzustellen, dass sie den aktuellen Anforderungen entsprechen.

Diese Maßnahmen dienen dazu, die Sicherheit der Räumlichkeiten und Daten bei Recruit United zu gewährleisten und einen angemessenen Schutz vor unbefugtem Zugriff zu bieten, insbesondere mit Blick auf zukünftige Mitarbeiter.

Protokollierung von An- und Abmeldevorgängen:

Anmeldeversuche und Abmeldungen von Admin-, Kunden- und Server-Systemen/Software werden protokolliert (mindestens E-Mail-Adresse, Benutzer-ID, IP-Adresse, Anmeldeergebnis und Zeitstempel) und für einen Zeitraum von bis zu 30 Tagen aufbewahrt. Diese Protokolle können bei Bedarf oder bei konkretem Verdacht ausgewertet werden.

Trennbarkeit:

Es wird sichergestellt, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben werden, separat verarbeitet werden können, um eine unbeabsichtigte Nutzung dieser Daten für andere Zwecke auszuschließen.

a) Trennung von Entwicklungs-, Test- und Betriebsumgebungen:

Daten aus der Betriebsumgebung dürfen nur in Test- oder Entwicklungsumgebungen übertragen werden, wenn sie vorher vollständig anonymisiert wurden. Die Übertragung anonymisierter Daten erfolgt verschlüsselt oder über ein vertrauenswürdiges Netzwerk. Software wird erst nach umfangreichen Tests in einer identischen Testumgebung in die Betriebsumgebung überführt. Programme zur Fehleranalyse oder zum Erstellen/Kompilieren von Software dürfen in der Betriebsumgebung nur eingesetzt werden, wenn dies unvermeidlich ist, insbesondere bei Fehlersituationen, die von Daten abhängen, die durch Anonymisierungsanforderungen in Testumgebungen verfälscht würden.

b) Softwareseitige Mandantentrennung:

Recruit United gewährleistet die getrennte Verarbeitung und Speicherung von Daten verschiedener Auftraggeber durch eine logische Mandantentrennung auf Basis einer Multi-Tenancy-Architektur. Die Daten werden über eine eindeutige Kennung je Auftraggeber (z. B. Kundennummer/ "Company ID") zugeordnet und identifiziert. Die Architektur ist durch Integrationstests abgesichert, um sicherzustellen, dass keine Datenbankabfragen ohne Abfrage und Zuordnung zu dieser Kennung erfolgen und das Risiko einer Umgehung der Mandantentrennung durch Programmfehler minimiert wird.

Maßnahmen zur Sicherstellung der Integrität:

Integrität bezieht sich auf die Sicherstellung der Korrektheit (Unverfälschtheit) von Daten und der ordnungsgemäßen Funktion von Systemen.

Transport- und Weitergabekontrolle:

Es wird sichergestellt, dass bei der Übertragung personenbezogener Daten und beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

a) Transportverschlüsselung ("Daten im Transit"):

Siehe "Verschlüsselung und Pseudonymisierung personenbezogener Daten".

b) Verbot der Weitergabe an unberechtigte Dritte:

Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, ist nur in dem Umfang gestattet, der zur Erfüllung der vertraglichen Leistungen für den Auftraggeber erforderlich ist. Insbesondere ist eine Weitergabe von personenbezogenen Daten aus dem Auftrag an unberechtigte Dritte untersagt.

c) Protokollierung der Weitergabe von Daten:

Siehe "Protokollierung von Systemaktivitäten innerhalb des Admin- und Kunden-Systems sowie Auswertung" unter "Eingabekontrolle".

Sicherheit der Datenverarbeitung außerhalb der Geschäftsräume:

Wenn personenbezogene Daten außerhalb der Geschäftsräume von Recruit United verarbeitet werden, z. B. im Homeoffice von Mitarbeitern, gelten die gleichen Sicherheitsstandards wie in den Geschäftsräumen. Dies umfasst den Schutz vor unbefugtem Zugriff, die Verschlüsselung von Datenübertragungen und die sichere Aufbewahrung von Datenträgern.

Durchführung von Datenschutz-Folgenabschätzungen:

Recruit United unterstützt den Auftraggeber bei der Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DS-GVO. Dies umfasst die Analyse von Datenschutzrisiken im Zusammenhang mit geplanten Datenverarbeitungsvorgängen sowie die Entwicklung von Maßnahmen zur Risikominimierung.

Durchführung von Konsultationen mit den Aufsichtsbehörden:

Recruit United steht dem Auftraggeber bei Konsultationen mit den Aufsichtsbehörden gemäß Art. 36 DS-GVO zur Verfügung. Dies beinhaltet die Zusammenarbeit bei der Erstellung von Stellungnahmen zu geplanten Datenverarbeitungsvorgängen und die Beantwortung von Anfragen der Aufsichtsbehörden.

Verantwortlichkeiten und Haftung:

Die Verantwortlichkeiten und Haftungsfragen im Zusammenhang mit der Verarbeitung personenbezogener Daten werden im Hauptvertrag zwischen den Parteien geregelt. Recruit United haftet für Schäden, die durch Verstöße gegen Datenschutzvorschriften oder vertragliche Vereinbarungen entstehen, soweit diese auf ihr Verschulden zurückzuführen sind.

Schlussbestimmungen:

Diese Anlage zur Datenschutzvereinbarung ist ein integraler Bestandteil der Vereinbarung über Auftragsverarbeitung zwischen den Parteien. Änderungen oder Ergänzungen bedürfen der Schriftform und expliziter Zustimmung beider Parteien.