Datenschutzvertrag zur Datenverarbeitung im Auftrag gemäß Art. 28 EU-Datenschutz-Grundverordnung (DSGVO)

Im Auftrag von	verarbeitet durch
	softgarden e-recruiting GmbH Tauentzienstraße 14 10789 Berlin
- nachfolgend „**Auftraggeber“** genannt	- nachfolgend „**Auftragnehmer“** genannt -

gemeinsam im Folgenden **Vertragspartner** genannt.

§ 1 Allgemeines

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO).
2. Bei etwaigen Widersprüchen gehen die Regelungen dieser Vereinbarung mit all seinen Bestandteilen den Regelungen des zugehörigen Hauptvertrages vor.
3. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) verwendet wird, ist dem die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.
4. Der Auftragnehmer verpflichtet sich, für die Bereitstellung des Recruiting- und Bewerbermanagementsystem nur Rechenzentren in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) einzusetzen.
5. Die Verlagerung zum Zweck der Bereitstellung gem. Abs. 4 in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44ff. DSGVO erfüllt sind und der Auftraggeber der Verlagerung im Vorfeld zugestimmt hat. Es gelten die Bestimmungen des § 7.

§ 2 Gegenstand und Dauer der Verarbeitung

1. Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Zusammenhang mit dem Einsatz des Recruiting- und Bewerbermanagementsystems als Software as a Service (SaaS) durch den Auftraggeber
2. Art, Umfang und Zweck der Verarbeitung personenbezogener Daten im Auftrag sind in **Anlage 1** dieser Vereinbarung konkretisiert. Die Verarbeitung richtet sich insbesondere nach den Weisungen des Auftraggebers sowie nach dem durch den Auftragnehmer bereitgestellten Produktumfang, dessen Bestandteilen und den für diese Zwecke erfolgten Verarbeitungen.
3. Eine von der Auftragsverarbeitung abweichende Verarbeitung von Daten ist dem Auftragnehmer nur gestattet, wenn er diese als eigener Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO durchführt und die Verarbeitung als solche kenntlich macht.
4. Die Laufzeit der Vereinbarung zur Auftragsverarbeitung richtet sich nach der Laufzeit der zugehörigen Vertragsverhältnisse (Leistungsvereinbarungen).

§ 3 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Wahrung der Betroffenenrechte verantwortlich, die sich aus den Art. 12 bis 23 DSGVO ergeben.
2. Der Auftraggeber ist als Verantwortlicher, im Rahmen der durch den Auftragnehmer durchgeführten Verarbeitung im Auftrag, für die Meldung und Benachrichtigung im Falle der Verletzung des Schutzes personenbezogener Daten verantwortlich, Art. 33 und 34 DSGVO. Dem Auftraggeber

ist bekannt, dass Meldungen der Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden gegenüber der Aufsichtsbehörde erfolgen sollten.

3. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform (mind. per E-Mail/Ticket) zu bestätigen.
4. Der Auftraggeber verpflichtet sich, Weisungen nur weisungsberechtigten Personen zu überlassen. Der Auftragnehmer ist berechtigt, bei einer durch den Auftraggeber erteilten Weisung von einer entsprechenden Weisungsberechtigung auszugehen.
5. Abweichend von Abs. 4 ist der Auftraggeber berechtigt, Personen gegenüber dem Auftragnehmer zu benennen, die gegenüber dem Auftragnehmer weisungsberechtigt sind.
6. Der Auftraggeber ist nach Maßgabe des § 6 dieser Vereinbarung zur Kontrolle der Einhaltung technischer und organisatorischer Maßnahmen des Auftragnehmers berechtigt.

§ 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer ist in Erfüllung des § 3 Abs. 2 dieser Vereinbarung verpflichtet, dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die voraussichtlich zu einem Risiko für die Rechte und Freiheiten Betroffener führt und die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet, unverzüglich mitzuteilen.
2. Die Meldung des Auftragnehmers an den Auftraggeber enthält mindestens die folgenden Angaben zum Vorfall:
   - Eine Beschreibung zum Vorfall der Verletzung des Schutzes personenbezogener Daten
   - Angaben zu betroffenen Daten und Datensätzen sowie der Umfang betroffener Personen
   - Eine Voreinschätzung zu den wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
   - Eine Beschreibung der vom Auftragnehmer bereits ergriffenen Maßnahmen und/oder Maßnahmen-Vorschläge, um nachteilige Folgen für Betroffene abzuwenden oder abzumildern
3. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betrifft.
4. Der Auftragnehmer wird in Erfüllung des § 3 Abs. 1 dieser Vereinbarung den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen. Der Auftragnehmer verpflichtet sich, den Auftraggeber bei der Erfüllung von Betroffenenrechten nach besten Kräften zu unterstützen, insbesondere nach Weisung des Auftraggebers sowie durch geeignete technische und organisatorische Maßnahmen.
5. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.
6. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist, ohne Anerkennung einer Prüfpflicht, ob eine rechtswidrige Weisung vorliegt, berechtigt, eine nach seiner Auffassung rechtswidrige Weisung abzulehnen oder auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird oder offensichtlich rechtswidrige Weisungen jederzeit abzulehnen oder dies bezogene Verarbeitungen auszusetzen.
7. Der Auftragnehmer benennt als berechtigte Weisungsempfänger den Bereich Customer Service und Support, Kontakt: support@softgarden.de. Mitarbeiter des Bereichs sowie Bereichsverantwortliche des Auftragnehmers sind zum Empfang von Weisungen berechtigt.
8. Der Auftragnehmer ist nach Maßgabe des § 9 dieser Vereinbarung zur Einhaltung der für die Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen verpflichtet.

§ 5 Mitteilungspflicht bei Offenlegung

1. Der Auftragnehmer wird den Auftraggeber unverzüglich über jedes Ersuchen oder Verlangen zur Offenlegung von Informationen, gleich welcher Art, seitens Strafverfolgungsbehörden und anderen staatlichen Stellen informieren, soweit diese in Zusammenhang mit den zwischen Auftraggeber und Auftragnehmer geschlossenen Vereinbarungen stehen („Mitteilungspflicht“)

2. Der Auftraggeber ist für die Entscheidung über und die Verfahrensweise der Offenlegung betroffener Informationen gegenüber staatlichen Stellen allein verantwortlich und ist vom Auftragnehmer nach besten Kräften bei der Offenlegung zu unterstützen.

3. Von der Mitteilungspflicht gegenüber dem Auftraggeber ist der Auftragnehmer nur dann befreit, wenn der Auftragnehmer selbst zur Offenlegung gegenüber staatlichen Stellen sowie zur Geheimhaltung gegenüber dem Auftraggeber verpflichtet ist.

§ 6 Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, Überprüfungen der Einhaltung technischer und organisatorischer Maßnahmen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mindestens 14 Tage zuvor unter Begründung des speziellen Anlasses anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten und im Benehmen mit dem Auftragnehmer zu überzeugen.

2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

3. Die Parteien vereinbaren, dass Vor-Ort Kontrollen i. S. d. Abs. 1 höchstens einmal jährlich stattfinden und nur dann erforderlich sind, wenn die Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO nicht bereits durch Nachweise im Sinne von Abs. 4 nachgewiesen werden kann. Darüber hinaus sind Vor-Ort Prüfungen vom Auftraggeber unter Angabe des speziellen Anlasses zu begründen und nur in besonderen Ausnahmefällen für mehr als einen Audit-Tag pro Jahr zulässig.

4. Der Nachweis der technischen und organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

   - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
   - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

   Wenn andere Nachweise es dem Auftraggeber in angemessener und den Schutzanforderungen gerechter Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag zu überzeugen, sind auch diese geeignet (z. B. Konzepte, Richtlinien, Stellungnahmen).

5. Im Falle einer erforderlichen (Vor-Ort-) Kontrolle des Auftraggebers beim Auftragnehmer trägt jede Partei die durch die Prüfung anfallenden Kosten, wie Prüfungs-, Personal- und Reisekosten, selbst. Soweit die Mitwirkung des Auftragnehmers im Zusammenhang mit Kontrollen über das erforderliche Maß i. S. d. Abs. 3 hinausgeht sowie dies mit einem höheren Prüfaufwand oder der Beauftragung externer Dienstleister durch den Auftragnehmer verbunden ist (z. B. mehrtägiges Audit), können die dafür anfallenden Kosten dem Auftraggeber nach den branchenüblichen Stunden- und Tagessätzen in Rechnung gestellt werden.

§ 7 Unterauftragsverhältnisse

1. Der Auftraggeber stimmt der Beauftragung der in **Anlage 1** bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu.
2. Der Wechsel der gemäß **Anlage 1** bestehenden Unterauftragnehmer oder die Hinzuziehung weiterer Unterauftragnehmer ist zulässig, soweit:
   - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab in Textform oder einer geeigneten elektronischen Form anzeigt und
   - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in geeigneter elektronischer Form Einspruch gegen die geplante Auslagerung erhebt und
   - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird, die dem für die Verarbeitung erforderlichen Datenschutz- und Sicherheitsniveau der Datenverarbeitung gerecht wird.
3. Als optional und/oder als kostenfrei erkennbare Leistungen von Drittanbietern bzw. Unterauftragnehmern des Auftragnehmers, die i. d. R. durch ein sog. „Opt-In“-Verfahren vom Auftraggeber eingesetzt werden können, begründen keinen Rechtsanspruch auf die betreffende Leistung oder einen bestimmten Anbieter der Leistung. Der Auftragnehmer behält insbesondere sich bei Vorliegen eines wichtigen Grundes vor, diese Leistungen zu deaktivieren oder einzuschränken.
4. Leistungen von Drittanbietern, die über den sog. Marketplace des Auftragnehmers und – soweit möglich –auch individuell gebucht und durch den Auftragnehmer im Auftrag des Auftraggebers in das System integriert werden können, werden – soweit nicht anders vereinbart – nicht Unterauftragnehmer des Auftragnehmers und begründen keine datenschutzrechtliche Prüfpflicht des Auftragnehmers. Der Auftragnehmer behält sich insbesondere bei Vorliegen eines wichtigen Grundes vor, diese Leistungen zu deaktivieren oder einzuschränken.

§ 8 Vertraulichkeitsverpflichtung

1. Der Auftragnehmer ist bei der Verarbeitung im Auftrag zur Wahrung der Vertraulichkeit personenbezogener Daten, die er im Zusammenhang mit den Leistungsvereinbarungen verarbeitet und/oder zur Kenntnis erlangt, verpflichtet.
2. Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut zu machen und auf die Vertraulichkeit personenbezogener Daten zu verpflichten. Der Auftragnehmer führt regelmäßige Datenschutzschulungen der Beschäftigten durch.

§ 9 Technische und organisatorische Maßnahmen

1. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Gewährleistung technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.
2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist der **Anlage 2** zu dieser Vereinbarung zu entnehmen. Die Vertragspartner sind sich einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können.
3. Der Auftragnehmer wird wesentliche Änderungen der getroffenen Maßnahmen dokumentieren und dem Auftraggeber auf Anfrage zur Verfügung stellen. Der Auftraggeber ist berechtigt, die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überprüfen oder diese durch einen sachverständigen Dritten überprüfen zu lassen. Es gelten die Bestimmungen des § 6 dieser Vereinbarung.

4. Der Auftragnehmer wird die Nachweise der Einhaltung technisch-organisatorischer Maßnahmen, sowie im Einklang mit § 6 dieser Vereinbarung, auf seiner Webseite veröffentlichten und regelmäßig aktualisieren, soweit diese nach billigem Ermessen und/oder aufgrund einer anderweitigen Verpflichtung des Auftragnehmers zur Veröffentlichung bestimmt sind.

§ 10 Verpflichtungen des Auftragnehmers nach Beendigung

Nach Beendigung der Leistungsvereinbarungen oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarungen – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl und auf Weisung des Auftraggebers an diesen zurückzugeben oder datenschutzkonform zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Etwaige gesetzliche Aufbewahrungspflichten sind von der Löschung ausgenommen. Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit der Leistungsvereinbarung bekannt gewordenen Informationen vertraulich zu behandeln.

§ 11 Haftung und Schadenersatz

1. Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.
2. Macht eine betroffene Person gegenüber einem der Vertragspartner Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.
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 oder zur Aufsichtsbehörde gefährden.

§ 12 Schlussbestimmungen

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

2. Wenn eine Bestimmung dieser Vereinbarung unwirksam sein oder werden sollte, wird dadurch die Wirksamkeit des Vertrages im Übrigen nicht berührt. Es gilt dann eine der unwirksamen Bestimmung dem Sinn und der wirtschaftlichen Bedeutung nach möglichst nahekommende andere Bestimmung zwischen den Parteien als vereinbart.

3. Diese Vereinbarung sowie Änderungen und Ergänzungen der Vereinbarung können sowohl schriftlich als auch in einer geeigneten elektronischen Form geschlossen werden. Wesentliche Änderungen oder Ergänzungen dieser Vereinbarung werden nur wirksam, wenn diese von der Geschäftsführung des Auftragnehmers angenommen oder unterzeichnet werden.

4. Die dem Vertrag beigefügten Anlagen 1 und 2 sind wesentlicher Bestandteil desselben.

5. Auf das Vertragsverhältnis und seine Durchführung findet ausschließlich das Recht der Bundesrepublik Deutschland Anwendung. Für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag gilt – soweit zulässig – die Gerichtsstandvereinbarung des Hauptvertrages.

Anlage 1: Konkretisierung des Auftragsinhalts

Anlage 2: Technische und organisatorische Maßnahmen

Ort, Datum	Ort, Datum
Auftraggeber Name/ Unterschrift/ Firmenstempel	Auftragnehmer Mathias Heese / CEO Claus Müller / CFO Name/ Unterschrift/ Firmenstempel

Konkretisierung der Verarbeitung

1. Gegenstand der Verarbeitung:

Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten durch die Recruiting- und Bewerbermanagement-Software einschließlich der gebuchten Produktbestandteile und Nebenverarbeitungen im weitesten Sinne, die im Auftrag des Auftraggebers verarbeitet werden.

2. Art der Verarbeitung:

Der „Verarbeitung“ wird die Definition des Art. 4 Nr. 2 DSGVO zugrunde gelegt. Umfasst ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solcher Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

3. Zwecke und Konkretisierung der Verarbeitung:

Hauptzwecke der Verarbeitung sind das Recruiting sowie das Bewerbermanagement einschließlich

- der strukturierten Erfassung und Erhebung von Bewerberdaten,
- der strukturierten Darstellung von Bewerberdaten,
- der Kommunikation von Bewerbern, Recruitern und Personalverantwortlichen,
- der Implementierung und Kommunikation von und mit Drittparteien und Kooperationspartnern,
- der Auswertung von Bewerberdaten in Form es Berichtswesens,
- der Bereitstellung eines Talentpools und
- der Abfrage von Feedback bei Bewerbern und über die Software eingestellten Mitarbeitern.

Kategorien betroffener Personen

Folgende Personengruppen sind von der Datenverarbeitung, die im Auftrag durchgeführt wird, betroffen:

- Bewerber des Auftraggebers
- Recruiter, Mitarbeiter und Personalverantwortliche des Auftraggebers
- Arbeitssuchende und Bewerbungsinteressenten

Kategorien personenbezogener Daten

Folgende Kategorien personenbezogener Daten der Bewerber können betroffen sein:

- Persönliche Angaben:
  Anrede, akademischer Grad, Vorname, Nachname, Nationalität, Geburtsdatum etc.
- Kontakt- und Adressdaten:
  Straße, Hausnummer, Postleitzahl, Ort, Land, Bundesland, Telefonnummer, Fax, E-Mail-Adresse etc.
- Bewerbungsdaten:
  Bewerbungsfoto, Anschreiben, Lebenslauf, Berufserfahrung/Arbeitszeugnisse, (Hochschul-)Zeugnisse und andere Qualifikationen, Fahrerlaubnisklasse, Reisebereitschaft etc.
- Account- und Protokolldaten:
  Bewerberaccount, Benutzerkennung, IP-Adresse, Logfiles

- Nutzungsdaten, falls personenbezogen:
  E-Mail-Inhalte, Einladungen, Feedbacks, Bewertungen etc.
- Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO:
  Soweit angegeben/eingewilligt, ein Rückschluss möglich oder aus sachlichen Gründen erforderlich: Ethnische Herkunft, politische Meinung/Parteizugehörigkeit, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugung, genetische/biometrische Daten (z. B. Bewerbungsfoto), Gesundheitsdaten (z. B. Angaben zu einer Schwangerschaft, Angaben zu einer Behinderung oder zu gesundheitlichen Einschränkungen), Angaben zur sexuellen Orientierung (z. B. Geschlecht/Gender, Homosexualität) etc.

Folgende Kategorien personenbezogener Daten von Recruitern, Mitarbeitern und Personalverantwortlichen können betroffen sein:

- Persönliche Angaben:
  Anrede, akademischer Grad, Vorname, Nachname, Funktionsebene, Unternehmen etc.
- Kontaktdaten- und Adressdaten:
  Unternehmenssitz, Telefonnummer, Fax, E-Mail-Adresse etc.
- Account- und Protokolldaten:
  Benutzerkennung, IP-Adresse, Logfiles, Rolle, Protokollierung der Verarbeitung innerhalb des Systems etc.
- Nutzungsdaten:
  Kommentare, E-Mail-Inhalte, Einladungen, Feedbacks, Bewertungen etc.

Standorte der Datenverarbeitung

Verarbeitung im Auftrag findet an folgenden Standorten statt:

softgarden e-recruiting GmbH (Geschäftsräume des Auftragnehmers)

Standort Berlin: Tauentzienstraße 14, 10789 Berlin

Standort Saarbrücken: Europaallee 29, 66113 Saarbrücken

myLoc managed IT AG Am Gatherhof 44 40472 Düsseldorf (Rechenzentrum)

Standorte des Dienstleisters: Am Gatherhof 44 40472 Düsseldorf; In der Steele 40599 Düsseldorf

PlusServer GmbH Welserstraße 14 51149 Köln (Rechenzentrum)

Standorte des Dienstleisters: In der Steele 40599 Düsseldorf; Welsestraße 14 51149 Köln

Weisungsempfangende Personen des Auftragnehmers

Folgende Personen des Auftragnehmers sind berechtigt, Weisungen des Auftraggebers entgegenzunehmen: Team Customer Service: support@softgarden.de

Datenschutzbeauftragter des Auftragnehmers

Der Datenschutzbeauftragte des Auftragnehmers ist:

Marco Tessendorf, procado Consulting, IT- & Medienservice GmbH, Warschauer Str. 58a, 10243 Berlin
Kontakt: ds-softgarden@procado.de

Beauftragte Unterauftragnehmer

Die Bestätigung des Einsatzes von Subunternehmern, bzw. von optionalen und/oder kostenfreien Leistungen, erfolgt i. d. R. über das Recruitingsystem durch ein sog. „Opt-In-Verfahren“ des Nutzers. Um die Bereitstellung und Nutzung der Software nicht von Drittanbieter-Diensten abhängig zu machen, wird der Auftragnehmer dem Auftraggeber zudem die Möglichkeit bieten, Dienste von Drittanbietern im Auftrag des Auftraggebers in das System zu implementieren, die insbesondere über den *Marketplace* des Auftragnehmers und – soweit möglich – auch individuell gebucht werden können.

Name und Anschrift des Unterauftragnehmers	Auftragsinhalt
myLoc managed IT AG Am Gatherhof 44 40472 Düsseldorf	Colocation und Managed Services Rackvermietung und Zurverfügungstellung von • redundanten Firewalls und Loadbalancern • redundanter Stromversorgung mittels Notstromgenerator, USV (n+1 Redundanz) und A/B-Zuführung in den Serverracks • mehrfachen redundante IP-Anbindungen und redundante Netzwerkinfrastruktur • separaten Backup-und Administrationsnetzen • redundanter, energieeffizienter Kühlung (n+1 Redundanz) • dedizierten Servern • SSL-Zertifikaten • Austausch defekter Server-Hardware • sonstigen Support-Tätigkeiten für sämtliche Server-Systeme (z.B. im Rahmen des proaktiven Monitorings)
PlusServer GmbH Welserstraße 14 51149 Köln	
Textkernel B.V. Nieuwendammerkade 26a5 NL-1022 AB Amsterdam (Serverstandort Deutschland)	CV-Parsing (optionales Opt-In) - Konvertieren von hochgeladenen Lebensläufen in strukturierte Form - Nutzung von KI zum Matching Bewerbungsprofile / Job Angebot - Wartungs- und Supportdienstleistungen für den CV-Parsing Service
Cronofy Ltd 9A Beck Street, Nottingham, NG1 1EQ, UK (Serverstandort Deutschland)	Kalenderintegration (optionales Opt-In) - zur Vereinbarung von Meetings, Terminen und Tasks - Verarbeitung von Kalenderstrukturen und Ereignissen

Technische und organisatorische Maßnahmen

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen sind vertraulich zu behandeln. Sie dürfen weder ganz noch auszugsweise vervielfältigt oder an Unbefugte weitergegeben werden.

Abkürzungen

- RZ: Rechenzentren
- B: softgarden Büro Berlin
- SB: softgarden Büro Saarbrücken

Vertraulichkeit

Zutrittskontrolle

softgarden stellt sicher, dass Unbefugte keinen Zutritt zu den Büro-, Server- und Archivräumen haben. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Zentraler Empfangsbereich	X	X	-	
Alarmanalage mit aufgeschaltetem Wachschutz	X	-	-	
Codierte Schlüssel und Schlüsselausgabe nur an Befugte	X	X	X	
Protokollierung von Schließungen	X	X	X	
Festlegung und Dokumentation der Zutrittsberechtigungen	X	X	X	
Dokumentation Zutritt Firmenfremde (z.B. Wartungspersonal, Kunden, Dienstleister, Partner, Besucher ...)	X	X	X	
Betreten der Räumlichkeiten durch Firmenfremde nur in Begleitung eines Mitarbeiters	X	X	X	
Legitimation der Zutrittsberechtigten (Schlüssel, Pin-Code)	X	X	X	
Zwei-Faktor-Authentifizierung beim Zutritt	X	-	-	
Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung	X	X	X	
Sicherheitsbereiche mit unterschiedlichen Zutrittsberechtigungen	X	X	X	

Zugangskontrolle

softgarden verhindert, dass EDV-Systeme von Unbefugten genutzt werden können. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Einrichtung eines Benutzerkontos pro Nutzer	X	X	X	Nutzung von personen-ungebundenen Support-Accounts für Zugriff auf Kundensysteme, Zugangsdaten sind nur berechtigten Mitarbeitern zugänglich

Maßnahmen	RZ	B	SB	Anmerkungen
Authentifikation der mit der Datenverarbeitung befugten Personen durch ein Kennwortverfahren (mit Sonderzeichen, Mindestlänge acht Zeichen, regelmäßiger Wechsel des Kennworts	X	X	X	
Verschlüsselte Speicherung von Passwörtern	X	X	X	
Automatische Sperrung des Benutzerkontos bei mehrfacher fehlerhafter Eingabe der Zugangsdaten	X	X	X	
Automatische Sperrung des Arbeitsplatzes bei Inaktivität	X	X	X	
Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern (Richtlinie/ Arbeitsanweisung)	X	X	X	
Regelmäßige Kontrolle der Gültigkeit von Berechtigungen	X	X	X	
Nutzung von abschließbaren Schränken zur Aufbewahrung von Papierakten	X	X	-	keine Papieraktenlagerung im Büro Saarbrücken
Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk mittels TLS/HTTPS, SSH, VPN (IPSec, openVPN)	X	X	X	
Manuelle Sperrung von Zugangskennungen zu Arbeitsplatzrechnern bei längerer Abwesenheit des entsprechenden Mitarbeiters (30 Tage)	X	X	X	nach Rückkehr müssen die Zugangskennungen wieder manuell durch die IT-Administration entsperrt werden
Zugriffsbeschränkung auf Office WLAN durch MAC-Adressen-Filter	-	-	X	
Betrieb eines Office-Gäste-WLANs für mobile Endgeräte und Besucher	-	X	X	

Zugriffskontrolle

softgarden gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Festlegung von Zugriffsberechtigungen für den Zugriff auf Daten (Erstellung eines Berechtigungskonzeptes)	X	X	X	
Speicherung der Daten auf verschlüsselten Datenträgern	X			
Festlegung von Befugnissen zur Kenntnis, Eingabe, Veränderung und Löschung von Daten, die im Rahmen der Auftragserfüllung durch den Auftragnehmer verarbeitet werden	X	X	X	
Regelmäßige Kontrolle von Zugriffen, der Eingaben, Veränderungen und Löschungen	X	-	-	
Entsorgung nicht mehr benötigter Datenträger (Richtlinie/ Arbeitsanweisung)	X	X	X	
Schriftliche Regelung zum Kopieren von Daten (IT Sicherheitsrichtlinie/ Arbeitsanweisung)	X	X	X	
Vergabe minimaler Berechtigungen (Need-to-know-Prinzip)	X	X	X	

Maßnahmen	RZ	B	SB	Anmerkungen
Keine Vergabe von generischen Passwörtern Gruppenkennungen	X	-	-	Nutzung von personenungebundenen Support-Accounts für Zugriff auf Kundensysteme, Zugangsdaten sind nur berechtigten Mitarbeitern zugänglich
Vermeidung der Konzentration von Funktionen/ Funktionstrennung von Administratorentätigkeiten auf unterschiedliche qualifizierte Personen	X	X	X	
Führen einer Historie durchgeführter administrativer Änderungen	X	X	X	
Zugriff auf die Produktionsinfrastruktur über VPN	-	X	X	

Trennungskontrolle

softgarden gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung; eine logische Trennung der Daten ist ausreichend. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Kennzeichnung der erfassten Daten (Aktenzeichen, ID, Kunden/ Vorgangsnummer)	X	X	X	
Logische Trennung der für unterschiedliche Auftraggeber verarbeiteten Daten Funktionstrennung/ Produktion/ Test	X	X	X	
Logische Trennung der personenbezogenen Daten der jeweiligen Auftraggeber durch Zuordnung zu den jeweiligen Benutzer-Accounts	X	X	X	Softwareseitige Trennung der Mandanten

Integrität

Weitergabekontrolle

softgarden gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Festlegung der zur Übermittlung bzw. den Transport (elektronisch, manuell) befugten Personen	X	X	X	
Prüfung der Daten auf Vollständigkeit nach Datentransport, -übertragung und Datenübermittlung oder -speicherung	X	X	X	Manueller Abgleich mit Checksummen
Implementation von Sicherheitsgateways an den Netzübergabepunkten	X	X	X	
Einsatz eines anerkannten Verschlüsselungsverfahrens, welches sämtliche Kommunikation zwischen dem Bewerber und den Servern des Auftragnehmers verschlüsselt.	X	X	X	
Ein- und ausgehende Datenströme werden durch eine moderne, kaskadiert aufgebaute Firewall-Lösung gefiltert	X	X	X	

Maßnahmen	RZ	B	SB	Anmerkungen
Soweit Datenträger durch Transportunternehmen übermittelt werden, werden die Datenträger nur nach vorheriger Authentisierung des Transportunternehmens weitergegeben.	X	X	X	
Papier- und Datenträger mit personenbezogenen Daten werden durch ein qualifiziertes Entsorgungsunternehmen datenschutzgerecht entsorgt.	X	X	X	
Die vollständige, datenschutzgerechte und dauerhafte Löschung von Datenträgern mit personenbezogenen Daten wird protokolliert. Die Protokolle werden mindestens 12 Monate revisionssicher aufbewahrt.	X	X	X	

Eingabekontrolle

softgarden gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Dokumentation der Zugriffsberechtigungen (Arbeitsanweisung Zugriffsgruppen und Zugriffsberechtigung)	X	X	X	
Erfassung der Tätigkeiten im Rahmen des Auftrags	X	X	X	
Stichprobenartige Kontrolle und Auswertung der Protokolldaten auf Missbrauch	X	-	X	Auswertung Protokolldateien über SysOps Team in Saarbrücken
Vorhaltung einer Historie für alle Nutzer, welche die entsprechenden Anwendungsprogramme zur Verarbeitung der personenbezogenen Daten nutzen, die erfasst, welcher Nutzer wann welche Aktion ausgeführt hat, sofern diese Aktion persönliche Daten modifiziert	X	X	X	Erfassung der Historie in der Anwendung „Just Hire“

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

softgarden gewährleistet, dass personenbezogene Daten gegen zufällige oder vorsätzliche Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Unterbrechungsfreie Stromversorgung (USV)	X	X	X	
Virenschutz (auf den Arbeitsplätzen)	X	X	X	Virenschutz auf Windows Arbeitsplätzen
Virenschutz (auf den Servern)	X	X	X	
Firewall	X	X	X	
Notfallplan	X	X	X	
Georedundante Rechenzentren	X	-	-	
Zentrale Brandmeldeanlage	X	X	-	
Verfügbarkeitsüberwachung (Monitoring)	X	X	X	24/7-Überwachung aller kritischen Systeme durch automatisierte Monitoring-Verfahren

Wiederherstellbarkeit

softgarden gewährleistet die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall durch die folgenden Maßnahmen rasch wiederherzustellen:

Maßnahmen	RZ	B	SB	Anmerkungen
Backup-Verfahren gem. Backupkonzept (täglich, wöchentlich, monatlich)	X	X	X	
Aufbewahrung der Backup-Daten in Datensicherungsschränken, Tresoren, in anderem Brandabschnitt	X	X	X	

Belastbarkeit

softgarden gewährleistet Verfügbarkeit und Belastbarkeit geschäftskritischer Systeme und der Systeme zur Verarbeitung personenbezogener Daten durch folgende technischen und organisatorischen Maßnahmen:

Maßnahmen	RZ	B	SB	Anmerkungen
Virtualisierung und Betrieb in Container-Infrastruktur mit Loadbalancern	X	-	-	
Regelmäßige Penetrationstests der softgarden-Produkte auf Sicherheitsschwachstellen	X	-	-	Getestet werden die softgarden-Produkte in der Umgebung der Rechenzentren. Nicht anwendbar in der Umgebung der Büroräume. Penetrationstests durch Kunden können nach Rücksprache mit softgarden auf der Staging Umgebung durchgeführt werden. Eine Durchführung in der Produktionsumgebung wird nicht erlaubt.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Zur Sicherstellung der Aufrechterhaltung und kontinuierlichen Verbesserung des Datenschutz- und Informationssicherheitsniveaus unterzieht sich softgarden regelmäßig (mindestens jährlich) internen und externen Audits.

softgarden ist zertifiziert nach

- DIN EN ISO 9001:2015
- DIN EN ISO/IEC 27001:2017 einschließlich der Forderungen der Normen ISO/IEC 27017:2015 und ISO/IEC 27018:2019

Datenschutz- und Informationssicherheitsmanagement

softgarden gewährleistet einen Prozess zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO	X	X	X	
Regelmäßige Bewertung des Datenschutzniveaus durch ein Datenschutzteam	X	X	X	
Dritte müssen eine Verschwiegenheitserklärung abgeben.	X	X	X	

Maßnahmen	RZ	B	SB	Anmerkungen
Wenn aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewendet und dokumentiert.	-	X	X	
Es existiert eine definierte Vertreterregelung innerhalb der Funktionsgruppen.	-	X	X	
Regelmäßige Überprüfung des Datenschutz- und Informationssicherheitsmanagementsystems durch interne und externe Audits	X	X	X	

Beurteilung des angemessenen Schutzniveaus (Art. 32 Abs. 2 DS-GVO)

softgarden gewährleistet eine dokumentierte Beurteilung eines angemessenen Schutzniveaus, bezüglich der Risiken, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang - der im Auftrag verarbeiteten personenbezogenen Daten. Dies geschieht durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Durchführung einer Risikoanalyse für die Verarbeitungen personenbezogener Daten	X	X	X	
Erstellung von Schutzbedarfskategorien	X	X	X	
Ausrichtung der Prozesse nach Privacy by Design und Privacy Default	-	X	X	
Durchführung von Datenschutz-Folgenabschätzungen (soweit gesetzlich vorgeschrieben)	X	X	X	

Auftragskontrolle (Art. 32 Abs. 3 und 4 DS-GVO)

softgarden gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und zur Erfüllung des vertraglich definierten Verwendungszweckes verarbeitet werden. Der Auftragnehmer kann dies durch ein gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO nachweisen. Sollte keine Zertifizierung vorliegen, geschieht der Nachweis durch:

Maßnahmen	RZ	B	SB	Anmerkungen
Eindeutige Vertragsgestaltung mit Unterauftragnehmern	X	X	X	
Formalisierung der Auftragserteilung (Formularwesen)	X	X	X	
Regelmäßige Kontrolle der Tätigkeiten	X	X	X	Überwachung der softgarden-Prozesse durch interne Audits
Die Weisungsberechtigten des Auftraggebers und die zur Entgegennahme von Weisungen befugten Personen sind vertraglich definiert, Weisungen erfolgen immer in Textform (z.B. per E-Mail oder Ticketsystem).	X	X	X	
softgarden informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder andere Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers.	X	X	X	
Aufträge werden als Support-Ticket (Mindestangaben: Auftraggeber/ Kunde, Aktion/ Teilauftrag, genaue Spezifikation der Verarbeitungsschritte/-parameter, Bearbeiter, Termine, ggf. Empfänger) erfasst,	X	X	X	

Maßnahmen	RZ	B	SB	Anmerkungen
dort werden die durchgeführten Arbeiten dokumentiert. Es gibt eine eindeutige Zuordnung zwischen Support-Ticketnummer und Kundenauftrag.				

Änderungen der Technischen und Organisatorischen Maßnahmen

softgarden ist bestrebt, die Technischen und Organisatorischen Maßnahmen zum Schutz personenbezogener Daten stetig weiterzuentwickeln. Es wird sichergestellt, dass Änderungen an den TOM nicht zu einer Verringerung des Sicherheitsniveaus führen. softgarden wird die Kunden über wesentliche Änderungen der TOM informieren.