Annex 1: Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem Verantwortlichen	und dem Auftragsverarbeiter
KUNDE (Unternehmen)	softgarden e-recruiting GmbH Tauentzienstraße 14 10789 Berlin
- nachfolgend „**Auftraggeber“** genannt	- nachfolgend „**Auftragnehmer“** genannt -

gemeinsam im Folgenden **Vertragspartner** genannt.

Der Auftragnehmer bietet dem Auftraggeber Leistungen rund um die elektronische Verwaltung und Abwicklung von Bewerbungen über ein Bewerbermanagementsystem (Software-as-a-Service) an und hostet zu diesem Zweck die im Bewerbermanagementsystem gespeicherten Bewerberdaten im Auftrag des Auftraggebers.

§ 1 Allgemeines

1. Im Rahmen des zwischen den Parteien bestehenden Leistungsverhältnisses (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO ist (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrages. Bei etwaigen Widersprüchen gehen die Regelungen dieser Vereinbarung mit all seinen Bestandteilen den Regelungen des zugehörigen Hauptvertrages vor.
2. 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.

§ 2 Gegenstand und Dauer der Verarbeitung

1. Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Auftraggeber-Daten durch den Auftragnehmer im Zusammenhang mit dem Einsatz des Recruiting- und Bewerbermanagementsystems als Software as a Service (SaaS) durch den Auftraggeber.
2. Der Auftragnehmer verarbeitet die personenbezogenen Auftraggeber-Daten während der Dauer des Hauptvertrages im Auftrag und nur nach Weisung des Auftraggebers. Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen werden in **Anlage 1** festgelegt.
3. Die Laufzeit der Vereinbarung zur Auftragsverarbeitung richtet sich nach der Laufzeit des zugehörigen Hauptvertrages (Leistungsvereinbarungen).

§ 3 Weisungsrechte des Auftraggebers

1. 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.

2. Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich oder ggf. unter Einhaltung einer durch den Auftraggeber festgelegten, angemessenen Frist auszuführen und insbesondere personenbezogene Daten auf Weisung des Auftraggebers unverzüglich zu berichtigen, zu löschen oder zu sperren und dies auf Verlangen schriftlich zu bestätigen.
3. 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.
4. Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber den Grund der Verarbeitung und die entsprechenden rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
5. 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.
6. 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.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber ist als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie 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.
3. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen (insbesondere in Bezug auf technische und organisatorische Maßnahmen der Datensicherheit) des Auftragnehmers streng vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 5 Pflichten des Auftragnehmers

1. Soweit sich eine betroffene Person in Wahrnehmung ihrer Rechte aus Kapitel 3 DSGVO (Art. 12 bis 23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32 bis 37 BDSG) unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. 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.
2. 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.
3. Wenn dem Auftragnehmer hinsichtlich der verarbeiteten Auftraggeber-Daten eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt wird („Datenschutzvorfall“), meldet er dies dem Verantwortlichen unverzüglich. Im Rahmen der Meldung gem. Art. 33 Abs. 2 DSGVO teilt der Auftragnehmer dem Auftraggeber nach Möglichkeit den Zeitpunkt sowie Art und Ausmaß des Vorfalls, das betroffene IT-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die daraufhin ergriffenen Maßnahmen mit.

4. 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.

§ 6 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 Auftraggeber-Daten 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.

§ 7 Kontrollrechte des Auftraggebers

1. Der Auftragnehmer räumt dem Auftraggeber ein Kontrollrecht zur Prüfung der Datenverarbeitung sowie Einhaltung dieses Vertrags bzw. des jeweiligen Projektauftrags ein. Insbesondere stellt der Auftragnehmer dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht die Durchführung von Überprüfungen einschließlich Inspektionen. Die Kontrollhandlungen können ebenfalls durch einen zur Geheimhaltung verpflichteten Dritten vorgenommen werden, sofern es sich bei dem Dritten um keinen Konkurrenten des Auftragnehmers handelt.

2. Die Parteien sind sich einig, dass der Auftraggeber eine Überprüfung nach Absatz 1 durchführt, indem er den Auftragnehmer anweist, nach seiner Wahl ein geeignetes Testat, einen Bericht oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditor oder Qualitätsauditor) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001 oder BSI-Grundschutz – („Prüfungsbericht“) vorzulegen. In begründeten Ausnahmen kann der Auftraggeber eigenständige Inspektionen durchführen.

3. Der Auftragnehmer verpflichtet sich, die Durchführung der Kontrollen zu unterstützen. Dies beinhaltet die Gewährung sämtlicher benötigter Zugangs-, Auskunfts- und Einsichtsrechte. Gleiches gilt für öffentliche Kontrollen durch die zuständige Aufsichtsbehörde gemäß den anwendbaren Datenschutzvorschriften.

4. Im Falle von eigenständigen Inspektionen 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 von maximal drei (3) Personentagen hinausgeht und dies mit einem höheren Prüfaufwand oder der Beauftragung externer Dienstleister durch den Auftragnehmer verbunden ist, können die dafür anfallenden Kosten dem Auftraggeber nach den branchenüblichen Stunden- und Tagessätzen in Rechnung gestellt werden.

§ 8 Unterauftragsverhältnisse

1. Der Auftragnehmer darf Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern (Subdienstleister) begründen. Zurzeit beschäftigt der Auftragnehmer die in **Anlage 1** bezeichneten Subdienstleister. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

2. Der Auftragnehmer informiert den Auftraggeber in Textform oder einer geeigneten elektronischen Form immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subdienstleistern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innerhalb von 14 Kalendertagen Einspruch zu erheben, wobei dies nicht ohne wichtigen datenschutzrechtlichen Grund erfolgen darf. Im Fall eines begründeten Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern

die Erbringung der Leistung ohne die beabsichtige Änderung für den Auftragnehmer nicht zumutbar ist – die Leistung gegenüber dem Auftraggeber innerhalb von zwei (2) Wochen nach Zugang des Einspruchs einstellen und den Hauptvertrag fristlos und mit sofortiger Wirkung kündigen. Davon unberührt bleibt ein außerordentliches Kündigungsrecht des Kunden aus wichtigem Grund.

3. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Datenschutzpflichten, auch gegenüber dem Subdienstleister gelten und diesen gem. Art. 28 Abs. 4 DSGVO vor Aufnahme der Tätigkeiten entsprechend im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zu verpflichten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.
4. Ist die Beauftragung eines Subdienstleisters mit einer Übermittlung der Auftraggeber-Daten in ein Land außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraum (EWR) („Drittland“) verbunden, gelten zusätzlich die Vorgaben aus § 9.
5. 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.

§ 9 Übermittlung von Auftraggeber-Daten an Drittländer

1. Die Erbringung der vertraglich vereinbarten Datenverarbeitung im Rahmen der Bereitstellung des Recruiting- und Bewerbermanagementsystem findet grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) statt.
2. Jede Übermittlung der Auftraggeber-Daten in ein Land außerhalb von EU/EWR („**Drittland**“) darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 10 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 gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 11 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. Der Auftragnehmer führt regelmäßig eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch und dokumentiert die Ergebnisse.
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. Änderungen der technisch-organisatorischen Maßnahmen dürfen nicht zu einer Unterschreitung des bestehenden Schutzniveaus führen. Der Auftragnehmer wird wesentliche Änderungen der getroffenen Maßnahmen dokumentieren.
3. Der Auftragnehmer wird die aktuellen technischen und organisatorischen Maßnahmen sowie die Nachweise der Einhaltung technisch-organisatorischer Maßnahmen auf seiner Webseite veröffentlichten und regelmäßig aktualisieren, soweit diese nach billigem Ermessen und/oder aufgrund einer anderweitigen Verpflichtung des Auftragnehmers zur Veröffentlichung bestimmt sind.

§ 12 Verpflichtungen des Auftragnehmers nach Beendigung

1. 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 datenschutzkonform zu löschen oder an diesen zurückzugeben und vorhandene Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für Test- und Ausschussmaterial.
2. Dokumentationen und Protokolle, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 13 Sonderbestimmungen für kirchliche Stellen

1. Sofern es sich bei dem Kunden um eine kirchliche Stelle handelt, die den Bestimmungen des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz) unterliegt, unterwirft sich der Auftragnehmer in Ergänzung zu den Bestimmungen aus diesem Auftragsverarbeitungsvertrag gemäß § 30 Absatz 5 Satz 3 EKD-Datenschutzgesetz der kirchlichen Datenschutzaufsicht. Die Unterwerfung erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz.
2. Sofern es sich bei dem Kunden um eine kirchliche Stelle handelt, die den Bestimmungen des Gesetzes über den Kirchlichen Datenschutz (KDG) unterliegt, beziehen die Parteien die Anwendung des KDG, insbesondere §§ 29 und 31 KDG, sowie die Beachtung der dort getroffenen Vorschriften ausdrücklich in diese Vereinbarung ein.

§ 14 Laufzeit und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

§ 15 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.

§ 16 Schlussbestimmungen

1. Diese Vereinbarung zur Auftragsverarbeitung ist ohne separate Unterschrift mit Abschluss des Hauptvertrages gültig.

2. Diese Vereinbarung zur Auftragsverarbeitung ersetzt alle vorherigen Vereinbarungen, Verträge oder Mitteilungen zwischen dem Auftraggeber und dem Auftragnehmer in Bezug auf die Verarbeitung personenbezogener Daten im Auftrag.

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

4. Bei Widersprüchen zwischen verschiedenen Sprachversionen dieser Vereinbarung ist die deutsche Version maßgeblich.

5. Wenn eine Bestimmung dieser Vereinbarung unwirksam sein oder werden sollte, wird dadurch die Wirksamkeit des Vertrages im Übrigen nicht berührt.

6. Die dieser Vereinbarung zur Auftragsverarbeitung beigefügten Anlagen 1 und 2 sind wesentlicher Bestandteil derselben.

7. 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

	27.03.2026
Ort, Datum	Ort, Datum
	Christian Heuermann Sophia Jenkner
Auftraggeber	Auftragnehmer
Name/ Unterschrift/ Firmenstempel	Name/ Unterschrift
	softgarden e-recruiting GmbH

Anlage 1 zur Vereinbarung zur Datenverarbeitung im Auftrag

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 und Zweck der Verarbeitung:

Im Rahmen der Recruiting- und Bewerbermanagementsoftware finden insbesondere folgende Datenverarbeitungen statt:

- Strukturierte Erfassung und Erhebung von Bewerberdaten,
- Strukturierte Darstellung von Bewerberdaten,
- Kommunikation von Bewerbern, Recruitern und Personalverantwortlichen,
- Implementierung und Kommunikation von und mit Drittparteien und Kooperationspartnern,
- Auswertung von Bewerberdaten in Form des Berichtswesens,
- Bereitstellung von Statusinformationen der Bewerbung an angebundene Jobbörsen,
- Bereitstellung eines Talentpools,
- Verarbeitung von Mitarbeiterdaten im Rahmen des Onboardings (gilt für den Fall, dass die Onboarding Software genutzt wird)
- Abfrage von Feedback bei Bewerbern und über die Software eingestellten Mitarbeitern.
- Wenn vertraglich mit dem Jobboard-Portal vereinbart, Weiterleitung des Quality Signals der Bewerbung

Der Auftraggeber bestimmt selbst, welche zusätzlichen Leistungsmodule über den Marketplace oder die optionalen Leistungen des Auftragnehmers in Anspruch genommen werden. Je nach Leistungsumfang kann daher eine Datenverarbeitung zu anderen als den oben genannten Zwecken stattfinden.

Kategorien betroffener Personen

Der Auftraggeber bestimmt selbst, welche Daten von welchen betroffenen Personengruppen verarbeitet werden.

Üblicherweise sind die folgenden Personengruppen von der Datenverarbeitung betroffen:

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

Kategorien personenbezogener Daten

Der Auftraggeber bestimmt selbst, welche Daten von welchen betroffenen Personengruppen verarbeitet werden.

Üblicherweise werden die folgenden Kategorien personenbezogener Daten von Bewerbern können verarbeitet:

- Persönliche Angaben:

  Anrede, akademischer Grad, Vorname, Nachname, Nationalität, Geburtsdatum
- Kontakt- und Adressdaten:

  Straße, Hausnummer, Postleitzahl, Ort, Land, Bundesland, Telefonnummer, Fax, E-Mail-Adresse

- Bewerbungsdaten:
  Bewerbungsfoto, Anschreiben, Lebenslauf, Berufserfahrung/Arbeitszeugnisse, (Hochschul-)Zeugnisse und andere Qualifikationen, Fahrerlaubnisklasse, Reisebereitschaft
- Account- und Protokolldaten:
  Bewerberaccount, Benutzerkennung, IP-Adresse, Logfiles, Status der Bewerbung
- Nutzungsdaten, falls personenbezogen:
  E-Mail-Inhalte, Einladungen, Feedbacks, Bewertungen
- 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)

Üblicherweise werden die folgenden Kategorien personenbezogener Daten von Recruitern, Mitarbeitern und Personalverantwortlichen können verarbeitet:

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

Standorte der Datenverarbeitung

Die 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

WIIT AG (ehemals myLoc managed IT AG), Am Gatherhof 44 40472 Düsseldorf (Firmensitz)

Standorte des Dienstleisters: Am Gatherhof 44, 40472 Düsseldorf (Rechenzentrum D1)

Equinix Germany GmbH, Rebstöcker Straße 33, 60326 Frankfurt (Firmensitz)

Standort des Dienstleisters: Kruppstraße 121-127, 60388 Frankfurt am Main (Rechenzentrum FR2)

Standort des Dienstleisters: Albertstr. 27, 40233 Düsseldorf (Rechenzentrum DU1)

Weisungsempfangende Personen des Auftragnehmers

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

Datenschutzbeauftragter des Auftragnehmers

Herting Oberbeck Datenschutz GmbH, Hallerstraße 76, 20146 Hamburg
Tel.: +49 40 226 34 56 0; E-Mail: datenschutzbeauftragter@softgarden.de

Beauftragte Subunternehmer

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.

Folgende Subunternehmer werden zum Zeitpunkt des Vertragsschlusses eingesetzt:

Name und Anschrift des Unterauftragnehmers	Auftragsinhalt
WIIT AG (ehemals 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)
Equinix (Germany) GmbH Rebstöcker Straße 33 60326 Frankfurt am Main	• Siehe oben: Zusätzliche Colocation und Managed Services wie oben beschrieben. • Serverstandort ist Kruppstraße, Frankfurt, Deutschland und Albertstraße 27, Düsseldorf, Deutschland.
Cloudflare Inc., 101 Townsend St, San Francisco, CA 94107, USA; Cloudflare Germany GmbH, Rosenthal 7, c/o Mindspace, 80331 München	Bereitstellung DDoS-Schutz/WAF. • Data Localization Suite mit „Regional Services“ und „Metadata Boundary for Customers“ zur Sicherstellung einer Datenlokalisierung auf Deutschland. • Die "Regionalen Dienste" stellen sicher, dass der Endkunden-Content-Traffic sicher an Cloudflare-PoPs innerhalb der von softgarden ausgewählten Region übertragen wird und innerhalb eines Point of Presence (PoP) in dieser definierten Region geprüft wird (Entschlüsselung dieses Contents zur Prüfung und anschließende Neuverschlüsselung). softgarden hat Deutschland als ausgewählte Region gewählt, daher wird der gesamte Datenverkehr des Endkunden ausschließlich auf Servern in Deutschland geprüft und der Datenverkehr des Endkunden wird nicht außerhalb von Deutschland geprüft. Metadata

	Boundary stellt sicher, dass Cloudflare keine Kundenprotokolle, die aus abgedeckten Services stammen, außerhalb der Europäischen Union überträgt.

Folgende Subunternehmer werden zum Zeitpunkt des Vertragsschlusses eingesetzt, sofern **optionale** Zusatzprodukte aktiviert sind:

Textkernel B.V. Nieuwendammerkade 26a5 NL-1022 AB Amsterdam (Serverstandort Deutschland)	CV-Parsing • Konvertieren von hochgeladenen Lebensläufen in strukturierte Form • Wartungs- und Supportdienstleistungen für den CV-Parsing Service
Cronofy B.V. Mr. Treublaan 7, 1097 DP Amsterdam, Niederlande (Serverstandort Deutschland)	Kalenderintegration • zur Vereinbarung von Meetings, Terminen und Tasks • Verarbeitung von Kalenderstrukturen und Ereignissen
360 Dialog GmbH Tölzer Straße 1 82031 Grünwald Deutschland (Serverstandorte Frankfurt, Deutschland und Dublin, Irland)	Produkt „Chat Recruiting und Chat Recruiting Plus“ durch Nutzung einer API zu 360 Dialog GmbH. Versendung einer Bewerbung an WhatsApp, Telegram oder Facebook Messenger, soweit dies gebucht wurde (optionales Modul); Nutzung der Messenger Kommunikation. 360 Dialog verarbeitet zur Bereitstellung des Dienstes die von den Bewerber:innen bei dem jeweiligen Messenger-Dienst hinterlegten personenbezogenen Daten, insbesondere Vor- und Nachname, Endgerät, Profilbild. Darüber hinaus werden die über den Messenger-Dienst übertragenen Nachrichten durch die API in das Recruiting-System übermittelt.

Sofern Sie unsere Produkte und Leistungen per Direktkauf über unsere Website beauftragt haben, sind die oben genannten optionalen Zusatzprodukte standardmäßig **aktiviert**. Sie haben jederzeit die Möglichkeit, gewählte Zusatzoptionen zu deaktivieren. Bitte wenden Sie sich dazu an unseren Support.

Für Kunden, die unsere Leistungen über unseren Vertrieb beziehen/bezogen haben, sind die optionalen Zusatzleistungen weiterhin standardmäßig **deaktiviert** und werden nur auf Anfrage aktiviert.

Anlage 2 zur Vereinbarung zur Datenverarbeitung im Auftrag

Technische und organisatorische Maßnahmen

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen beschreiben den Stand zum Zeitpunkt des Vertragsschlusses. Die Vertragspartner sind sich gemäß § 11 Abs. 2 des Vertrages einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Änderungen der technisch-organisatorischen Maßnahmen dürfen nicht zu einer Unterschreitung des bestehenden Schutzniveaus führen. Eine aktuelle Übersicht der getroffenen technischen und organisatorischen Maßnahmen kann jederzeit auf unserer Website unter https://softgarden.com/de/datenschutz/ abgerufen 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	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 sowie eines grundsätzlichen Admin-Accounts für

Maßnahmen	RZ	B	SB	Anmerkungen
				Zugriff auf Kundensysteme, Zugangsdaten sind nur berechtigten Mitarbeitern zugänglich
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		X	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 und individuelle Verschlüsselung der Dateien (Lebensläufe, Anschreiben, Zeugnisse)	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	

Maßnahmen	RZ	B	SB	Anmerkungen
Schriftliche Regelung zum Kopieren von Daten (IT-Sicherheitsrichtlinie/ Arbeitsanweisung)	X	X	X	
Vergabe minimaler Berechtigungen (Need-to-know-Prinzip)	X	X	X	
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
Implementation von Sicherheitsgateways an den Netzübergabepunkten	X	X	X	
DDoS-Protection/ WAF (Cloudflare)	X			SaaS
Einsatz eines anerkannten Verschlüsselungsverfahrens, welches sämtliche Kommunikation zwischen dem Bewerber und den Servern des Auftragnehmers verschlüsselt.	X	X	X	
Systemseitige Verschlüsselung von mobile Endgeräten (Verschlüsselung der Festplatten)		X	X	Mobile Endgeräten von softgarden-Mitarbeitern

Maßnahmen	RZ	B	SB	Anmerkungen
Ein- und ausgehende Datenströme werden durch eine moderne, kaskadiert aufgebaute Firewall-Lösung gefiltert	X	X	X	
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	
Anlassbezogene Kontrolle und Auswertung der Protokolldaten auf Missbrauch im Verdachtsfall	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	
DDoS-Protection/ WAF (Cloudflare)	X	-	-	SaaS
Georedundante Rechenzentren	X	-	-	
Zentrale Brandmeldeanlage	X	X	-	
Überwachung der Verfügbarkeit (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	n.a.	
Aufbewahrung der Backup-Daten in Datensicherungsschränken, Tresoren, in anderem Brandabschnitt	X	X	n.a.	

Belastbarkeit

softgarden gewährleistet Verfügbarkeit und Belastbarkeit geschäftskritischer Systeme und der Systeme zur Verarbeitung personenbezogener Daten durch folgende technische und organisatorische 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. Die Kosten für die Bereitstellung einer Staging Umgebung werden ggfs. nach branchenüblichen Stundensätzen in Rechnung gestellt.
DDoS-Protection/ WAF (Cloudflare)	X	-	-	SaaS

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	

Maßnahmen	RZ	B	SB	Anmerkungen
Regelmäßige Bewertung des Datenschutzniveaus durch ein Datenschutzteam	X	X	X	
Dritte müssen eine Verschwiegenheitserklärung abgeben.	X	X	X	
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	

Maßnahmen	RZ	B	SB	Anmerkungen
Aufträge werden als Support-Ticket (Mindestangaben: Auftraggeber/ Kunde, Aktion/ Teilauftrag, genaue Spezifikation der Verarbeitungsschritte/-parameter, Bearbeiter, Termine, ggf. Empfänger) erfasst, dort werden die durchgeführten Arbeiten dokumentiert. Es gibt eine eindeutige Zuordnung zwischen Support-Ticketnummer und Kundenauftrag.	X	X	X	

Datenlöschung/ Anonymisierung:

Datenlöschung:

Abgesagte und eingestellte Bewerbungen werden zunächst auf den Status „abgesagt/eingestellt“ gesetzt und in der Standardkonfiguration, sofern nicht anders durch den Auftraggeber eingestellt, 6 Monate nach Absage bzw. Einstellung gelöscht bzw. anonymisiert. Die Anonymisierung der abgesagten Bewerber, die nicht im Talentpool aufgenommen werden wollen, erfolgt automatisch. Eine darüberhinausgehende Löschung/Anonymisierung einzelner Bewerber (z.B. nach Aufforderung durch den Bewerber) erfolgt manuell. Bewerberdaten können auch manuell von Benutzern mit entsprechender Berechtigung gelöscht werden.

Anonymisierung gelöschter Bewerber:

Nach Ablauf der Frist werden die Bewerbungen im softgarden Papierkorb vollständig anonymisiert:

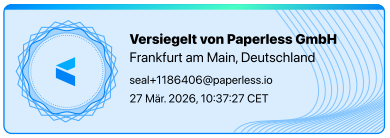
- Alle Anhänge der Bewerbung werden mit einem Dummy-Inhalt überschrieben. Dateiname, Größe und Inhalt werden dabei gelöscht. Lediglich die Tatsache, dass und wie viele Anhänge zu einer Bewerbung vorhanden waren, bleibt für Reportingzwecke erhalten.
- Korrespondenzdaten werden anonymisiert. Dabei werden
    - Anhänge anonymisiert
    - Betreff, Text und HTML, CC und BCC der Nachricht mit einem Blindtext "deleted text" überschrieben
    - bei eingehenden Mails die Absenderadresse und bei ausgehenden die Empfängeradresse mit einer Zufallszeichenkette überschrieben
- Stammdaten der Bewerbung werden anonymisiert
    - alle vom Kunden festgelegten Daten der Bewerbung werden dabei mit einer Zufallszeichenkette überschrieben
- Die Bewerbung wird aus dem Index der Bewerbungssuche entfernt

Wenn die zu löschende Bewerbung die letzte Bewerbung des Bewerberaccounts war, werden zusätzlich folgende Daten mit einer Zufallszeichenkette überschrieben:

- Login-Name
- Passwort
- Vor- und Nachname
- E-Mail-Adresse
- IP-Adresse, von der der Account angelegt wurde
- IP-Adresse, von der die Datenschutzerklärung bestätigt wurde
- Außerdem werden alle Tags des Bewerbers gelöscht

Es gibt die Möglichkeit, dass quantitative Auswertungen zu den Teilnehmern durchgeführt werden, um zu ermitteln, welche Bewerber, an welchem Ort, welches Interesse hatten. Dazu werden die anonymisierten Daten verwendet. Die Anonymisierung ersetzt alle Daten mit Personenbezug durch Blindtexte, so dass ein Rückschluss bzw. eine Identifikation hinterher nicht mehr möglich ist.

Paperless



AUDIT TRAIL

Dokument-Informationen

Vorgangsnummer:
686699

Name:
20260326_DPA_deutsch_Rev_2_11

Eigentümer:
softgarden e-recruiting GmbH

Status: Abgeschlossen

Sprachvariante: de-DE

Zeitzone: UTC+01:00 (Berlin)

Ereignisübersicht

Dokument erstellt von **Sophia Jenkner** (sophia.jenkner@softgarden.de)	27. März 2026, 09:42:08 Uhr
Prozess gestartet von **Sophia Jenkner** (sophia.jenkner@softgarden.de)	27. März 2026, 09:45:44 Uhr
Prozess von allen Beteiligten abgeschlossen	27. März 2026, 10:37:22 Uhr
Dokument und Audit Trail versiegelt	27. März 2026, 10:37:26 Uhr

Beteiligte

Sophia Jenkner (sophia.jenkner@softgarden.de)
Rolle: Versender

Christian Heuermann (christian.heuermann@softgarden.de)
Rolle: Empfänger (Ausfüllen & Unterschreiben)
Email Link gesendet am 27. März 2026 um 09:45:46 Uhr, **zugestellt** am 27. März 2026 um 09:45:49 Uhr
Authentifizierung: Geheimer Link per Email an christian.heuermann@softgarden.de
Geschäftsbedingungen akzeptiert am 27. März 2026 um 10:37:11 Uhr

Sophia Jenkner (sophia.jenkner@softgarden.de)
Rolle: Empfänger (Ausfüllen & Unterschreiben)
Email Link gesendet am 27. März 2026 um 09:45:46 Uhr, **zugestellt** am 27. März 2026 um 09:45:49 Uhr
Authentifizierung: Geheimer Link per Email an sophia.jenkner@softgarden.de
Geschäftsbedingungen akzeptiert am 27. März 2026 um 09:45:45 Uhr

Sitzungen

Sophia Jenkner (sophia.jenkner@softgarden.de)
Zeitraum: 27. März 2026, 09:46:10 Uhr - 27. März 2026, 09:46:11 Uhr
IP Adresse: 2a01:4f8:120:70f6::2
Browser: Chrome 146.0.0.0

27. März 2026, 09:46:10 Uhr	**Daten erfasst**	**Texteingabe:** softgarden e-recruiting GmbH **Unterschrift Sophia Jenkner:**  Unterschrieben am 27.03.2026
27. März 2026, 09:46:11 Uhr	**Abschluss**	Dokument vollständig ausgefüllt, Daten validiert und abgeschlossen

Christian Heuermann (christian.heuermann@softgarden.de)
Zeitraum: 27. März 2026, 10:37:21 Uhr - 27. März 2026, 10:37:22 Uhr
IP Adresse: 78.46.93.69
Browser: Edge 146.0.0.0

27. März 2026, 10:37:21 Uhr	**Daten erfasst**	**Unterschrift Christian Heuermann:**  Unterschrieben am 27.03.2026 **Datum:** 27.03.2026
27. März 2026, 10:37:22 Uhr	**Abschluss**	Dokument vollständig ausgefüllt, Daten validiert und abgeschlossen