***Vom Auftraggeber auszufüllen.***

|  |
| --- |
| Gegenstand des Auftrags |

Der Auftragnehmer erbringt für den Auftraggeber folgende Leistungen:

Nutzung des Bewerbermanagementsystems von softgarden

Umfang, Art und Zweck der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in folgendem Vertrag beschrieben:

<Bezeichnung/ Datum einfügen>

- Erheben von personenbezogenen Daten

- Verarbeitung/ Speicherung von personenbezogenen Daten in den nachfolgenden beschriebenen Rechenzentren,

-Nutzung der Daten zur Kommunikation mit den Bewerbern

- Darstellung der Daten gegenüber dem Auftraggeber, strukturierte Darstellung der Kandidatendaten

- ggf weiterführende Speicherung der Kandidatendaten nach Einwilligung im Talent Pool, Löschung der Daten 6 Monate nach Abschluss des Bewerbungsverfahrens

- sofern der Kandidat nicht der Einwilligung der weiterführenden Speicherung seiner Daten im Talent Pool entsprochen hat

- Auswertung von Kandidatendaten im Rahmen von Berichten,

**Dauer des Auftrags**

Die Dauer dieses Auftrags entspricht der Laufzeit des oben genannten Vertrags.

|  |
| --- |
| Weisungsberechtigte Personen des Auftraggebers |

Der Auftraggeber bestimmt folgenden Personenkreis, der berechtigt ist, Weisungen an den Auftragnehmer zu erteilen: *Bitte Namen und Funktion angeben!*



|  |
| --- |
| Datenschutzbeauftragter des Auftraggebers |

Der Datenschutzbeauftragte des Auftraggebers ist: *Bitte Namen und Kontaktdaten angeben!*



|  |
| --- |
| Kreis der Betroffenen |

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

* Interessenten
* Recruiter
* Bewerber bei der Nutzung des Angebots auf den Webseiten

|  |
| --- |
| Art der Daten/ Datenkategorien |

Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung der personenbezogenen Daten sind folgende Daten bzw. Datenkategorien:

* Kontaktdaten des Bewerbers (Straße, Hausnummer, Postleitzahl, Ort, Land, Bundesland, Tel, Fax, Mobil, E-Mail)
* Persönliche Daten des Bewerbers (Anrede, Akademischer Titel, Vorname, Nachname, Nationalität, Geburtsdatum)
* Bewerbungsanschreiben
* Berufserfahrung des Bewerbers (Unternehmen, Branche, Position, Karrierestufe, Beschäftigungsart, Unternehmensgröße, Homepage, Art des Unternehmens, von, bis, Beschreibung)
* Bildung / Ausbildung des Bewerbers (von, bis, (Hoch-)Schule, Fachrichtung, Abschluss/akad. Grad, Schwerpunkte, Sprachkenntnisse (Sprache, Level))
* Bewerbungsfoto des Bewerbers
* Lebenslauf
* Fahrerlaubnisklasse des Bewerbers
* Reisebereitschaft des Bewerbers
* weitere Anhänge und Angaben gemäß dem bestehenden Dienstleistungsvertrag
* IP-Adresse

***Vom Auftragnehmer auszufüllen!***

|  |
| --- |
| Standorte der Datenverarbeitung |

Die von dem Auftragnehmer ausgeführte Datenverarbeitung findet an folgenden Standorten statt:

**Standort der Geschäftsräume des Auftragnehmers:**

softgarden e-recruiting GmbH

Tauentzienstraße 14

10789 Berlin

**ggf. Standort der Rechenzentren des Auftragnehmers:**

* myLoc managed IT AG Am Gatherhof 44 40472 Düsseldorf
  + RZ-Standorte des Dienstleisters:
    - Am Gatherhof 44 40472 Düsseldorf
    - In der Steele 40599 Düsseldorf
* PlusServer GmbH Welserstraße 14 51149 Köln
  + RZ-Standorte des Dienstleisters:
    - In der Steele 40599 Düsseldorf
    - Welsestraße 14 51149 Köln

Eine Veränderung der Standorte, in denen Daten des Auftraggebers verarbeitet und/ oder genutzt werden, bedarf der schriftlichen Zustimmung des Auftraggebers.

|  |
| --- |
| Weisungsempfangende Personen des Auftragnehmers |

Der Auftragnehmer benennt folgende Personen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind:

* Herr Philipp Mager, Vice President Service

softgarden e-recruiting GmbH, Tauentzienstraße14, 10789 Berlin

|  |
| --- |
| Datenschutzbeauftragter des Auftragnehmers |

Der Datenschutzbeauftragte des Auftragnehmers ist:

Marco Tessendorf, procado Consulting, IT- & Medienservice GmbH

Warschauer Str. 58a

10243 Berlin

|  |
| --- |
| Vereinbarungen zu Unterauftragnehmern |

Zum Zeitpunkt des Vertragsabschlusses bestehen Untervertragsverhältnisse zu folgenden Untervertragsnehmern, die Unterstützungsleistungen im Rahmen des Hauptvertrags erbringen (z.B. Rechenzentren):

|  |  |
| --- | --- |
| Name und Anschrift des Unterauftragnehmers | Auftragsinhalt (kurze Beschreibung der erbrachten Dienstleistung) |
| myLoc managed IT AG Am Gatherhof 44  40472 Düsseldorf | Colocation und Managed Services  Rackvermietung und Zurverfügungstellen von   * redundante Firewalls und Loadbalancer * Redundante Stromversorgung mittels Notstromgenerator, USV(n+1 Redundanz) und A/B-Zuführung in den Serverracks * mehrfache redundante IP-Anbindungen und redundante Netzwerkinfrastruktur * Separate Backup-und Administrationsnetze * Redundante, energieeffiziente Kühlung (n+1 Redundanz) * dedizierte Server * SSL-Zertifikate * Austausch defekter Server-Hardware * sonstigen Support-Tätigkeiten für sämtliche Server-Systeme (z.B. im Rahmen des proaktiven Monitorings) |
| PlusServer GmbH  Welserstraße 14  51149 Köln |

Für die Beauftragung weiterer Unterauftragnehmer zu einem späteren Zeitpunkt ist die **vorherige schriftliche Zustimmung** des Auftraggebers erforderlich.

**Unterauftragnehmer mit Sitz in Deutschland/ EU/ EWR**

Der Auftragnehmer bestätigt, mit den genannten Unterauftragnehmern gesonderte Datenschutzverein­barungen gemäß Art. 28 Abs. 3 DSGVO abgeschlossen zu haben, die den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

Bitte Vertragsart benennen (z.B. EU-Standardvertrag):

* Verträge zur Auftragsdatenverarbeitung bzw. Auftragsverarbeitung:
  + myLoc managed IT AG
  + PlusServer GmbH

|  |
| --- |
| **Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO** |

**Die technischen und organisatorischen Maßnahmen sind bei Vorhandensein eines Rechenzentrums für die Geschäftsräume des Auftragnehmers und das Rechenzentrum gesondert auszufüllen.**

Bitte geben Sie an, welche **konkreten** technischen und organisatorischen Maßnahmen Sie zur Gewährleistung von Datenschutz und Datensicherheit getroffen haben und liefern Sie uns einen Nachweis hierzu.

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind nicht für die Öffentlichkeit bestimmt. Zugriff auf diese Informationen haben nur der betriebliche Datenschutzbeauftragte, die jeweils zuständigen Aufsichtsbehörden zum Datenschutz und die eigenen die dazu befugten Mitarbeiter der jeweiligen datenverarbeitenden Stelle.

**Nach Prüfung durch den Auftraggeber** werden die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen – als Bestandteil des vorliegenden Datenschutzvertrags – verbindlich: Sie sind wie folgt zwischen Auftragnehmer und Auftraggeber festgelegt:

|  |
| --- |
| **Vertraulichkeit** |

**Zutrittskontrolle**

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

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ)[[1]](#footnote-1) des Auftragnehmers) | Anmerkungen |
| Zentraler Empfangsbereich (Empfang) | RZ & O |
| Zugang durch eine Alarmanalage mit aufgeschaltetem Wachschutz | RZ |
| Zugang mit codierten Schlüsseln und Schlüsselausgabe nur an Befugte | RZ & O |
| Festlegung der Zutrittsberechtigten einschließlich ihrer Dokumentation für Mitarbeiter und Firmenfremde (Wartungspersonal, Besucher) / Pförtner, Werkschutz | RZ |
| Firmenfremde, Wartungspersonal und Besucher dürfen nur in Begleitung eines Mitarbeiters die Räumlichkeiten betreten | RZ & O |
| Legitimation der Zutrittsberechtigten (Schlüssel, PinCode) | RZ & O |
| Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung | RZ & O |
| Es existieren Sicherheitsbereiche mit unterschiedlichen Zutrittsberechtigungen | RZ & O |

**Zugangskontrolle**

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

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Einrichtung eines Benutzerkontos pro Nutzer | RZ & O |
| Authentifikation der mit der Datenverarbeitung befugten Personen durch ein Kennwortverfahren (mit Sonderzeichen, Mindestlänge 8 Zeichen, regelmäßiger Wechsel des Kennworts nach 90 Tagen (RZ) 180 Tagen (O)) | RZ & O |
| Automatische Sperrung des Benutzerkontos bei mehrfacher fehlerhafter Eingabe der Zugangsdaten | RZ |
| Automatische Sperrung des Arbeitsplatzes bei Inaktivität | RZ & O |
| Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern (Richtlinie/Arbeitsanweisung) | RZ & O |
| Regelmäßige Kontrolle der Gültigkeit von Berechtigungen | RZ & O |
| Die Nutzung von abschließbaren Schränke zur Aufbewahrung von Papierakten | RZ & O |
| Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk mittels TLS/HTTPS, SSH, VPN (IPSec, openVPN) | RZ & O |
| Zugangskennungen zu Arbeitsplatzrechnern werden bei längerer Abwesenheit des entsprechenden Mitarbeiters (30 Tage) manuell gesperrt und müssen nach Rückkehr wieder manuelle durch die IT-Administration entsperrt werden. | RZ& O |

**Zugriffskontrolle**

Der Auftragnehmer 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:

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Festlegung der Zugriffsberechtigungen für den Zugriff auf Daten (Erstellung eines Berechtigungskonzeptes) | RZ & O |
| Festlegung der Befugnisse zur Kenntnis, Eingabe, Veränderung und Löschung von Daten, die im Rahmen der Auftragserfüllung durch den Auftragnehmer verarbeitet werden | RZ & O |
| Regelmäßige Kontrolle des Zugriffs, Eingabe, Veränderung und Löschung | RZ |
| datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger (Richtlinie / Arbeitsanweisung) | RZ & O |
| Schriftliche Regelung zum Kopieren von Daten (IT Sicherheitsrichtlinie / Arbeitsanweisung) | RZ & O |
| Vergabe minimaler Berechtigungen (Need-to-know -Prinzip) | RZ & O |
| Keine Vergabe von generischen oder Gruppenkennungen oder Passwörtern | RZ & O |
| Vermeidung der Konzentration von Funktionen - Funktionstrennung von Administratorentätigkeiten auf unterschiedliche qualifizierte Personen | RZ & O |
| Führen einer Historie durchgeführter administrativer Änderungen | RZ |

**Trennungskontrolle**

Der Auftragnehmer 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:

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Kennzeichnung der erfassten Daten (Aktenzeichen. ID, Kunden/Vorgangsnummer) | RZ & O |
| Logische Trennung der für unterschiedliche Auftraggeber verarbeiteten Daten Funktionstrennung /Produktion/ Test | RZ & O |
| Die personenbezogenen Daten der jeweiligen Auftraggeber werden durch Zuordnung zu den jeweiligen Benutzeraccounts logisch voneinander getrennt. | O |

|  |
| --- |
| **Integrität** |

**Weitergabekontrolle**

Der Auftragnehmer 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:

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers** (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Festlegung der zur Übermittlung bzw. den Transport (elektronisch, manuell) befugten Personen | RZ & O |
| Prüfung der Daten auf Vollständigkeit nach Datentransport, -übertragung und Datenübermittlung oder -speicherung | RZ |
| Implementation von Sicherheitsgateways an den Netzübergabepunkten | RZ & O |
| Einsatz eines anerkannten Verschlüsselungsverfahrens, welches sämtliche Kommunikation zwischen dem Bewerber und den Servern des Auftragnehmers verschlüsselt. | RZ & O |
| Ein- und ausgehende Datenströme werden durch eine moderne, kaskadiert aufgebaute Firewall-Lösung gefiltert | RZ & O |
| Soweit Datenträger durch Transportunternehmen übermittelt werden, werden die Datenträger nur nach vorheriger Authentisierung des Transportunternehmens weitergegeben. | RZ & O |
| Papier- und Datenträger mit personenbezogenen Daten werden durch ein qualifiziertes Entsorgungsunternehmen datenschutzgerecht entsorgt. | RZ & O |
| Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit personenbezogenen Daten wird protokolliert. Die Protokolle werden mindestens 12 Monate revisionssicher aufbewahrt. | RZ & O |

**Eingabekontrolle**

Der Auftragnehmer 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:

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Führung einer Dokumentation der Zugriffsberechtigungen (Arbeitsanweisung Zugriffsgruppen und Zugriffsberechtigung) | RZ & O |
| Erfassung der Tätigkeiten im Rahmen des Auftrags | RZ & O |
| Stichprobenartige Kontrolle und Auswertung der Protokolldaten auf Missbrauch | RZ |
| Für alle Nutzer, die die entsprechenden Anwendungsprogramme zur Verarbeitung der personenbezogenen Daten nutzen, wird eine Historie vorgehalten, die erfasst, welcher Nutzer wann welche Aktion ausgeführt hat, sofern diese Aktion persönliche Daten modifiziert. | O |

|  |
| --- |
| **Verfügbarkeit und Belastbarkeit** |

**Verfügbarkeitskontrolle**

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

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Unterbrechungsfreie Stromversorgung (USV) | RZ & O |
| Virenschutz (auf den Arbeitsplätzen) | RZ & O |
| Virenschutz (auf den Servern) | RZ & O |
| Firewall | RZ & O |
| Es existiert ein Notfallplan | RZ |

**Wiederherstellbarkeit**

Der Auftragnehmer 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:

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Backup-Verfahren (tägliches Veränderungsbackup, wöchentliches Vollbackup) | RZ & O |
| Aufbewahrung der Backup-Daten in Datensicherungsschränken, Tresoren, im anderen Brandabschnitt | RZ & O |

|  |
| --- |
| **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** |

**Datenschutzmanagement**

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

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Alle Mitarbeiter wurden schriftlich auf das Datengeheimnis (Art. 28 Abs.3 lit.b)) verpflichtet und unterwiesen. | RZ & O |
| Regelmäßige Bewertung des Datenschutz-Niveaus durch die Datenschutz-Gruppe | RZ & O |
| Dritte müssen eine Verschwiegenheitserklärung abgeben | RZ & O |
| Wenn aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewendet und dokumentiert. | O |
| Es existiert eine definierte Vertreterregelung innerhalb der Funktionsgruppen | O |

**Beurteilung des angemessenen Schutzniveaus (Art. 32 Abs. 2 DSGVO)**

Der Auftragnehmer 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:

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Durchführung einer Risikoanalyse für die Verarbeitungen personenbezogener Daten | RZ & O |
| Erstellung von Schutzbedarfskategorien | RZ & O |
| Ausrichtung der Prozesse nach „Privacy by Design & Default“. | O |
| Bei Bedarf die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) | RZ & O |

**Auftragskontrolle (Art. 32 Abs. 3 und 4 DSGVO)**

Der Auftragnehmer 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 Auftraggeber kann dies durch ein gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO nachweisen. Sollte keine Zertifizierung vorliegen geschieht der Nachweis durch:

|  |  |
| --- | --- |
| **Pflichten des Auftragnehmers**  (Geschäftsräume (O) und Rechenzentrum (RZ) des Auftragnehmers) | Anmerkungen |
| Eindeutige Vertragsgestaltung mit Unterauftragnehmern | RZ & O |
| Formalisierung der Auftragserteilung (Formularwesen) | RZ & O |
| Regelmäßige Kontrolle der Tätigkeiten | RZ |
| Die Weisungsberechtigten des Auftraggebers und die zur Entgegennahme von Weisungen befugten Personen sind vertraglich definiert, Weisungen erfolgen immer schriftlich. | RZ & O |
| Der Auftragnehmer informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. | RZ & O |
| 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. | RZ & O |
| Der Auftragnehmer informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. | O |

|  |
| --- |
| **Verpflichtungserklärung zur Umsetzung der  technischen und organisatorischen Maßnahmen** |

Der Auftragnehmer bestätigt, dass er die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten des Auftraggebers – wie in **Anlage 2** beschrieben – vor Beginn der Datenverarbeitung umgesetzt hat. Der Auftragnehmer verpflichtet sich, die Erfüllung dieser Anforderungen für die Dauer der Zusammenarbeit sicherzustellen, regelmäßig zu kontrollieren, zu dokumentieren und auf Nachfrage des Auftraggebers zur Verfügung zu stellen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Ort, Datum |  | Mathias Heese / Geschäftsführer  Martin Behrend / VP Finance  Name des Auftragnehmers/ Unterschrift / Firmenstempel |

1. [↑](#footnote-ref-1)