

Verarbeitung personenbezogener Daten im Auftrag des Kunden durch Stepstone – Auftragsverarbeitungsvertrag (AVV)

Stepstone verarbeitet personenbezogene Daten im Auftrag des Kunden im Sinne des Art. 28 Datenschutzgrundverordnung („DSGVO“) nach den folgenden Bestimmungen. Die vorliegende AVV gilt insoweit für den Kunden, als er die hier beschriebenen Produkte nutzt.

1. Art der Verarbeitung

Die Beschreibung der Verarbeitungen, bei denen Stepstone als Auftragsdatenverarbeiter für den Kunden tätig wird, sowie die von der Verarbeitung betroffenen Personen, die Art der personenbezogenen Daten, der Zweck und die Dauer der Verarbeitung, befinden sich in Anlage 1 zu dieser AVV.

2. Rahmen der Verarbeitung

Stepstone verarbeitet personenbezogenen Daten ausschließlich im Rahmen eines Auftrags und gemäß den dokumentierten Weisungen des Kunden. Es sei denn, es liegt ein Ausnahmefall im Sinne von Art. 28 (3) lit. a DSGVO vor.

3. Ort der Verarbeitung

Die Auftragsverarbeitung erfolgt in Mitgliedsstaaten der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, soweit nicht eine anderweitige Weisung erteilt wurde und eine Übermittlung nach den Regelungen der Art. 44 bis 49 DSGVO zulässig ist. Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Kunden und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO. Der Kunde gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage werden die vom Kunden genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert. Soweit der Kunde eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

4. Pflichten des Kunden als Auftraggeber

Der Kunde ist gemäß Art. 4 Nr. 7 DSGVO Verantwortlicher im datenschutzrechtlichen Sinne für die von Stepstone vertragsgemäß erhobenen und verarbeiteten personenbezogenen Daten. Der Kunde informiert Stepstone unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt. Der Kunde führt ein Verzeichnis für Verarbeitungstätigkeiten gemäß Art. 30 (1) DSGVO.

5. Pflichten von Stepstone als Auftragnehmer

Stepstone informiert den Kunden unverzüglich, wenn Stepstone der Auffassung ist, dass eine Weisung vom Kunden gegen anwendbare Gesetze verstößt. Stepstone darf die Umsetzung der Weisung so lange aussetzen, bis diese vom Kunden als zulässig bestätigt wurde oder abgeändert wurde.

Stepstone hält die Bestimmungen dieser Auftragsverarbeitungsvereinbarung und einschlägige anwendbare Datenschutzrechte, insbesondere der DSGVO, ein. Stepstone trifft geeignete technische und organisatorische Maßnahmen entsprechend den einschlägigen Datenschutzgesetzen, insbesondere deren Art. 32 DSGVO, um die personenbezogenen Daten der Betroffenen und ihre Rechte und Freiheiten unter Berücksichtigung von Implementierungskosten, dem Stand der Technik, Art, Umfang und Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos zu schützen. Diese Schutzmaßnahmen sind in der Übersicht zu technisch-organisatorischen Maßnahmen festgehalten, welche unter Anlage 3 eingesehen werden können. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist Stepstone zur Wirkungsüberprüfung und entsprechender Anpassung bei Fortschritten nach dem Stand der Technik verpflichtet. Alternative Sicherheitsmaßnahmen sind gestattet, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Kunden unverzüglich anzuzeigen. Werden die Maßnahmen so geändert, sodass diese keinen gleichwertigen oder einen höheren Schutz der Daten garantieren können, hat der Kunde nach erfolgloser Erteilung von Weisungen das Recht zur außerordentlichen Kündigung in Bezug auf die nach diesen Zusatzbedingungen zur Auftragsverarbeitung erfassten Leistungen. Gleiches gilt bei unterlassener Anzeige solcher Änderungen.

Stepstone stellt dem Kunden auf Nachfrage die für das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 (1) DSGVO notwendigen Angaben zur Verfügung und führt gemäß Art. 30 (2) bis (5) DSGVO ein eigenes Verzeichnis zu allen Kategorien von im Auftrag von Kunden durchgeführten Tätigkeiten der Verarbeitung. Alle Personen, die

auftragsgemäß auf im Auftrag des Kunden verarbeitete personenbezogene Daten zugreifen können, sind gemäß Art. 28 (3) lit. b DSGVO zur Vertraulichkeit zu verpflichten und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung zu belehren.

Stepstone ist zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage von Stepstone leicht zugänglich hinterlegt.

Stepstone gewährleistet den Schutz der Rechte betroffener Personen und unterstützt den Kunden im notwendigen Umfang bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten gemäß Art. 12 bis 23 DSGVO. Stepstone informiert den Kunden unverzüglich, falls sich ein Betroffener zum Zwecke der Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung seiner personenbezogenen Daten unmittelbar an Stepstone wendet.

Stepstone unterstützt den Kunden bei der Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO und der daraus resultierenden Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO im notwendigen Umfang.

Stepstone unterstützt den Kunden im Hinblick auf die Gewährleistung der Melde- und Benachrichtigungspflichten im Fall von Datenschutzverletzungen im Sinne von Art. 33 und 34 DSGVO. Stepstone unterrichtet den Kunden unverzüglich in Textform bei Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen gemäß Art. 4 Nr. 12 DSGVO im Zusammenhang mit der Datenverarbeitung oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten für den Kunden. Stepstone hat im Benehmen mit dem Kunden angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen, soweit die Datenschutzverletzung in der Verantwortung von Stepstone lag. Bei Ermittlungen der Datenschutzbehörde bei Stepstone, ist der Kunde – soweit diese Ermittlungen den Vertragsgegenstand betreffen – unverzüglich zu informieren.

Für den Fall, dass Stepstone eine Verarbeitung von Daten vom Kunden – einschließlich einer Übermittlung in ein Drittland oder an eine internationale Organisation – beabsichtigt, ohne hierzu vom Kunden angewiesen worden zu sein, d.h. weil Stepstone hierzu entsprechend Art. 28 (3) S. 1 lit. a DSGVO verpflichtet ist, wird Stepstone den Kunden unverzüglich über Zweck, Rechtsgrund und betroffene Daten informieren, soweit und solange Stepstone eine solche Mitteilung nicht gesetzlich untersagt ist.

6. Überprüfungen einschließlich Inspektionen

Stepstone stellt dem Kunden alle erforderlichen Informationen zum Nachweis der in diesem Vertrag niedergelegten Pflichten zur Verfügung. Stepstone ermöglicht dem

Kunden vor Beginn und während der Laufzeit dieser Vereinbarung und nach angemessener vorheriger Ankündigung sowie während der üblichen Geschäftszeiten (9:00–17.00 Uhr) die Durchführung von Überprüfungen, einschließlich Inspektionen nach Maßgabe des Art. 28 (3) lit. h DSGVO. Der Kunde ist berechtigt, sich selbst oder durch geeignete, zur Berufsverschwiegenheit verpflichtete Dritte vor Beginn und während der Auftragsverarbeitung, nach rechtzeitiger Anmeldung in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis dieser Überprüfungen wird jeweils dokumentiert und ist von beiden Parteien zu unterschreiben. Zum Nachweis der technischen und organisatorischen Maßnahmen kann Stepstone auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) vorlegen.

7. Weitere Auftragsverarbeiter

Mit Erteilung des Auftrags werden die im unter untenstehender Anlage 2 abrufbaren Unterauftragnehmerverzeichnis aufgelisteten Unterauftragsverarbeiter genehmigt. Stepstone kann Aufträge an weitere Auftragsverarbeiter (Unterauftragsverarbeiter) vergeben, indem Stepstone den Kunden vorab über die Hinzuziehung oder Ersetzung neuer Unterauftragsverarbeiter durch Mitteilung über die Änderung des Unterauftragsverzeichnisses in Textform informiert und der Kunde binnen 4 Wochen keinen Einspruch erhebt. Im Falle eines Einspruches ist Stepstone berechtigt, die Leistung, einzustellen. Kunden können sich unter https://email.stepstone.com/optiext/optiextension.dll?ID=9%2BD9ftIAomswSBbo8j%2BA7LUArgxz3WqYdqFJx4QacQYBlcWVbWzJkXFqV8mua3oacydyjqk5YR__%2BO für Mitteilungen über Änderungen des Unterauftragnehmerverzeichnisses von Stepstone in Anlage 2 anmelden.

Stepstone hat den Unterauftragsverarbeitern dieselben Datenschutzpflichten aufzuerlegen, die in dieser Auftragsverarbeitungsvereinbarung festgelegt sind, so dass die Verarbeitung den Anforderungen der DSGVO entspricht.

Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

Dienstleistungen, die bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch genommen werden, gelten nicht als

Unterauftragsverarbeiter. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Stepstone ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten vom Kunden auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Überprüfungsmaßnahmen zu ergreifen.

8. Löschung und Rückgabe von personenbezogenen Daten

Stepstone erstellt Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Kunden – spätestens aber mit Beendigung der Leistungsvereinbarung – hat Stepstone sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kunden datenschutzgerecht zu vernichten.

Anlage 1 zur Stepstone Auftragsverarbeitung – Prozessbeschreibung

1. Kommentarfunktion in der Lebenslaufdatenbank

1.1. Beschreibung der Verarbeitung

Stepstone verarbeitet personenbezogene Daten im Auftrag des Kunden, soweit die Kommentarfunktion der Stepstone Lebenslaufdatenbank durch den Kunden genutzt wird. Mithilfe der Lebenslaufdatenbank ist es dem Kunden möglich, Profile von Kandidat*innen einzusehen und insbesondere Kommentare zu den jeweiligen Profilen zu speichern. Nur für den Fall der Nutzung der Kommentarfunktion (Speicherung der jeweiligen Kommentare zu einem Kandidaten*innen Profil), verarbeitet Stepstone personenbezogene Daten im Auftrag des Kunden. Im Übrigen wird festgehalten, dass die weiteren Leistungen im Rahmen der Lebenslaufdatenbank nicht als Auftragsverarbeitung erfolgen, hier stellt Stepstone lediglich die von Kandidat*innen bei Stepstone gespeicherten Inhalte bereit und bleibt datenschutzrechtlich Verantwortlicher. Soweit der Kunde diese Daten nutzt, wird er gegebenenfalls weiterer Verantwortlicher.

1.2. Betroffene Personen

Sind Kandidat*innen, an deren Lebensläufe Kommentare durch den Kunden hinterlegt werden.

1.3. Art der Daten

Es werden solche personenbezogenen Daten über Kandidat*innen verarbeitet, die der Kunde über Kandidat*innen erlangt hat und den Profilen hinzufügt.

1.4. Zweck der Datenverarbeitung

Die Verarbeitung personenbezogener Daten, erfolgt zum Zweck der Organisation des Bewerbungsprozesses und um Kunden das Management bei der Suche von Kandidat*innen zu erleichtern.

1.5. Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Dauer der Nutzung der jeweiligen Dienstleistungen. Entfernen Kandidat*innen ihren Lebenslauf aus der Datenbank, so werden Kommentare zum entsprechenden Lebenslauf gelöscht.

2. Kundencenter

2.1. Beschreibung der Verarbeitung

Im Stepstone Kundencenter kann der Kunde ein Kundenkonto anlegen, auf das auch mehrere User des Kunden zugreifen können. Im Stepstone Kundencenter kann der Kunde Stellenanzeigen anlegen und auf der Stepstone Plattform veröffentlichen. Wenn Kandidat*innen sich auf diese Stellen über die Stepstone-Plattform bewerben, werden diese Bewerbungen an das Stepstone Kundenkonto geschickt, um dort vom Kunden verwaltet zu werden. Im Rahmen dieser Verwaltung kann der Kunde im Kundenkonto Notizen zu den Bewerber*innen anlegen, Organisationszugehörigen des Kunden die Bewerbungen zugänglich machen, Nachrichten versenden, Bewerbungsgespräche vereinbaren, sowie Kandidat*innen ab- und zusagen

2.2. Betroffene Personen

Die Betroffenen sind in diesem Zusammenhang Personen, die sich auf die Stellen der Kunden bewerben und im Stepstone Kundencenter hinterlegt sind oder solche, deren Nutzerprofile die Kunden mit eigenen Kommentaren versehen können, sowie Mitarbeitende des Kunden, die Zugriff oder Zugang zum Kundencenter durch den Kunden erhalten.

2.3. Art der Daten

Im Kundencenter werden die personenbezogenen Daten der Kandidat*innen verarbeitet, die die Kandidat*innen mit ihrer Bewerbung an den Kunden teilen. Darunter fallen insbesondere Name, Kontaktdaten und Lebenslauf, sowie weitere Notizen zu den Kandidat*innen, die die Kunden innerhalb des Stepstone Kundencenters zu den jeweiligen Kandidat*innen anfertigen, sowie der Bewerbungsstatus.

2.4. Zweck der Datenverarbeitung

Die Verarbeitung personenbezogener Daten, erfolgt zum Zweck der Organisation des Bewerbungsprozesses und um Kunden das Management bei der Suche von Kandidat*innen zu erleichtern.

2.5. Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Dauer der Nutzung der jeweiligen Dienstleistungen. In diesem Fall werden die Bewerber*innendaten 3 Monate nach Beendigung des Bewerbungsverfahrens, spätestens jedoch 6 Monate nach Eingang der jeweiligen Bewerbung gelöscht, wenn keine Anhaltspunkte für die Beendigung des Bewerbungsverfahrens vorliegen.

3. Hosted Apply und Appcast Apply

3.1. Beschreibung der Verarbeitung

Stepstone verarbeitet personenbezogene Daten im Auftrag des Kunden, soweit der Kunde die Funktion Hosted Apply oder Appcast Apply nutzt. Bewerber*innen können sich auf Stellen des Kunden, die durch Stepstone unter Nutzung des Teilproduktes Stepstone Programmatic auf anderen Plattformen ausgespielt worden sind, bewerben. Bewerber*innen geben sodann ihre Bewerbungsdaten in eine Eingabemaske ein, die durch Stepstone ausgelesen und dem Kunden übermittelt wird. Sofern der Kunde dem Bewerbungsformular Qualifizierungsfragen („Screening Questions“) hinzufügt, werden diese ebenfalls den Kandidat*innen ausgespielt und die Antworten dem Kunden zur weiteren Verarbeitung übertragen.

3.2. Betroffene Personen

Die Betroffenen sind Personen, die sich auf die Stellen des Kunden bewerben.

3.3. Art der Daten

Die personenbezogenen Daten, die verarbeitet werden, sind die Bewerbungsdaten der Kandidat*innen. Diese umfassen Lebenslauf- und Kontaktdaten, sowie ggf. Screening Questions.

3.4. Zweck der Datenverarbeitung

Gegenstand und Zweck der Verarbeitung besteht in der Übermittlung der Bewerbungen von Kandidat*innen an den Kunden.

3.5. Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Dauer der Nutzung der jeweiligen Dienstleistungen. Die Daten werden gelöscht, sobald der Zweck entfällt und der Löschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen. In diesem Fall endet der Zweck, sobald die Daten an den Kunden übermittelt worden sind.

4. Dashboard Nutzung All Jobs 360

4.1. Beschreibung der Verarbeitung

Stepstone verarbeitet personenbezogene Daten im Auftrag des Kunden, wenn der Kunde das Dashboard benutzt, um das Produkt All Jobs 360 Hire zu nutzen.

4.2. Betroffene Personen

Die Betroffenen sind die Mitarbeitenden des Kunden, die das Dashboard nutzen.

4.3. Art der Daten

Die personenbezogenen Daten, die verarbeitet werden, sind Namen und Geschäftskontaktdaten der Mitarbeitenden des Kunden, die das Dashboard nutzen.

4.4. Zweck der Datenverarbeitung

Gegenstand und Zweck der Verarbeitung besteht in der Organisation der gekauften Produkte im Rahmen von All Jobs 360 Hire in dem zur Verfügung gestellten Dashboard. Zudem ist es für die Zugriffskontrolle und das Autorisierungskonzept notwendig, die Nutzer*innen des Dashboards mit Namen, bzw. E-Mail-Adresse zuordnen zu können.

4.5. Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Dauer der Nutzung der jeweiligen Dienstleistungen. Die Daten werden gelöscht, sobald der Zweck, entfällt und der Löschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen. In diesem Fall entfällt der Zweck, sobald der Kunde sein Kundenkonto löscht oder mitteilt, dass Zugänge einzelner Mitarbeiter*innen entfernt werden sollen.

5. Dashboard Nutzung Talent Finder

5.1. Beschreibung der Verarbeitung

Stepstone verarbeitet personenbezogene Daten im Auftrag des Kunden, wenn der Kunde das Dashboard benutzt, um das Produkt Talent Finder zu nutzen.

5.2. Betroffene Personen

Die Betroffenen sind die Mitarbeitenden des Kunden, die das Dashboard nutzen.

5.3. Art der Daten

Die personenbezogenen Daten, die verarbeitet werden, sind Login-Name, Name und Vorname und E-Mail-Adresse der Mitarbeitenden des Kunden die das Dashboard nutzen, sowie das Datum der getätigten Unlocks.

5.4. Zweck der Datenverarbeitung

Gegenstand und Zweck der Verarbeitung besteht in der Organisation der gekauften Produkte im Rahmen von Talent Finder in dem zur Verfügung gestellten Dashboard. Zudem ist es für die Zugriffskontrolle und das Autorisierungskonzept notwendig, die Nutzer*innen des Dashboards mit Namen, bzw. E-Mail-Adresse zuordnen zu können.

5.5. Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Dauer der Nutzung der jeweiligen Dienstleistungen. Die Daten werden gelöscht, sobald der Zweck, entfällt und der Löschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen. In diesem Fall entfällt der Zweck, sobald der Kunde sein Kundenkonto löscht oder mitteilt, dass Zugänge einzelner Mitarbeiter*innen entfernt werden sollen.

6. Screening Agent

6.1. Beschreibung der Verarbeitung

Stepstone verarbeitet personenbezogene Daten im Auftrag des Kunden, soweit der Kunde das Produkt „Screening Agent (Talent Assessor)“ nutzt. Der Screening Agent ist ein KI-gestützter Service zur strukturierten Darstellung von Bewerbenden anhand der Anforderungen einer konkreten Stellenanzeige. Hierzu werden die in der Stellenanzeige enthaltenen Anforderungen ausgelesen und als „Pflicht-“ bzw. „Kann“-Kriterien klassifiziert; anschließend werden Bewerbungsunterlagen (insb. Lebenslauf) sowie ggf. Antworten auf Screening-Fragen je Anforderung bewertet und ein Ergebnis erzeugt. Zudem können gezielte Rückfragen (Gap Questions) an Bewerber*innen generiert werden, wenn Anforderungen unklar oder nur teilweise erfüllt sind und um dem Kunden strukturierte Nachfragen für den weiteren Auswahlprozess zu ermöglichen.

6.2. Betroffene Personen

Betroffene sind Bewerber*innen, deren Bewerbungsdaten im Rahmen des Screening Agent bewertet werden.

6.3. Art der Daten

Es werden die Bewerbungs- und Profildaten der Bewerber*innen verarbeitet, insbesondere Lebenslauf- und Kontaktdaten sowie ggf. weitere vom Kunden abgefragte Screening-Antworten. Des Weiteren werden Ergebnis- und technische Protokolldaten der Bewertung verarbeitet.

6.4. Zwecke der Datenverarbeitung

Zweck der Verarbeitung ist die Durchführung einer strukturierten, konsistenten Einordnung von Bewerbungen zu einer Stelle sowie die Bereitstellung nachvollziehbarer Ergebnisinformationen. Zudem werden solche Daten verarbeitet, die im Rahmen der KI-Verordnung notwendig sind, um deren Voraussetzungen zu erfüllen. Darunter fallen zum

Beispiel die Dokumentation für die Erklärbarkeit der Ergebnisse oder die Robustheit des KI-Systems.

6.5. Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Dauer der Nutzung der jeweiligen Dienstleistungen und der Speicherung der Bewerber*innendaten im jeweiligen Produkt-/Prozesskontext. Protokoll- und Nachvollziehbarkeitsdaten werden grundsätzlich nur so lange vorgehalten, wie dies zur Speicherung der Bewerber*innendaten bzw. zur Nachvollziehbarkeit einzelner Entscheidungen im Zusammenhang mit der Nutzung erforderlich ist oder es eine gesetzliche Speicherfrist vorsieht. Danach werden sie gelöscht bzw. anonymisiert.

7. Gender Pay Gap Report / Salary-Navigator-Compliance-Modul

7.1. Beschreibung der Verarbeitung

Stepstone verarbeitet personenbezogene Daten im Auftrag des Kunden, soweit der Kunde das Modul „Gender Pay Gap Report“ im Salary Navigator nutzt. Der Kunde lädt Beschäftigungs- und Vergütungsdaten seiner Mitarbeitenden hoch. Stepstone verarbeitet die vom Kunden bereitgestellten Daten unter Einsatz geeigneter Pseudonymisierungs- und statistischer Schutzmaßnahmen, führt statistische Analysen durch und stellt dem Kunden die Ergebnisse als GPG Report zur Verfügung. Hierbei können kleine oder seltene Vergleichsgruppen normalisiert, zusammengefasst oder von einzelnen Auswertungen ausgeschlossen werden. Soweit Stepstone die Daten im Auftrag des Kunden anonymisiert, endet die Auftragsverarbeitung für die hiervon erzeugten anonymen Informationen, sobald die betroffenen Personen unter Berücksichtigung aller Mittel, die nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, nicht oder nicht mehr identifiziert werden können und keine Zuordnung zum beitragenden Kunden möglich ist.

7.2. Betroffene Personen

Betroffen sind Mitarbeitende des Kunden, deren Daten in das Modul hochgeladen oder dort ausgewertet werden.

7.3. Art der Daten

Verarbeitet werden Beschäftigungs- und Vergütungsdaten, insbesondere Geschlecht, Entgelt- und Bonusangaben, Arbeitszeit, Vergleichsgruppe bzw. Jobfamilie, Tätigkeit oder normalisierter Jobtitel, Karrierestufe bzw. Grading, Betriebszugehörigkeit, Berufserfahrung, Ausbildung, Abteilung, Region sowie pseudonymisierte Mitarbeitenden-

IDs. Namen, Kontaktdaten und identifizierende Freitexte sind für die vertragsgemäße Nutzung nicht erforderlich und dürfen nicht bereitgestellt werden. Pseudonymisierte Mitarbeitenden-IDs dürfen verarbeitet werden, soweit dies für die Zuordnung und Bereitstellung der Ergebnisse erforderlich ist.

7.4. Zweck der Datenverarbeitung

Zweck der Verarbeitung ist die Berechnung und Bereitstellung geschlechtsspezifischer Entgeltkennzahlen und des GPG Reports für den Kunden sowie die Durchführung der hierfür erforderlichen Validierungs-, Pseudonymisierungs-, Aggregations- und Anonymisierungsschritte. Personenbezogene oder pseudonymisierte Daten werden nicht für eigene Zwecke von Stepstone, insbesondere nicht für kundenübergreifendes Benchmarking, Modelltraining oder Modellverbesserung, verwendet.

7.5. Dauer der Verarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Dauer der Nutzung des Moduls. Kundenbezogene personenbezogene und pseudonymisierte Daten werden auf dokumentierte Anweisung des Kunden und spätestens nach Beendigung der Leistung gelöscht, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Temporäre Berechnungs- und Zwischendaten werden gelöscht, sobald sie für die Bereitstellung des GPG Reports nicht mehr erforderlich sind. Informationen, die vor einer weiteren Verwendung wirksam anonymisiert wurden, sind keine personenbezogenen Daten und fallen ab diesem Zeitpunkt nicht mehr unter diesen Auftragsverarbeitungsvertrag.

Anlage 2 zur Stepstone Auftragsverarbeitung – Unterauftragnehmersverzeichnis

Die im Folgenden aufgelisteten Unterauftragsverarbeiter von der The Stepstone Group Deutschland GmbH werden bei Erteilung des Auftrags genehmigt.

The Stepstone Group GmbH, Völklinger Str. 1, 40219 Düsseldorf, Deutschland

Leistungen:

- Hosting and damit verbundene Sicherheitsleistungen
- Back-Up Leistungen
- Kundendienst-Unterstützung zur Fehlerbehebung
- Zur Verfügungstellung einer Web-Application Firewall

The Stepstone Group EMEA GmbH, Völklinger Straße 1, 40219 Düsseldorf, Deutschland

Leistungen:

- Hosting and damit verbundene Sicherheitsleistungen
- Back-Up Leistungen
- Kundendienst-Unterstützung zur Fehlerbehebung
- Zurverfügungstellung und Verwaltung des Stepstone Kundencenters, gemäß Ziffer 2 der Anlage 1

The Stepstone Group Belgium NV., Wolstraat 70 Rue aux Laines, 1000 Brussel, Belgien

Leistungen:

- Hosting and damit verbundene Sicherheitsleistungen
- Back-Up Leistungen
- Kundendienst-Unterstützung und Fehlerbehebung

The Stepstone Group Polska sp. z o.o. Domaniewska 50, 02-672 Warschau, Polen

Leistungen:

- Kundendienst-Unterstützung zur Fehlerbehebung

Appcast Inc., 10 Water Street, Lebanon, NH 03766, USA

Leistungen:

Zur Verfügungstellung der Eingabemaske und Übertragung der Bewerbungsdaten und Screening Questions von Kandidat*innen an den Kunden nach Ziffer 3 der Anlage 1.

Zur Verfügungstellung und technische Unterhaltung des Dashboards All Jobs 360 Hire, gemäß Ziffer 4 der Anlage 1.

Anlage 3 zur Stepstone Auftragsverarbeitung – technisch-organisatorischen Maßnahmen

1. Vertraulichkeit (Art. 32 (1) lit. b DSGVO)

1.1. Zutrittskontrolle:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, gewährleistet durch:

Die Datencenter haben eine vielschichtige Sicherheitsstruktur. Die Außenbereiche der Datencenter sind durch Hochsicherheitszäune und Mauern ausgestattet. Die Eingänge sind durch Sicherheitspersonal 24 Stunden, sieben Tage die Woche geschützt. Die Anlagen werden mit Sicherheitskameras überwacht. Zugang zu den Serverräumen ist durch Magnetkarten gesichert. Die Anlagen sind in verschlossenen Serverschränken aufbewahrt. Umfassende Sicherheitsmaßnahmen bestehen auch bei den jeweiligen Stepstone-Standorten. Zutritt ist nur mittels Magnetkarten möglich und Besuchern muss speziell Zutritt gewährt werden.

1.2. Zugangskontrolle:

Keine unbefugte Systembenutzung, gewährleistet durch:

Der Kunde kann ausschließlich auf die in seinem Auftrag verarbeiteten Daten zugreifen, nachdem er sich in den Kundenbereich mit dem von ihm definierten Passwort eingeloggt hat. Stepstone speichert die Log-In Details ausschließlich in verschlüsselter Form. Der Datenfluss zwischen Nutzern und dem System ist standardmäßig Ende-zu-Ende verschlüsselt, wobei das Transport Layer Security (TLS) Protocol genutzt wird. Stepstone hat eine interne Passwortrichtlinie für seine Mitarbeiter, die unter anderem erfordert, dass Passworte mindestens acht Zeichen lang sein und regelmäßig gewechselt werden müssen, nicht identisch oder ähnlich mit dem Benutzernamen sein dürfen, mindestens drei der vier folgenden Zeichen enthalten müssen: i) Großbuchstaben, ii) Kleinbuchstaben, iii) Ziffern, iv) Symbole.

1.3. Zugriffskontrolle:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, gewährleistet durch:

Die Zugriffsrechte des Kunden sind streng begrenzt auf die Daten, die tatsächlich im Auftrag des jeweiligen Kunden verarbeitet werden. Nur spezifisch definiertes Stepstone-Personal kann auf Daten zugreifen, die im Auftrag des Kunden verarbeitet werden, soweit dies im Rahmen von Systemadministration und Kundendienstzwecken auf Anfrage des

Kunden erforderlich ist. Das System protokolliert sämtliche Vorgänge über Datenverarbeitungen im Auftrag des Kunden.

1.4. Trennungskontrolle:

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, gewährleistet durch:

Das Stepstone Kundencenter ist mandantenfähig, so dass jeder einzelne eingeloggte Kunde nur die Daten einsehen kann, die mit seinem Account verbunden sind.

1.5. Pseudonymisierung

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) wird eingesetzt, soweit dies für die jeweilige Leistung geeignet und erforderlich ist. Beim Gender Pay Gap Report werden direkte Identifikatoren nicht vertragsgemäß verarbeitet; Mitarbeitenden-IDs und vergleichbare Zuordnungsmerkmale werden auf das für die Bereitstellung des Reports erforderliche Maß beschränkt. Zusätzlich werden statistische Schutzmaßnahmen wie Normalisierung, Zusammenfassung oder Ausschluss kleiner bzw. seltener Vergleichsgruppen eingesetzt.

2. Integrität (Art. 32 (1) lit. b DSGVO)

2.1.

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, gewährleistet durch: Sämtliche über öffentlich zugängliche Netzwerke gesendete Daten sind Ende-zu-Ende verschlüsselt, wobei das Transport Layer Security (TLS) Protocol genutzt wird

2.2.

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind, gewährleistet durch: Das Stepstone System protokolliert die Aktivitäten eines jeden Log-Ins und Log-Outs sowie jegliche Bearbeitung, Hinzufügung, Veränderung und Löschung von Daten durch den jeweils vornehmenden Nutzer, sowie die Zeit (durch Zeitstempel).

3. Verfügbarkeit und Belastbarkeit (Art. 32 (1) lit. b DSGVO)

3.1.

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, gewährleistet durch:

Antivirusprogramme und Firewalls werden eingesetzt. Die Hosting Umgebung ist mit Feuermeldern, Wasserundichtigkeitsdetektoren und erhöhten Böden ausgestattet. Temperatur und Luftfeuchtigkeit werden konstant überwacht, um vordefinierte Werte einzuhalten. Es besteht eine ununterbrochene Stromversorgung von mindestens 72 Stunden.

3.2.

Rasche Wiederherstellbarkeit (Art. 32 (1) lit. c DSGVO), wird gewährleistet durch

- Back-up Prozeduren;
- Ununterbrochene Stromversorgung (USV);
- Getrennte Speicherung;
- Virenschutz und Firewalls;
- Notfallpläne und Krisenpläne;
- Mitarbeiterschulungen;

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 (1) lit. d DSGVO; Art. 25 (1) DSGVO), wird gewährleistet durch:

4.1.

Stepstone veranstaltet regelmäßige Prüfungen mit externen Dienstleistern, um seine Datensicherheitsstandards und -prozesse zu prüfen. Network Penetration Tests werden regelmäßig durchgeführt.

4.2.

Wir verfolgen und überprüfen Protokolle auf zwei Ebenen, bevor die entsprechende Anfrage unsere Anwendungsserver erreicht. Dies erfolgt auf einer Firewall und einer Web Application Firewall Ebene. Dadurch können wir sämtliche außergewöhnlichen Anfragen auf Datenbereitstellungsebene an die Datenbank analysieren und sperren, und dadurch SQL injection-Versuche unterbinden. Das System selbst protokolliert fehlerhafte Anmeldeversuche, wenn die Anfrage durch Firewall und WAF erfolgte.

4.3.

Unsere Datenschutzmaßnahmen werden kontinuierlich in einem PDCA-Zyklus überprüft.