# Vereinbarung zur Auftragsverarbeitung – Advisory und Activation

## Präambel

StepStone Deutschland GmbH („StepStone“), Völklinger Str.1, 40219 Düsseldorf, Deutschland und der Kunde haben einen Vertrag über Beratungsleistugnen (Advisory und/oder Activation) geschlossen und sind darüber übereingekommen, dass dieser Vertrag zur Auftragsverarbeitung als Anhang zum Hauptvertrag Bestandteil des Hauptvertrages wird. Mit Wirksamkeit des Hauptvertrages tritt insoweit dieser Vertrag in Kraft und Bedarf zur Wirksamkeit keiner weiteren Unterschrift. Rechte und Pflichten aus diesem Vertrag leiten sich nur ab, soweit der Kunde mit StepStone den Hauptvertrag abgeschlossen hat. Für Leistungen, die nicht als Beratungsleistung „Advisory“ oder „Activation“ gekennzeichnet oder benannt sind, ist dieser Vertrag nicht anwendbar.

## 1. Auftragsverarbeitung

1.1. Gemäß der Präambel haben StepStone und der Kunde einen Vertrag über Advisory und/oder Activation Leistungen geschlossen. Gegenstand und Zweck der Verarbeitung richten sich nach dem Statement of Work.

1.2. Unter Advisory versteht man die Entwicklung und Implementierung einer Employer Branding Strategie für den Kunden. Diese Advisory Dienstleistungen beinhalten verschiedene methodische Ansätze wie beispielsweise interne und/oder externe auf den Kunden zugeschnittene Umfragen und Kommunikationsstrategien mit dem Ziel für den Kunden eine Arbeitgebermarke („Employer Value Proposition“) zu entwickeln und zu implementieren. Im Rahmen dieser methodischen Ansätze verarbeitet StepStone für den Kunden personenbezogene Daten im Auftrag.

1.3. Innerhalb "Activation" wird die Arbeitgebermarke neu positioniert und an die ausgewählten Empfänger transportiert. Zu diesem Zwecke können für die Anfertigung relevanten Inhalts unter anderem Fotos und/oder Videos von Mitarbeitern des Kunden, sowie verschiedenste andere Medialeistungen erbracht werden, abhängig von den Kundenwünschen.

1.4. StepStone verarbeitet als Auftragsverarbeiter für den Kunden personenbezogene in der jeweils beschriebenen Art im Auftrag im Sinne des Art. 28 DSGVO unter Beachtung nachfolgender Regelungen und den Regelungen des Statements of Work und dies ausschließlich zu den dort beschriebenen Zwecken.

1.5. Gegenstand und Zweck sowie die Dauer der Auftragsverarbeitung richten sich nach den Regelungen und Laufzeit des Hauptvertrages.

1.6. Die Kategorien der Betroffenen und die Art der personenbezogenen Daten richten sich nach der konkreten gebuchten Leistung und ergeben sich aus dem Appendix 1 des Statement of Work.

1.7. StepStone verarbeitet die personenbezogenen Daten ausschließlich im Rahmen des Auftrages und gemäß den dokumentierten Weisungen des Kunden außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor.

1.8. Die Auftragsverarbeitung erfolgt ausschließlich 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.

## 2. Pflichten des Kunden als Auftraggeber

2.1. Der Kunde ist gemäß Art. 4 Nr. 7 DSGVO Verantwortlicher im datenschutzrechtlichen Sinne für die bei StepStone vertragsgemäß verarbeiteten personenbezogenen Daten.

2.2. Der Kunde informiert StepStone unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2.3. Der Kunde führt ein Verzeichnis für Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO.

## 3. Pflichten von StepStone als Auftragnehmer

3.1. StepStone informiert den Kunden unverzüglich, wenn StepStone der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. StepStone darf die Umsetzung der Weisung solange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde.

3.2. StepStone hält die Bestimmungen dieses Vertrages und einschlägige Datenschutzrechte, einschließlich der DSGVO, ein.

3.3. StepStone trifft geeignete organisatorische und technische Maßnahmen entsprechend den einschlägigen Datenschutzgesetzen, einschließlich der DSGVO und insbesondere deren Art. 32, 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 beiliegenden Übersicht zu technisch-organisatorischen Maßnahmen festgehalten. 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, dass aus der Sicht des Kunden StepStone keinen gleichwertigen oder einen höheren Schutz der Daten garantieren kann, hat der Kunde nach erfolgloser Erteilung von Weisungen das Recht zur außerordentlichen Kündigung in Bezug auf die nach dieser Vereinbarung zur Auftragsverarbeitung erfassten Leistungen. Gleiches gilt bei unterlassener Anzeige solcher Änderungen.

3.4. StepStone stellt dem Kunden die für das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO notwendigen Angaben zur Verfügung und führt gemäß Art. 30 Abs. 2 bis 5 DSGVO ein eigenes Verzeichnis zu allen Kategorien von im Auftrag von Kunden durchgeführten Tätigkeiten der Verarbeitung.

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

3.6. StepStone ist zur Bestellung eines **betrieblichen Datenschutzbeauftragten** verpflichtet und dieser kann jederzeit unter **datenschutz@stepstone.de** kontaktiert werden.

3.7. 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 – 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.

3.8. 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 der Verantwortung von StepStone lag.

3.9. Bei Ermittlungen der Datenschutzbehörde bei StepStone ist der Kunde, soweit diese Ermittlungen den Vertragsgegenstand betreffen, unverzüglich zu informieren.

3.10. 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 Abs. 3 S. 1 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.

3.11. Soweit eine Übermittlung von personenbezogenen Daten des Verantwortlichen in Drittstaaten außerhalb der europäischen Union/EEA vorgesehen ist oder bereits vorgenommen wird und kein Angemessenheitsbeschluss der Europäischen Union gem. Art 45 DSGVO vorliegt, wird StepStone die Daten nur übermitteln, sofern geeignete Garantien vorgesehen sind und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Soweit die Übermittlung

personenbezogener Daten auf dem Abschluss der Standardvertragsklauseln (SCC) der Europäischen Union stützt, wird hiermit vereinbart, dass der Verantwortliche als unabhängiger Inhaber von Rechten und Pflichten diesen Standardvertragsklauseln beitritt (Beitrittsmodell). Es ist dem Verantwortlichen zudem unbenommen die Standardvertragsklauseln mit dem Datenimporteur direkt abzuschließen.

## 4. Überprüfungen einschließlich Inspektionen

4.1. 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 nach angemessener vorherige Ankündigung und während der üblichen Geschäftszeiten (9:00-18.00 Uhr) die Durchführung von Überprüfungen, einschließlich Inspektionen nach Maßgabe des Art. 28 Abs. 3 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.

4.2. 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.

## 5. Weitere Auftragsverarbeiter

5.1. Mit Erteilung des Auftrags werden die im beiliegenden Unterauftragnehmerverzeichnis aufgelisteten Unterauftragsverarbeiter genehmigt. Ferner definieren StepStone und der Kunde im Rahmen des Statement of Work weitere Auftragsnehmer, soweit diese zur Erfüllung der Leistung notwendig sind. 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 Leistungen einzustellen wenn eine Erbringung der vertraglichen Leistung nicht mehr gewährleistet werden kann.

5.2. StepStone hat den Unterauftragsverarbeitern dieselben Datenschutzpflichten aufzuerlegen, die in dieser Vereinbarung zur Auftragsverarbeitung festgelegt sind, so dass die Verarbeitung den Anforderungen der DSGVO entspricht.

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

5.4. 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.

## 6. Löschung und Rückgabe

StepStone löscht sämtliche mit dem Vertrag einhergehenden personenbezogenen Daten drei Monate nach Lieferung der Hauptleistung oder wenn ein legitimer Kontakt des Kunden dies schriftlich (Textform genügt) beauftragt.

## Anlage 1 zur StepStone Auftragsverarbeitung – Unterauftragnehmerverzeichnis

Die im Folgenden aufgelisteten Unterauftragsverarbeiter von StepStone werden bei Erteilung des Auftrags genehmigt.

Universum Communications Sweden AB, Jakobsbergsgatan 22, 111 44 Stockholm, Schweden.
Leistungen: StepStone nutzt Universum für die Durchführung von Befragungen/Studien der beauftragten Hauptleistung. Im Zuge dessen kann Universum, soweit dies für den Auftrag notwendig ist Unternehmenstöchter (Affiliates) einsetzen. Dies können sein:
Universum Communications Sweden Aktiebolag Finland Filial (Branch), 2039587, Espoo, Finnland
Universum Communications Ltd., org. nr. 3121113, London, Vereinigtes Königkreich
Universum Communications Norway A/S (NO), org. nr. 992 297 786, Oslo, Norwegen
Universum Communications Switzerland AG, org. nr. CH270.3.014.025-6, Zürich, Schweiz
Universum Communications SARL, org. nr. FR96 802 026 583, Paris, Frankreich
Universum Communications Pte. Ltd., org. nr. 199502683R, Singapore, Singapur
Universum Communications Inc, org. nr. 134094742, New York, USA
Universum Communications SA (PTY) LTD, org. nr. 2012/166762/07, Johannesburg, Süd Afrika
Universum Business Consulting Shanghai Co. Ltd.91310000674593535E, Shanghai, China
Universum Employer Branding Services GmbH, HRB 10178 B, Berlin, Deutschland Universum Communications Italy S.R.L., org.nr. 11036880968, Milan, Italien

StepStone GmbH, Völklinger Str. 1, 40215 Düsseldorf, Deutschland Leistungen:
– Hosting and damit verbundene Sicherheitsleistungen
– Back-Up Leistungen
– Kundendienst-Unterstützung zur Fehlerbehebung
– Zur Verfügung Stellung einer Web-Application Firewall

StepStone Continental Europe GmbH, Völklinger Straße 1, 40219 Düsseldorf, Deutschland Leistungen:
– Hosting and damit verbundene Sicherheitsleistungen
– Back-Up Leistungen
– Kundendienst-Unterstützung zur Fehlerbehebung

StepStone N.V., Koningsstraat 47 Rue Royale, 1000 Brüssel, Belgien Leistungen:
– Hosting and damit verbundene Sicherheitsleistungen
– Back-Up Leistungen
– Kundendienst-Unterstützung und Fehlerbehebung

StepStone Services sp. z o.o., ul. Domaniewska 50, 02-672 Warschau, Polen Leistungen:
– Kundendienst-Unterstützung zur Fehlerbehebung

## Anlage 2 zur StepStone Auftragsverarbeitung – technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- 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.
- 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 nutzt die Dienste von Akamai als Web Application Firewall für seine Systeme.
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.

- 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.
- 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.
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO): Ist nicht einschlägig, da der Kunde einen nicht-pseudonymisierten Zugriff auf die Daten benötigt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- 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
- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme 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 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, gewährleistet durch:
  Antivirusproramme und Firewalls werden eingesetzt. StepStone nutzt Akamais Dienste als Web Application Firewall für seine Systeme.
  Die Hosting Umgebung ist mit Feuermeldern, Wasserundichtigkeitsdetektoren und erhöhten Böden ausgestattet. Temepratur und Luftfeuchtigkeit werden konstant überwacht, um vordefinierte Werte einzuhalten. Es besteht eine ununterbrochene Stromversorgung von mindestens 72 Stunden.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO), 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 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO), wird gewährleistet durch:

- StepStone veranstaltet regelmäßige Prüfungen mit externen Dienstleistern, um seine Datensicherheitsstandards und-prozesse zu prüfen. Network Penetration Tests werden regelmäßig durchgeführt.
- 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 injectionVersuche unterbinden. Das System selbst protokolliert fehlerhafte Anmeldeversuche, wenn die Anfrage durch Firewall und WAF erfolgte.

- Unsere Datenschutzmaßnahmen werden kontinuierlich in einem PDCA-Zyklus überprüft.

Stand 12. Januar 2023