Data Processing Agreement (DPA) – Advisory and Activation

Preamble

StepStone Deutschland GmbH ("StepStone") Voelklinger Str.1, 40219, Duesseldorf, Germany and the customer entered into a contract about consultancy services ("Advisory" and/or "Activation") and agreed that this data processing agreement shall be deemed as annex of the main contract be part of these. The DPA shall become effective with the signing date of the Main agreement. Rights and duties of these DPA shall only be binding if StepStone and the customer have signed the Main Agreement. Services which are not consultancy services ("Advisory" or "Activation") are not covered under this agreement.

1. Data processing

1.1. According to the preamble StepStone and customer entered into a contract about consultancy services ("Advisory" and /or "Activation"). Context and purpose of data processing are defined within the Statement of Work.

1.2. Advisory is the development and implementation of an employer branding strategy for Client. Advisory includes different methodologies such as internal and external tailored surveys and communication strategies to develop and implement an Employer Value Proposition for Client. Within this methodologies StepStone may process personal data on behalf of the customer.

1.3. Within "Activation", the employer brand is repositioned and conveyed to the selected recipients. For this, service can include the providing and/or creation of photos and videos of the Client's company, its working environment or workplaces, or its employees, depending on the Client's wishes.

1.4. StepStone processes personal data for the purpose specified in the respective clause and in the manner specified in the respective clause on the customer's behalf within the meaning of Article 28 General Data Protection Regulation (GDPR) observing the following provisions.

1.5. Context and purpose, as well the period of this data processing agreement are defined within the main agreement.

1.6. Categories of data subjects as well the type of processed personal data are defined within Annex-1 of the Statement of Work.

1.7. StepStone processes personal data only under a contract and in accordance with the customer's documented instructions unless a derogation within the meaning of Art. 28 (3) (a) GDPR applies.

1.8. The contract of data processing is performed exclusively in Member States of the European Union or in another Contracting State to the Agreement on the European Economic Area unless instructions to the contrary have been issued and transmission is permitted in accordance with the provisions of Art. 44 to 49 GDPR. Upon conclusion of the contract, the instruction is given to transfer personal data to the other processor Akamai Technologies, Inc., 150 Broadway, Cambridge, 02142 MA, USA as part of the measures to be implemented in accordance with Part C, clause 3.3 as provided in section 6 below. This transfer is permitted under Art. 46 (2) lit. c GDPR, since the Standard Contractual Clauses of the European Commission ('EU Model Clauses') has been concluded with Akamai Technologies and the customer entered into the EU Model Clauses already according of that agreement. The customer may also directly enter into the EU Model Clauses with Akamai Technologies. These are available under https://www.akamai.com/de/de/multimedia/documents/akamai/akamai-pre-signed-eu-

standard-contractual-clauses.pdf. Akamai Technologies' Data Protection Officer may be contacted at privacy@akamai.com.

2. Obligations of the customer as client

2.1. Pursuant to Art. 4 No. (7) GDPR, the customer is the controller under data protection law for personal data collected and processed by StepStone in accordance with the terms of the contract.

2.2. The customer shall comprehensively inform StepStone without undue delay if it discovers errors or irregularities with regard to data protection regulations when reviewing the results of the processing.

2.3. The customer shall keep a record of processing activities pursuant to Art. 30 (1) GDPR.

3. Duties of StepStone as processor

3.1. StepStone shall inform the customer without undue delay if StepStone is of the opinion that an instruction from the customer breaches applicable laws. StepStone may suspend implementation of the instruction until it has been confirmed as being permitted or modified by the customer.

3.2. StepStone shall comply with the provisions of this data processing agreement and relevant applicable data protection laws, in particular the GDPR.

3.3. StepStone shall take appropriate organisational and technical measures in accordance with the relevant data protection laws, including the GDPR and in particular Art. 32 thereof, to protect the personal data of the data subjects and their rights and freedoms, taking into account implementation costs, the state of the art, nature, scope and purpose of processing as well as the likelihood of occurrence and severity of the risk. These protective measures are recorded in the overview of technical and organisational measures, which can be referred to in Annex 2. The technical and organisational measures are subject to technical progress and further development. In this respect, StepStone is required to check the effectiveness of the measures and adapt them accordingly as technology progresses. Alternative protective measures are permitted as long as they do not fall below the protective level of the defined measures. Significant changes must be documented and reported to the customer without undue delay. If the measures are changed in such a way that, from the customer's point of view, StepStone cannot guarantee equivalent or higher protection of the data, the customer has the right to extraordinary termination after unsuccessful issuance of instructions with regard to the services covered by these additional conditions for contract data processing. The same applies if notice of such changes is not provided.

3.4. StepStone shall provide the customer with the information necessary for the record of processing activities pursuant to Art. 30 (1) GDPR and shall keep a separate list of all categories of processing activities carried out on behalf of the customer pursuant to Art. 30 (2) to (5) GDPR.

3.5. All persons who can access personal data processed on behalf of the customer in accordance with the customer's contract shall be bound to confidentiality in accordance with Art. 28 (3) (b) GDPR and shall be informed of the special data protection obligations resulting from the contract as well as the existing binding instructions and/or purpose.

3.6. StepStone is required to appoint a company **data protection officer** (DPO). The DPO can be contacted at any time under **datenschutz@stepstone.de.**

3.7. StepStone guarantees protection of data subject rights and supports the customer to the necessary extent in responding to requests to exercise data subject rights pursuant to Art. 12 – 23 GDPR. StepStone shall inform the customer without undue delay if a data subject contacts StepStone directly for the purpose of providing access, rectification, erasure or restricting the processing of their personal data. StepStone shall support the customer in carrying out data protection impact assessments pursuant to Art. 35 GDPR and the resulting consultation of the supervisory authority pursuant to Art. 36 GDPR to the necessary extent. StepStone shall support the customer with regard to compliance with reporting and notification obligations in the event of data protection breaches within the meaning of Art. 33 and 34 GDPR.

3.8. StepStone shall inform the customer in text form without undue delay in the event of operational disruptions, suspected personal data breaches pursuant to Art. 4 No. 12 GDPR in connection with data processing or other irregularities in the processing of the data for the customer. In consultation with the customer, StepStone shall take appropriate measures to secure the data and to minimize possible adverse consequences for data subjects insofar as the personal data breach was StepStone's responsibility.

3.9. In the event that the data protection authorities investigate StepStone, the customer must be informed without undue delay to the extent the investigation relates to the subject matter of the contract.

3.10. In the event that StepStone intends to process data from the customer – including transfer to a third country or an international organisation – without having been instructed to do so by the customer, i.e. because StepStone is required to do so pursuant to Art. 28 (3) first sentence (a) GDPR, StepStone will inform the customer without undue delay of the purpose, legal basis and data concerned, unless and to the extent that such a notification is prohibited by law.

3.11. As far as a transfer of controller's personal data outside of the European Union is planned or is already being carried out by StepStone and no adequacy decision of the European Union according to Art. 45 GDPR is available, StepStone has or will conclude the EU Model Clauses. It is hereby agreed that the data controller as an independent holder of rights and obligations will enter these EU Model Clauses. The data controller is still free to conclude the EU Model Clauses directly with the data importer.

4. Audits including inspections

4.1. StepStone shall provide the customer all necessary information to verify the obligations set out in the contract. StepStone shall permit the customer to conduct audits, including inspections in accordance with Art. 28 (3) (h) GDPR, before the commencement and during the term of this agreement after reasonable prior notice and during normal business hours (9:00-18:00). The customer is entitled to satisfy itself directly, or through suitable third parties bound to professional secrecy, of the observance of the technical and organisational measures before commencement and during contract data processing, after timely notification at the business premises during normal business hours without disturbing the course of business. The result of these audits shall be documented and signed by both parties.

4.2. As verification of the technical and organisational measures, StepStone may also submit current certificates, reports or report extracts from independent bodies (e.g.

auditors, internal auditors, data protection officers, IT security department, data protection auditors, quality auditors) or a suitable certification by IT security or data protection audit (e.g. in accordance with BSI baseline protection).

5. Additional processors

5.1. The subcontractors included in the list of subcontractors available in Annex 1 are approved as subcontractors upon award of the contract. If necessary, to achieve the contractual defined services, StepStone and customer may define further sub processors within the statement of work. StepStone may award contracts to other processors (subcontractors) by informing the customer in advance of the inclusion or replacement of new subcontractors by notification in text form of the change to the subcontractor list, provided the customer does not object within four weeks. If the customer does object, StepStone is entitled to discontinue the service if the contractual agreed service cannot be achieved anymore.

5.2. StepStone will impose the same data protection obligations on the subcontractors as those set out in this data processing agreement, so that the processing complies with the requirements of the GDPR.

5.3. Further outsourcing by the subcontractor requires the express consent of the primary contractor (at least in text form); all contractual provisions in the contract chain must also be imposed on the additional subcontractor.

5.4. Services used by third parties as ancillary services to assist in the execution of the contract processing shall not be deemed to be subprocessors. These include, for example, telecommunications services, maintenance and user service, cleaning staff, inspectors or the disposal of data media. StepStone is, however, required to make appropriate and lawful contractual agreements as well as take control measures with such service providers for the assurance of the protection and security of the customer's data; this also applies to outsourced ancillary services.

6. Erasure and return

StepStone deletes processed personal data according to the service three month after final delivery or if a legitimate point of contact instructs us in writing (text form) to do so.

Annex 1 to StepStone Data Processing Agreement
List of subcontractors

StepStone's subcontractors listed below are deemed to have been approved when the contract is awarded:

Universum Communications Sweden AB, Jakobsbergsgatan 22, 111 44 Stockholm, Schweden.

Services: StepStone uses Universum for the purpose to perform the contractual agreed services. Universum is entitled to use affiliates if necessary, for the contract. These might be:

- Universum Communications Sweden Aktiebolag Finland Filial (Branch), 2039587, Espoo, Finland
- Universum Communications Ltd., org. nr. 3121113, London, Great Britain
- Universum Communications Norway A/S (NO), org. nr. 992 297 786, Oslo, Norway
- Universum Communications Switzerland AG, org. nr. CH270.3.014.025-6, Zurich, Switzerland
- Universum Communications SARL, org. nr. FR96 802 026 583, Paris, France
- Universum Communications Pte. Ltd., org. nr. 199502683R, Singapore, Singapore
- Universum Communications Inc, org. nr. 134094742, New York, USA
- Universum Communications SA (PTY) LTD, org. nr. 2012/166762/07, Johannesburg, South Africa
- Universum Business Consulting Shanghai Co. Ltd.91310000674593535E, Shanghai, China
- Universum Employer Branding Services GmbH, HRB 10178 B, Berlin, Germany
- Universum Communications Italy S.R.L., org.nr. 11036880968, Milan, Italy

StepStone GmbH, Völklinger Str. 1, 40215 Düsseldorf, Germany
Services:

- Hosting and related security services
- Back-up services
- Customer-service troubleshooting support

StepStone Continental Europe GmbH, Völklinger Straße 1, 40219 Düsseldorf, Germany
Services:

- Hosting and related security services
- Back-up services
- Customer-service troubleshooting support

StepStone N.V., Koningsstraat 47 Rue Royale, 1000 Brussels, Belgium
Services:

- Hosting and related security services
- Back-up services
- Customer-service troubleshooting support

StepStone Services sp. z o.o., ul. Domaniewska 50, 02-672 Warsaw, Poland
Services:

- Customer-service troubleshooting support

Akamai Technologies GmbH, Parkring 20-22, 85748 Garching, Germany
Services:

- StepStone uses Akamai as a Web Application Firewall as part of its technical and organisational protection measures and therefore delivers content to website visitors via Akamai in order to protect its systems.

Akamai Technologies, Inc., 150 Broadway, Cambridge, 02142 MA, USA
Services:

- see Akamai Technologies GmbH, Akamai Technologies GmbH uses Akamai Technologies, Inc. as a subcontractor.

Amazon Webservices, Inc., 410 Terry Drive Ave North, WA 98109-5210 Seattle, USA
Services:

- Hosting and related security services (provided exclusively within the EU).

Cammio GmbH, Alexanderstraße 1, 10178 Berlin, Germany
Services:

- StepStone uses Cammio to conduct Video Job Interviews.

Annex 2 to the StepStone Data Processing Agreement Technical and organisational measures

1. Confidentiality (Art. 32 (1) (b) GDPR)

1.1 Physical access control

No unauthorized physical access to the data-processing facilities, ensured as follows:
The data centres have a multi-layered security structure. The exterior areas of the data centres are equipped with high-security fences and walls. The entrances are protected by security personnel 24 hours a day, seven days a week. The facilities are monitored by security cameras. Access to the server rooms is secured by magnetic cards. The systems are stored in locked server cabinets.
Comprehensive security measures are also in place at the respective StepStone sites. Access is only possible by means of magnetic cards and visitors must be granted special access.

1.2 System access control

No unauthorized system use, ensured as follows:
The customer can only access the data processed on its behalf after logging into the customer area using the password it has specified. StepStone only stores the log-in details in encrypted form.
By default, the data flow between users and the system is end-to-end encrypted using the Transport Layer Security (TLS) protocol.
StepStone uses Akamai's services as a Web Application Firewall for its systems.
StepStone has an internal password policy for its employees that requires, among other things, that passwords must be at least eight characters long and be changed regularly, must not be identical or similar to the user name, must contain at least three of the four following characters: i) upper-case letters, ii) lower-case letters, iii) digits, iv) symbols.

1.3 Data access control

No unauthorized reading, copying, changing or removal within the system, ensured as follows:
The data access rights of the customer are strictly limited to the data that is actually

processed on behalf of the respective customer. Only specifically defined StepStone personnel can access data that is processed on behalf of the customer, provided this is required for system administration and customer service purposes at the request of the respective customer.
The system logs all events related to data processing on behalf of the customer.

1.4 Separation control

Separate processing of data collected for different purposes, ensured as follows:
The StepStone Recruiter Space is multi-client capable, so that every logged-in customer can only see the data that is connected to its account.

1.5 Pseudonymisation (Art. 32 (1) (a) GDPR; Art. 25 (1) GDPR)

Not relevant, as the customer requires non-pseudonymised access to the data.

2. Integrity (Art. 32 (1) (b) GDPR)

2.1

No unauthorized reading, copying, changing or removal during electronic transfer or transport, ensured as follows:
All data sent over publicly accessible networks is end-to-end encrypted using the Transport Layer Security (TLS) protocol.

2.2

Determining if and by whom personal data has been entered, modified or removed within data processing systems, ensured as follows:
The StepStone system logs the activities of each log-in and log-out as well as any processing, addition, modification and deletion of data by the respective user, as well as the relevant time (by time stamp).

3. Availability and resilience (Art. 32 (1) (b) GDPR)

3.1

Protection from accidental or intentional destruction or loss, ensured as follows:
Anti-virus programs and firewalls are used. StepStone uses Akamai's services as a Web Application Firewall for its systems. The hosting environment is equipped with fire detectors, water leakage detectors and raised floors. Temperature and humidity are constantly monitored to maintain predefined values. There is an uninterruptible power supply for at least 72 hours.

3.2

Timely restoration (Art. 32 (1) (c) GDPR), ensured by

- Back-up procedures;
- Uninterruptible power supply (UPS);
- Separate storage;
- Virus protection and firewalls;
- Emergency and contingency plans;
- Employee training.

4. Procedures for regular testing, assessment and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR), ensured as follows:

4.1

StepStone organizes regular audits with external service providers to check its data security standards and processes. Network penetration tests are carried out regularly.

4.2

We track and verify protocols on two levels before the request reaches our application servers. This is done on a firewall and a web application firewall level. This allows us to analyze and block any unusual queries to the database at the data provisioning level, preventing SQL injection attempts. The system itself logs incorrect log-in attempts if the request was made through firewall and WAF.

4.3

Our data protection measures are continuously reviewed in a PDCA cycle.

Date: 01.02.2021