Data Processing Agreement – Advisory and Activation

Preamble

StepStone Deutschland GmbH ("StepStone"), Völklinger Str.1, 40219 Düsseldorf, Germany and the customer have entered into an agreement on consultancy services (advisory and/or activation) and agree that this Data Processing Agreement shall be a component of the Main Agreement as an annex to the Main Agreement. To that extent, this Agreement shall take effect on commencement of the Main Agreement and requires no further signature to come into force. Any rights and obligations under this Agreement shall only accrue to the extent that the customer has entered into the Main Agreement with StepStone. This Agreement shall not apply to services that are not labelled or designated "advisory" or "activation" consultancy services.

1. Contract data processing

1.1. In accordance with the recitals, StepStone and the customer have entered into an agreement on advisory and/or activation services. The subject matter and purpose of the processing are based on the Statement of Work.

1.2. Advisory is considered to mean the development and implementation of an employer branding strategy for the customer. These advisory services include a range of methodological approaches such as internal and/or external surveys and communication strategies tailored to the customer with the aim of developing and implementing an employer brand ("employer value proposition") for the customer. These methodological approaches involve StepStone processing personal data on behalf of the customer.

1.3. "Activation" entails a repositioning of the employer brand and communication to the selected recipients. To this end, inter alia photos and/or videos of the customer's employees as well as a range of other media services may be carried out to produce relevant content, depending on the customer's wishes.

1.4. StepStone shall process personal data as a contract data processor on the customer's behalf within the meaning of Art. 28 GDPR in the manner described in the specific case in compliance with the following provisions and the provisions of the Statement of Work and shall do so exclusively for the purposes set down there.

1.5. The object and purpose as well as the duration of the contract data processing are based on the provisions and term of the Main Agreement.

1.6. The categories of data subjects and the type of personal data are based on the specific service booked and derive from Appendix 1 of the Statement of Work.

1.7. StepStone processes personal data exclusively within the scope of the order and in accordance with the documented instructions of the customer unless an exceptional case within the meaning of Article 28(3)(a) GDPR applies.

1.8. Contract data processing is performed exclusively within Member States of the European Union or in another signatory 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 Articles 44 to 49 GDPR.

2. Obligations of the customer as client

2.1. Pursuant to Art. 4(7) GDPR, the customer is the controller under data protection law for personal data processed by StepStone in accordance with the terms of the contract.

2.2. The customer shall inform StepStone immediately and comprehensively 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 contractor

3.1. StepStone shall inform the customer immediately if StepStone is of the opinion that an instruction violates applicable laws. StepStone may suspend implementation of the instruction until it has been confirmed or modified by the customer.

3.2. StepStone shall comply with the provisions of this contract and relevant data protection rights, including 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 Article 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, type, scope and purpose of processing as well as the probability of occurrence and severity of the risk. These protective measures are set down in the accompanying overview of technical and organisational measures. 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 this Data Processing Agreement. 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 order 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 this order as well as the existing binding instructions and/or purpose.

3.6. StepStone is obliged to appoint a **company data protection officer**, who may be contacted at any time at **datenschutz@stepstone.de**.

3.7. StepStone guarantees the protection of the rights of data subjects and supports the customer to the necessary extent in responding to requests for the exercise of rights of data subjects 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 Articles 33 and 34 GDPR.

3.8. StepStone shall immediately inform the customer in text form in the event of operational disruptions, suspected personal data breaches pursuant to Art. 4(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 minimise 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 authority investigates StepStone, the customer must be informed immediately to the extent the investigation relates to the contractual object.

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 obliged to do so pursuant to Art. 28(3)(a) GDPR, StepStone will inform the customer immediately of the purpose, legal basis and data concerned, unless and to the extent that such a notification is prohibited by law.

3.11. If the controller is intending to transfer personal data to third countries outside the European Union/EEA or is already doing so and no adequacy decision from the European Union pursuant to Art. 45 GDPR has been provided, StepStone shall only transfer the data to the extent that suitable guarantees are envisaged and the data subjects may avail themselves of enforceable rights and effective legal remedies. If the transfer of personal data is based on the standard contractual clauses (SCC) of the European Union, it is hereby agreed that the controller shall accede to these standard contractual clauses as the independent holder of rights and obligations (accession model). The controller is additionally free to enter into the standard contractual clauses directly with the data importer.

4. Audits including inspections

4.1. StepStone shall provide the customer with 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 a.m.-6:00 p.m.). 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 Basic Protection).

5. Additional contract data processors

5.1. The sub-contractors included in the enclosed list of sub-contractors are deemed to have been approved as data processing sub-contractors upon award of the contract. Moreover, StepStone and the customer shall define further contractors in the Statement of Work to the extent required to perform the service. StepStone may award contracts to other processors (data processing sub-contractors) by informing the customer in advance of the inclusion or replacement of new sub-contractors by notification in text form of the change to the sub-contractor list, provided the customer does not object within four weeks. If an objection is made, StepStone is entitled to discontinue the services if performance of the contractual service can no longer be guaranteed.

5.2. StepStone will impose the same data protection obligations on the data processing sub-contractors as those set out in this Data Processing Agreement, so that such processing complies with the requirements of GDPR.

5.3. Further outsourcing by the sub-contractor 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 sub-contractor.

5.4. Services used by third parties as ancillary services to assist in the execution of the contract data processing shall not be deemed to be data processing sub-contractors. These include, for example, telecommunications services, maintenance and user service, cleaning staff, inspectors or the disposal of data media. However, StepStone is 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 shall delete all personal data associated with the Agreement three months after delivery of the principal service or if a legitimate contact of the customer so requests in writing (text form is sufficient).

Annex 1 to StepStone Data Processing Agreement – List of sub-contractors

StepStone's data processing sub-contractors listed below are deemed to have been approved when the contract is awarded:

Universum Communications Sweden AB, Jakobsbergsgatan 22, 111 44 Stockholm, Sweden. Services: StepStone deploys Universum to perform surveys/studies concerning the assigned principal service. In the course of this, Universum may deploy affiliates as far as necessary for the assignment. This may include:
Universum Communications Sweden Aktiebolag Finland Filial (Branch), 2039587, Espoo, Finland
Universum Communications Ltd., org. nr. 3121113, London, United Kingdom
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
– Backup services
– Customer service troubleshooting support
– Provision of a web application firewall

StepStone Continental Europe GmbH, Völklinger Straße 1, 40219 Düsseldorf, Germany
Services:
– Hosting and related security services
– Backup services
– Customer service troubleshooting support

StepStone N.V., Koningsstraat 47 Rue Royale, 1000 Brussels, Belgium
Services:
– Hosting and related security services
– Backup services
– Customer service & troubleshooting support

StepStone Services sp. z o.o., ul. Domaniewska 50, 02-672 Warsaw, Poland
Services:
– Customer service troubleshooting support

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

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

- Physical entry control: No unauthorised 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.
- System access control: No unauthorised 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.
- Data access control: No unauthorised 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.
- Separation control: Separate processing of data collected for different purposes, ensured as follows:
  The StepStone Customer Centre is multi-client capable, so that every logged-in customer can only see the data that is connected to its account.
- Pseudonymisation (Art. 32(1)(a)) GDPR; Art. 25(1) GDPR): not relevant, as the customer requires non-pseudonymised access to the data.

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

- Transfer control: No unauthorised 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.
- Input control: Determining if and by whom personal data has been entered, modified or removed within data processing systems, ensured by: 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)

- Availability control: 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.
- Rapid recoverability (Art. 32(1)(c) GDPR) is guaranteed through
- Back-up procedures;
  Uninterruptible power supply (UPS);
  Segregated storage;
  Virus protection and firewalls;
  Contingency plans and crisis planning;
  Employee training.

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

- StepStone organises regular audits with external service providers to check its data security standards and processes. Network penetration tests are carried out regularly.
- We track and verify protocols at 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 analyse and block any unusual queries to the database at the data provisioning level, preventing SQL injection attempts. The system itself logs incorrect log-on attempts if the request was made by firewall and WAF.
- Our data protection measures are continuously reviewed in a PDCA cycle.

Last revised: 12. January 2023