GTC Smartbridge AG, Appendix 1

Data Processing Agreement

Table of contents

1 Preamble

(a) This Data Processing Agreement specifies the obligations of the parties with regard to data protection issues based on the provisions of the European General Data Protection Regulation (GDPR) and the Swiss Federal Data Protection Act (FADP, 2023) and supplements the contractual provisions under the main contract concluded between the parties and the associated General Terms and Conditions of Smartbridge (GTC), which form an integral part of the main contract. This Data Processing Agreement applies to all activities under the main contract in which the customer and Smartbridge process the customer's personal data.

2 Subject, duration and specification of the data processing

(a) The customer is responsible for the ensuring compliance of the data processing itself, including the permissibility of engaging a data processor. Smartbridge processes the customer's data exclusively for the purposes stated in the main contract. Smartbridge reserves the right to fulfil legal, regulatory or official obligations.

(b) The duration of this Data Processing Agreement corresponds with the term of the main contract, unless the provisions of this Data Processing Agreement impose obligations that extend beyond the term of the main contract.

3 Categories of data subjects and personal data

(a) The categories of data subjects and personal data processed by Smartbridge on behalf of the customer as part of the main contract are listed in Annex 1.

4 Scope of application and responsibility

(a) Smartbridge processes personal data on behalf of the customer. This includes activities that are specified in the main contract or the GTC. The customer remains responsible for compliance with data protection laws and decides solely on the purposes and means of processing the personal data that it transfers to Smartbridge ("controller" within the meaning of Art. 4 No. 7 GDPR and Art. 5 lit. j FADP). Within the scope of this Data Processing Agreement, the customer is solely responsible for compliance with the legal provisions of data protection laws, in particular for the lawfulness of data transfer to Smartbridge and for the lawfulness of data processing.

(b) The customer undertakes and guarantees in particular that:

(i) the data processing and the associated instructions to Smartbridge are legally compliant;

(ii) it has obtained any necessary notifications, registrations, regulatory approvals and authorisations for the legally compliant processing of personal data by Smartbridge (including disclosure to Smartbridge).

(iii) it has obtained the legally required consents from the data subjects and has fully complied with its information obligations in this regard, in particular by informing the data subjects about the controller, the purpose of data collection, any justifications for data collection, the category of data recipients, possible transfers of data to third countries, the duration of data storage, the rights of access, rectification and erasure, and the possibility of lodging a complaint with the competent data protection authority. At the customer's request, the consent obtained can be integrated into the Smartbridge application so that the customer has the consents on file at all times.

(c) The customer shall independently take appropriate technical and organisational measures to protect the relevant data in its area of responsibility (e.g. on its own systems, buildings, applications/environments under its operational responsibility). The customer is primarily responsible for compliance with data protection regulations, in particular also for compliance with data protection in the employment context or employee data protection.

(d) The customer’s instructions are initially determined by the main contract and can be amended, supplemented or replaced by the customer in written form or in an electronic format (text form) to Smartbridge’s designated contact. The customer must immediately confirm verbal instructions in writing/text form. Smartbridge will inform the customer immediately if Smartbridge is of the opinion that an instruction violates the GDPR, the FADP or any other applicable data protection laws. In this case, Smartbridge may suspend the implementation of the instruction until it has been confirmed or amended by the customer in writing. Smartbridge may assume that the customer's instructions in connection with the allocation of access authorisations or the disclosure of relevant data to the customer are legally compliant.

(e) If such instructions lead to additional costs for Smartbridge or a change in the scope of services, the parties are obliged to enter into a corresponding addendum to the main contract.

5 Duties of Smartbridge

(a) Data protection and data security are top priorities for Smartbridge. Smartbridge strictly adheres to the applicable data protection laws in Switzerland. Smartbridge has designed its internal organisation in such a way that it meets the requirements of the FAPD. Smartbridge has taken technical and organisational measures to ensure the continuous confidentiality, integrity, availability and resilience of the systems and services in connection with data processing. These measures are described in detail in Annex 2. The customer is aware of these technical and organisational

measures and is responsible for ensuring that they offer an appropriate level of protection for the risks of the processed data.

(b) Smartbridge reserves the right to change the security measures taken, however, while ensuring that the contractually agreed upon level of protection is upheld. Smartbridge will inform the customer of any significant changes that Smartbridge assumes could be of interest to the customer, e.g. because they have an impact on the customer's usage or result in the customer having to make adjustments.

(c) If specifically agreed, Smartbridge supports the customer within its possibilities in fulfilling the requests and claims of data subjects in accordance with Chapter III of the GDPR and in complying with the obligations specified in Art. 33 to 36 GDPR and the respective provisions under the FADP. Smartbridge will invoice the customer separately for such additional efforts in accordance with its applicable rates.

(d) Smartbridge ensures that the employees involved in the processing of the customer's data and other individuals working for Smartbridge are prohibited from processing the data beyond the instructions provided by the customer. Furthermore, Smartbridge ensures that the persons authorised to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal confidentiality obligation. The confidentiality/secrecy obligation continues to exist even after the termination of this Data Processing Agreement.

(e) Smartbridge informs the customer immediately if Smartbridge or a subcontractor becomes aware of a data breach affecting the customer's personal data. Smartbridge informs the customer in an appropriate manner about the type and extent of the data breach as well as possible remedial measures in order for the customer to comply with its obligations in the context of data breach, in particular notification obligations. In such a case, the parties will take the necessary measures to ensure the protection of the relevant data and to minimise possible negative consequences for the affected data subjects.

(f) Smartbridge provides the customer with the contact person for data protection issues.

(g) Smartbridge ensures the implementation of procedures to regularly review the effectiveness of the technical and organisational measures to safeguard the security of the data processing.

(h) Smartbridge corrects or deletes the relevant data if instructed to do so by the customer and if this is covered by the customer’s instruction right. Smartbridge will invoice the customer for additional efforts in accordance with its applicable rates.

(i) Data, data carriers and all other materials must either be returned or deleted at the customer's request and expense after the termination or expiry of this Data Processing Agreement. Smartbridge utilises industry-standard procedures.

(j) In the event of a claim being asserted against the customer by a data subject in accordance with Art. 82 GDPR or Art. 28 Civil Code, Smartbridge undertakes to support the customer at the customer's expense in the defence of the claim within its possibilities.

6 Obligations of the customer

(a) The customer must inform Smartbridge immediately and comprehensively if it discovers errors or irregularities regarding data protection during the provision of services agreed under the main contract.

(b) The customer designates a contact person for Smartbridge for all data protection issues arising under the main contract (see GTC section "Notifications").

7 Enquiries from affected persons

(a) If a data subject contacts Smartbridge with requests for correction, deletion or information, Smartbridge will refer the data subject to the customer, provided that the information provided by the data subject suffice to identify the customer as the controller. Smartbridge immediately forwards the data subject's request to the customer. Smartbridge supports the customer within its possibilities in such data subject rights requests. Smartbridge cannot be held liable if the request of the data subject is not answered by the customer, not answered correctly or not answered in a timely manner.

8 Audit / Inspection

(a) Upon request, Smartbridge will provide the customer with suitable evidence of compliance with the obligations set out in this Data Processing Agreement.

(b) Should audits at Smartbridge’s premises by the customer or an independent external auditor engaged by the customer be necessary in individual cases, these will be carried out during normal business hours after prior notification and with a reasonable lead time and without disrupting Smartbridge's business operations. Smartbridge may make an audit dependent on advance notification with an appropriate lead time as well as the signing of a confidentiality agreement issued by Smartbrigde. Should the auditor engaged by the customer be in a competitive relationship with Smartbridge, Smartbridge has the right to object.

(c) The customer provides Smartbridge with a copy of the engaged auditor's audit report.

(d) The time & efforts for Smartbridge in the context of an audit shall be limited to one day per calendar year. Smartbridge is entitled to charge a fee for the support provided during the audit.

(e) Should a data protection supervisory authority or another competent supervisory authority of the customer carry out an inspection, section 8(b) shall apply accordingly. It is not necessary to sign a non-disclosure agreement if this supervisory authority is subject to a professional or statutory confidentiality obligation where a breach is sanctioned by law.

9 Subcontractors (subprocessors)

(a) For the provision of the contractually agreed services, Smartbridge may engage the subcontractors listed in Annex 3.

(b) Smartbridge shall inform the customer via e-mail of any intended changes regarding new subcontractors or the replacement of subcontractors listed in Annex 3. To this end, the customer must register in Smartbridge's information system which Smartbridge introduces the customer to within onboarding. The customer can object to such changes of subcontractors within 30 days of notification. In this case, the main contract and this Data Processing Agreement will be deemed terminated as per the date the new subcontractor shall begin performing its services to Smartbridge.

(c) Smartbridge shall contractually oblige its subcontractors to fulfil their obligations as regards data protection in accordance with this Data Processing Agreement. In particular, Smartbridge will provide sufficient guarantees that the appropriate technical and organisational measures are implemented in such a way that the processing is carried out in accordance with the relevant data protection and the main contract.

10 Place of data processing

(a) Data processing activities must generally take place in Switzerland and/or the European Economic Area (EEA). Data processing activities outside this area are only permitted if the requirements of this Data Processing Agreement are met and suitable measures have been taken in advance to comply with the legal requirements. Specifically, there must be an adequacy decision by the competent authority. In the absence of such a decision, the transfer of personal data must take place on the basis of suitable guarantees (in particular standard contractual clauses approved by the European Commission and the Federal Data Protection and Information Commissioner [FDPIC]) or there are exceptions for certain situations (contract processing, legal enforcement abroad, etc.).

11 Written form clause, choice of law

(a) Amendments and additions to this Data Processing Agreement require a written agreement (which can also be in an electronic format (text form)) and an express reference to the fact that it is an amendment or addition to these terms and conditions. This also applies to the waiver of this formal requirement.

(b) In the event of any contradictions, the provisions of this Data Processing Agreement shall take precedence over the provisions of the main contract. Should individual parts of this Data Processing Agreement be invalid, this shall not affect the validity of the remainder of this Data Processing Agreement.

(c) Swiss law applies.

Annex 1: Categories of data subjects and personal data

The following categories of persons are affected as part of data processing in accordance with the main contract:

(d) Personnel who are to be placed or whose deployment is to be planned via a Smartbridge application;

(e) Other individuals working for the customer;

(f) Customers and interested parties of the customer.

The following categories of personal data are processed as part of data processing:

(a) Master data, names, address data, e-mail addresses, telephone numbers;

(b) Photos, employment contracts and related documents such as CVs, references and training certificates, assessments;

(c) Wage-related data, bank details and other wage and financial data.

Annex 2: Technical and organisational data protection measures (TOM)

Smartbridge undertakes to implement the following technical and organisational measures when processing personal data and to adapt them to the current state of the art.

1 Access controls

The following measures ensure that unauthorised persons do not gain access to the facilities where personal data is processed:

(a) Access to Smartbridge's premises is only possible with a contactless and personalised chip card. Two security doors (main entrance and office entrance) can only be opened with a chip card.

(b) Access controls at the data centres are carried out in accordance with the provisions of the subcontractors used, see section 9 of the Data Processing Agreement.

2 Physical availability assurance

(a) Availability is ensured in accordance with the provisions of the subcontractors engaged, see section 9 of the Data Processing Agreement.

(b) Smartbridge does not have root access to the AWS infrastructure, which is based on the principle of least privilege (PoLP) and is limited to the privileges that the development team needs to carry out their tasks.

3 Authorisations

(a) The following technical measures ensure that unauthorised processing is prevented:

3.1 Authentication

(a) Access to the infrastructure on Staffcloud is controlled by Skaylink in accordance with their GTC (see section 9 of the Data Processing Agreement). Developers and employees of Smartbridge only have the privileges necessary to do their work (PoLP):

(i) User ID and password are required on all computers and servers;

(ii) Access to customer servers as root is only possible with a personal certificate and from a defined jump hosts. Only people with an authorised account (username/password) who can also identify themselves with a certificate or OneTimeToken have access to the jump hosts;

(iii) Server management via SSH.

(b) In addition, a user ID and password are always required for access to computers and servers on Smartbridge premises. The network on Smartbridge's premises is also protected by a firewall.

(c) Customer authentication for Staffcloud login: 2-factor authentication is supported.

(d) Staffcloud is not a public platform. All areas (customer or employee area) are only accessible via authentication.

3.2 Authorisation concepts

(a) Registration, allocation of rights and assignment of rights for administrators are separated at process level.

(b) Access to customer data is only possible using special support accesses, where all processing procedures are logged.

4 Transfer control and encryption

(a) All data, including personal data, is encrypted at rest and during transmission in accordance with the state of the art.

5 Separation control

(a) The databases of different customers are separate.

6 Traceability

(a) Log data allows the subsequent control of all accesses to and transmissions of personal data of customers and their assignment to the corresponding employee.

(b) The log data is stored for 90 days.

(c) The log files are provided with a time stamp and are only accessible via SSH with an authorised SSL key.

(d) The application is hosted on Linux machines so that various actions such as authentication attempts, Sudo access and SSH logins are logged.

(e) Based on the principle of least privilege (PoLP), users have no rights to modify or delete system resources, including log files.

(f) Based on logs and other resources, monitoring systems are in place to detect possible suspicious activities and to report and prevent them.

7 Contractual obligations of employees

(a) Access by authorised persons is restricted to the personal data they need to fulfil their task. Among other things (in addition to the measures under section 3 above) with the following measures:

(i) Written commitment of employees to comply with data protection and data confidentiality in accordance with section 3 above; Smartbridge has drawn up and documented an information security policy and an acceptable use policy, both of which are approved by the management and passed on to all employees in accordance with ISO 27002 A.5.1.1.

(ii) Access to personal data for employees only on a "need-to-know" basis.

(iii) We have a dedicated security coordinator who is responsible for coordinating responses to incidents and data protection requests, in accordance with ISO 27002 6.1.1.

(iv) A Privacy Information Management System (PIMS) is in place, which covers compliance with applicable data protection laws, identification and control of personal data, access management, data protection guidelines, an emergency plan and a designated data protection officer in accordance with ISO 27701 6.4.2.2 and is accessible to employees.

8 Further protective measures

(a) The following measures also form part of Smartbridge's comprehensive data security measures:

(i) Regular security audits.

(ii) Employees are regularly informed about potential risks, vulnerabilities and handling procedures, which reflects the training aspect of ISO 27002 7.2.2.

(iii) Documented business continuity and IT contingency plans are in place. The IT infrastructure is managed by a specialised partner certified to ISO 27001, 9001, 20000-1 and 22301 and Amazon Web Services, which demonstrates compliance with ISO 27002 17.1.1 and 17.1.2.

(iv) Information security is an integral part of our development cycle, using best security practices, code reviews, automated vulnerability testing and an authentication and authorisation system in accordance with ISO 27002 clauses 14.2.1, 14.2.5 and 14.2.6.

9 Precautions in the event of technical incidents

(a) There is a documented process for technical incidents that ensures efficient and proper management of security incidents and is a key component of our security strategy.

Annex 3: Subcontractors

Smartbridge engages the following subcontractors for the provision of services in accordance with the main contract:

Contracting party	Role and affected services	Type and category of personal data concerned	Place of data processing
Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States. Amazon Web Services, Inc. is a company incorporated and registered under the laws of the State of Delaware (registration number: 4152954, Secretary of State, State of Delaware)	Data centre services	All data in accordance with Annex 1 of the Smartbridge Data Protection Agreement	Frankfurt, Germany (see below)
Skaylink GmbH Zielstattstr. 42 81379 Munich	Implements and operates scalable cloud hosting solutions based on Amazon Web Services (AWS) as an Amazon Web Partner. The services include in particular Core Compliance Core Security Standard logging Standard DDoS protection	All data in accordance with Annex 1 of the Smartbridge Data Protection Agreement	Frankfurt, Germany https://www.skaylink.com/de/datenschutzhinweise/
ActiveCampaign, 1 North Dearborn Street, 5th floor, Chicago, IL 60602 privacy@activecampaign.com	ActiveCampaign operates the Postmark e-mail service	Email dispatch from Staffcloud	Chicago, USA DPA and SCC according to: https://postmarkapp.com/eu-privacy https://postmarkapp.com/dpa https://postmarkapp.com/support/article/1218-gdpr-faq Retention period: 45 days storage of emails at Postmark,

			45 days +1deletion of all emails + log. https://post-markapp.com/terms-of-service
Hubspot GmbH, Am Postbahnhof 17, 10243 Berlin	Hubspot is a CRM for managing customer data. Smartbridge uses it for collaboration with the customer.	First and last name, e-mail address and telephone number, company name of the customer.	On AWS servers in the EU Hubspot Regional Data Policy https://knowledge.hubspot.com/account-security/hubspot-cloud-infrastructure-and-data-hosting-frequently-asked-questions
Freshworks Inc. 2950 S. Delaware St, Suite 201, San Mateo, CA 94403, USA	Freshdesk is a support system. Smartbridge uses the system to answer customer support enquiries. Only the personal data of the customer's contact persons (personnel) is processed. https://www.freshworks.com/privacy/	E-mail address of the customer	EEA DPA and SCC according to https://www.freshworks.com/privacy/
JoinCube, Inc. 3500 S Dupont Hwy Dover, DE, 19901-6041 United States	JoinCube operates the Get Beamer information service. This is Smartbridge's information system for its customers.	E-mail address of the customer	DPA and SCC according to https://www.getbeamer.com/privacy-policy

AWS provides the following information on the data centre services provided by AWS:

(a) Standard Contractual Clauses (SCCs): AWS integrates SCCs into its Data Processing Addendum (DPA) to enable legal data transfers from the EU to countries outside the EEA (Amazon Web Services) https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html

(b) Supplementary measures: AWS has implemented technical and organisational measures to protect data. These include strong encryption both in transit and at rest, robust access controls and customer control over storage and access to their data (Amazon Web Services): https://aws.amazon.com/de/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/

(c) Requests from law enforcement agencies: AWS is committed to challenging overbroad or unlawful requests for data from government agencies. They will only disclose the minimum necessary data when compelled to do so by law and will notify

customers of such requests to the extent permitted by law (Amazon Web Services): https://aws.amazon.com/de/blogs/security/how-aws-is-helping-eu-customers-navigate-the-new-normal-for-data-protection/

(d) Data transfer tools: AWS provides resources to help customers assess data transfers and understand the implications of using AWS services under the GDPR. This includes detailed documentation on processing activities and the locations of data processors (Amazon AWS Docs): https://aws.amazon.com/de/blogs/security/how-aws-is-helping-eu-customers-navigate-the-new-normal-for-data-protection/

(e) Regional data storage: AWS allows customers to select the AWS region in which their data is stored and ensures that data is not transferred outside the selected region without the customer's consent (Amazon Web Services): https://aws.amazon.com/de/compliance/gdpr-center/

(f) Further information can be found on the AWS compliance page: https://aws.amazon.com/de/compliance/eu-data-protection/

(g) The AWS compliance programmes are listed at https://aws.amazon.com/de/compliance/programs/. ISO27001 in particular is described and can be viewed at https://aws.amazon.com/de/compliance/iso-27001-faqs/

(h) For a "Data Transfer Impact Assessment", AWS makes the following statement in addition to the measures mentioned above: "AWS clarifies that the CLOUD Act does not grant unlimited or uncontrolled access rights and that they have the right to challenge requests that conflict with the laws of other countries or national interests. AWS has a history of challenging requests from government agencies that they deem overbroad or unreasonable. This applies to requests from any country, including the United States. AWS carefully reviews each request to ensure that it complies with applicable laws and informs customers unless prohibited by law. https://aws.amazon.com/de/compliance/cloud-act/