GTC Smartbridge AG, Appendix 1

Data Protection Agreement

Table of Contents

1 Preamble

(a) This attachment gives concrete form to the obligations of the parties concerning data protection aspects based on the European General Data Protection Regulation (GDPR) as well as the Swiss Data Protection Law (as applicable in 2018) and supplements the contractual regulations of the main contract finalised between the two parties and the accompanying General Terms and Conditions of Smartbridge which form an integral part of the main contract. This attachment is applicable to all actions which are performed within the scope of the main contract, and in which the client and Smartbridge process any personal data belonging to the client.

(b) Smartbridge acknowledges that the client is obliged to bind Smartbridge to certain obligations resulting from the GDPR, even if the GDPR is not directly applicable to Smartbridge, in the following cases:

(i) The client is a responsible party or processor within the jurisdiction of the EU GDPR, and

(ii) The client involves Smartbridge as a processor or subcontractor in the processing of personal data which falls within the jurisdiction of the EU GDPR.

2 Subject, Duration and Specification of Order Processing

(a) The client is responsible for the legality of data processing, including the legitimacy of order processing. Smartbridge processes the client's data solely for the purposes defined in the main contract. The compliance with legal, regulatory or official obligations remains reserved.

(b) The duration of this attachment is defined by the duration of the main contract, insofar as the regulations of this attachment do not generate obligations beyond this duration.

3 Personal Data and the Groups of Affected Persons

(a) Within the scope of ordered data processing, the following personal data is processed in particular:

(i) Names, address details, E-mail-addresses, phone numbers;

(ii) Photos, work contracts and corresponding documents, such as CVs, employer references and qualification certificates, ratings;

(iii) Data pertaining to wages, bank account details, and other payroll and financial data.

(b) The scope of ordered data processing concerns the following groups of persons:

(i) The client's employees;

(ii) Other persons acting on behalf of the client;

(iii) The client's customers and potential customers.

4 Applicability and Responsibility

(a) Smartbridge processes personal data on behalf of the client. This includes actions defined by the main contract or the General Terms and Conditions, respectively. The client retains all responsibility for data protection and solely decides on the purpose and the measures taken for the processing of such personal data that is handed over to Smartbridge. Within the scope of this attachment, the client is solely responsible for complying with the legal regulations of data protection laws, particularly for the legality of transferring data to Smartbridge and the legality of data processing ("Controller" as defined by Art. 4 No. 7 GDPR).

(b) The client commits to the following and guarantees in particular that:

(i) the data processing and the corresponding orders placed with Smartbridge are lawful;

(ii) the client has sent any necessary notices, made any necessary registrations, and has received any necessary legal approval and authorisation for the lawful processing of personal data by Smartbridge (including the disclosure of such data to Smartbridge).

(iii) the client has received the consent of concerned persons required by law and fulfilled their information obligations regarding this, particularly by informing the concerned persons about the data processor, the purpose of data collection, any justification for data collection, the type of data recipient, possible data transfer into third countries, the duration of data storage, all rights regarding information, notification and deletion as well as the possibility of lodging complaints with the responsible data protection authorities.

(c) The client independently takes appropriate technical and organisational measures within the scope of their responsibility (e.g. concerning their own systems, buildings, applications/operational environments within their operational responsibility) in order to protect the relevant data. The client is primarily responsible for complying with any data protection regulations (and particularly for complying with any data protection regulations regarding employment relationships and employee data protection regulations).

(d) The directives are initially defined by the main contract. After its finalisation, the client can alter, augment or substitute them with individual directives in written or electronic form (as a text) sent to an address defined by Smartbridge. Smartbridge shall inform the client immediately if Smartbridge considers the directive to be in violation of the GDPR, the Swiss Data Protection Law or any other applicable data

protection laws. In such a case, Smartbridge may defer the implementation of the directive until it has been confirmed or altered by the client in writing. In the event of receiving directives from the client concerning the allocation of permissions or the publication of relevant data to the client themselves, Smartbridge may consider these directives to be compliant with the law.

(e) Should such directives generate further costs for Smartbridge or change the scope of services, the parties are obliged to make a corresponding addition to the main contract.

5 Obligations Smartbridge

(a) Data protection and data security are of the highest priority to Smartbridge. Smartbridge strictly complies with the applicable data protection laws within Switzerland. Smartbridge has designed their inner-operational organisation in order to ensure that it complies with the requirements of data protection. Smartbridge has taken technical and organisational measures that permanently ensure the confidentiality, integrity, availability and capacity of the systems and services concerning data processing. The client is aware of these technical and organisational measures and is responsible for ensuring that they provide an adequate level of protection for the processed data.

(b) Smartbridge reserves the right to change the security measures taken while ensuring that they do not fall below the agreed-upon security level.

(c) Where agreed, and within the limits of their possibilities, Smartbridge supports the client in fulfilling the queries and requirements of concerned persons as defined in Chapter 3 of the GDPR, as well as in complying with the obligations defined by Articles 33 to 36 GDPR. Within this scope, any additional services performed by Smartbridge shall be subject to a separate invoice to the client.

(d) Smartbridge guarantees that any employees or other persons acting on behalf of Smartbridge involved in data processing are strictly prohibited from processing the data in any way outside of the scope of the directives given to them. Furthermore, Smartbridge guarantees that any persons authorised to process personal data are bound by an obligation of confidentiality or by an appropriate secrecy obligation within the law. The confidentiality/secrecy obligation continues to be applicable after the end of the contract.

(e) Smartbridge shall inform the client immediately when they are aware of any breach of the protection of personal client data that occurred at Smartbridge or through any subcontractor. Smartbridge informs the client in an appropriate manner about the type and scope of the violation as well as possible remedial actions. In such a case, the parties take the necessary measures to ensure the security of the

relevant data and to minimise possible disadvantageous consequences for the affected persons.

(f) Smartbridge indicates a point of contact to the client for any data protection concerns that arise within the scope of the main contract.

(g) Smartbridge guarantees the implementation of a process for regular monitoring of the effectiveness of the technical and organisational measures to ensure the security of processing.

(h) Smartbridge corrects or deletes relevant data insofar as the client gives corresponding directives and the action lies within the scope of agreed-upon directives. Additional costs are subject to a separate invoice to the client according to the applicable rates.

(i) At the end of the contract, any data, data carriers as well as any other materials are to be either returned to the client or to be deleted upon request and at the cost of the client. Smartbridge uses customary processes for this.

(j) In the event that the client is subject to a claim by an affected person concerning Article 82 GDPR, Smartbridge undertakes to support the client in the defence against such claims within the realm of their possibilities at the cost of the client.

6 Client Obligations

(a) The client shall inform Smartbridge immediately and in full in the event that they find errors or irregularities in the service delivery as defined by the main contract concerning any data regulation requirements.

(b) The client indicates a point of contact to Smartbridge for any data protection concerns that arise within the scope of the main contract.

7 Queries of Affected Persons

(a) In the event that an affected person contacts Smartbridge requesting that data be corrected, deleted or disclosed, Smartbridge will refer the affected person to the client insofar that the person’s statements allow for an association with the client. Smartbridge immediately refers the affected person’s query to the client. Smartbridge supports the client within the realm of their possibilities. Smartbridge does not assume any liability in the event that the client fails to answer the affected person’s request correctly, in a timely manner or altogether.

8 Audit / Inspection

(a) Smartbridge provides the client with proof of the compliance with the obligations laid out by this appendix by appropriate means.

(b) Should it be necessary to subject Smartbridge to audits by the client or an independent external auditor on behalf of the client, such audits will take place after prior notice and an appropriate time period given in advance, during the office hours of Smartbridge, without interrupting the daily operations. Smartbridge may make such an audit dependent on the appropriate time period of the prior notice as well as on the signing of a confidentiality agreement concerning the data of other Smartbridge clients and the established technical and organisational measures. In the event that there is a relationship of competition between the auditor acting on behalf of the client and Smartbridge, Smartbridge is granted the power of veto.

(c) The client provides Smartbridge with a copy of the audit report.

(d) In general, the time expenditure of the audit is limited to one day per calendar year for Smartbridge. Smartbridge may charge a fee for work provided within the scope supporting the conduct of an inspection.

(e) In the event that a data protection authority or another supervisory authority from a sovereign territory upon which the client resides conducts the inspection, item 8(b) is generally applicable respectively. Signing a confidentiality agreement is not necessary if the supervisory authority is subject to professional or legal confidentiality and if the violation of this confidentiality is punishable by law.

9 Subcontractors (Further Data Processors)

(a) The contractually agreed-upon services are provided through the deployment of the following subcontractors:

(i) Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States. Amazon Web Services, Inc. is a corporation founded and registered under the federal law of Delaware (Registry number: 4152954, Secretary of State, State of Delaware);

(ii) The used data warehouse of Amazon Web Services has its location in Frankfurt/Germany.

(iii) root360 GmbH, Beethovenstraße 35, 04107 Leipzig, as a corporation implements and runs scalable cloud hosting solutions based on Amazon Web Services (AWS) as an Amazon Web Partner.

10 Written Form, Applicable Law

(a) Amendments and Additions to this appendix require a written agreement (which can take an electronic form as a text) and the explicit indication that this agreement constitutes an amendment or addition to these conditions. This also applies to a waiver of this formal requirement.

(b) In the event of contradictions, the regulations of this appendix take precedence over the regulations of the main contract. Should parts of this appendix be legally invalid, the validity of the appendix as such shall remain unchanged.

(c) The applicable law shall be Swiss Law.

Technical and Organisational Measures for Data Protection (TOM)

Smartbridge undertakes to implement the following technical and organisational measures in the processing of personal data, and to adjust these measures to the current state of the art.

1 Access Monitoring

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

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

(b) Data Centre Security:

(i) Fencing around the entire facility;

(ii) Secured vehicle entrance with security gate and barrier;

(iii) Access through barrier system and security gates;

(iv) 24-hour monitoring of the facility and the building through the security and operational control room;

(v) Access checks via contactless chip card as well as biometric fingerprint scanners;

(vi) Access only with full authorisation based on prior arrangement and an ID check;

(vii) Video monitoring of the entire facility and in the building;

(viii) Various sensors inside and outside the building to detect intruders;

(ix) Anti-theft protection via protection of the perimeter of the data centre.

(c) Security at the Premises:

(i) Access checks with contactless chip card; seamless video monitoring of doors and access points with automatic intruder alarm;

(ii) Various sensors inside and outside the building to detect intruders.

2 Physical Availability Assurance

(b) The following measures for the physical protection of data against destruction and loss are implemented at the data centre:

(i) Fire early-warning system (RAS smoke aspiration system);

(ii) Separate, redundant power supplies, each with 30 MVA, from two separate sub-stations;

(iii) Mains connection with dedicated cables at the 16 kV level, to which no other external clients are connected;

(iv) Two independent supplies at the medium-voltage level 16 kV;

(v) Two separate UPS systems (A and B supply); redundantly designed mains replacement system with diesel generators;

(vi) Temperature and humidity regulation according to the latest state of the art:

(1) Use-adaptive cold water aggregates with high-level control as refrigeration manager;

(2) Innovative cold water distributors and transport systems such as stratified storage tanks and hydraulic special switches, pump management systems and automatic hydraulic compensation;

(3) New free-cooling systems with integrated EC ventilated technology and internally programmed, weather-resistant energy management systems;

(4) Decentralised ventilation and bleeding system with optimised power-saving control points (speed control, humidity-dependent control, etc.); decentralised humidifying and de-humidifying systems for controlling the humidity of the IT areas;

(5) Adiabatic support of refrigeration and air conditioning (humidification and condensation cooling);

(vii) Safeguarding of redundancy through RAID (redundant array of independent discs), Levels 1 and 6 (with two or several plates);

(viii) Daily creation and geo-redundant storage of backups.

3 Permissions

(c) The following technical measures ensure the prevention of unauthorised editing:

3.1 Authentication

(a) Access to computers/systemd in the data centre (authentication):

(i) User identification with password is demanded on all computers and servers;

(ii) Additionally, access to customer servers as root is only possible with a personal certificate and from 3 pre-defined jump hosts. Only persons with an enabled account (username/password) and who can also identify themselves with a certificate have access to the jump hosts;

(iii) A local firewall with iptables is active on all servers. A login as root on the customer servers is only possible from the defined jump hosts.

(b) In addition, user identification with password is required for access to the computers and servers within the premises of Smartbridge. The network in the Smartbridge premises is also protected by a firewall.

3.2 Permission Concepts

(a) The registration, assignment of rights and granting of rights for administrators are segregated at the process level.

(b) Access to customer data is possible only via specific support access points where all the processing operations are recorded.

3.3 Secured Interfaces (USB, Firewire, Network, etc.)

(a) The network is segmented between root servers and managed servers, and network traffic is managed separately.

4 Transfer Security

(a) The system prevents personal data from being read, copied, modified or deleted without authorisation, particularly during transport.

(b) Security during electronic transfers:

(i) Encryption via TLS (Transport Layer Security, 128bit PKCS 1 SHA-1 RSA SSL encryption);

(ii) Server management via SSH;

(iii) Setup of VPN at the client’s request and site-to-site;

(c) Firewall:

(i) Locally, a firewall with iptables is active on all servers. Aside from SSH, all ports are locked and can only be unlocked by services booked previously for this purpose.

(d) Transport security:

(i) Data carriers are removed from the data centre only if they cease to be functional;

(ii) Otherwise, data carriers for transport purposes are always carried on the respective person and are demagnetised and disposed of immediately.

5 Separation Assurance

(a) The following measures ensure that the data records of various clients are kept separate:

(i) Dedicated database and dedicated file system storage for each instance of the software as licensed by the client;

6 Transparency

(a) Subsequent inspection of all access to and transfer of personal data of clients and their allocation to corresponding employees is facilitated through log data.

7 Contractual Obligations for Employees

(a) Access of authorised persons is limited to the specific personal data that they require in order to perform their particular task. This is ensured through the following measures, among others (in addition to those described under item **Error! eference source not found.** above):

(i) Written obligation of employees to comply with data protection, or data secrecy respectively, in accordance with item 3 above;

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

8 Further Secutiry Measures

(a) Furthermore, the following measures form part of the comprehensive data security measures at Smartbridge:

(i) Encrypted storage of client data in databases via AES/Rijndael 256-bit encryption;

(ii) Brief session time-outs for data input by the client to prevent so-called session hijacking;

(iii) ISO 27001 certification of the data centre and presence of a comprehensive anti-virus protection concept;

(iv) Regular penetration tests and security audits.