Preamble to the Data Processing Agreement pursuant to Art. 28 (3) DSGVO based on the EU standard contractual clauses ("DPA")

This DPA is conlcuded between the respective contractual parties("Parties"), consisting of (1) the "Customer" of SVA, in its capacity as the controller within the meaning of Art. 4 No. 7 GDPR[1] and (2) SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden within the meaning of Art. 4 No. 8 DSGVO, hereinafter referred to as "Contractor", "SVA" or "processor".

Upon commissioning of SVA by the Customer, latest by conclusion of a data protection-relevant service agreement, the Parties conclude this Data Processing Agreement based on the Standard Contractual Clauses of the EU for the EU/EEA.

Scope

This DPA specifies the data protection obligations of the contracting parties resulting from the agreed services. Therefore this agreement covers any activities which are to be regarded as processing to be carried out on behalf of a controller, within the meaning of Art. 28 GDPR. According to the interpretation of the national supervisory authorities and the European Data Protection Committee, this may also include activities in which the processing of personal data is not the objective of the commissioned service, but access to such data during the provision of the service (e.g. (remote) maintenance of IT systems by SVA), is at least theoretically possible.

Applicability and precedence

This Agreement may be replaced, supplemented or specified at any time via an individual agreement, negotiated between the Parties – by contacting the Data Protection Team of SVA (Datenschutz@SVA.de). If an applicable Data Processing Agreement pursuant to Art. 28 (3) GDPR already exists between the contracting parties for the respective object of processing, that arrangement shall take precedence over this agreement. The mapping of the respective commissioned service(s) and the associated Data Processing Agreement is documented in the records of processing activities pursuant to Art. 30 (2) GDPR of the contractor.

If the type, scope or nature of the cooperation, requires an individual Data Processing Agreement, this shall be decided by both parties in consultation. This is in particular considered necessary in cases of legal requirements, relevant risks to the rights and freedoms of the data subjects or due to the utlization of additional processors subject to approval.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (“sensitive data”), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller’s request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller’s general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least two weeks (where possible) in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller’s request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor’s obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

  (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

  (2) the likely consequences of the personal data breach;

  (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

  (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

  (b) the details of a contact point where more information concerning the personal data breach can be obtained;

  (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Clause 11
(Supplements to the standard contractual clauses by the contracting parties)

11.1 Choice of law and place of jurisdiction

a) This contract and all legal transactions concluded in the context of its execution shall be governed by German law and, to the extent applicable, the GDPR. The UN Convention on Contracts for the International Sale of Goods (UNCITRAL) and the reference norms of private international law shall be excluded.

b) The parties agree for all legal disputes arising from or in connection with this contract that the competent courts are those of the registered office of the controller or customer respectively.

11.2 Responsibilities and roles of the contracting parties

a) All references to the Controller and its rights and obligations set forth in this Agreement shall be applied to the commissioning Processor (Customer) utilizing the other Processor (Contractor) in cases where both Contracting Parties act as Processors within the meaning of Art. 4 No. 8.

b) If the Agreement is concluded directly between a Controller (Customer) and a Processor (Contractor), the provisions set forth in this Agreement shall apply according to the wording.

11.3 Regulation on Affiliates

a) The provisions of this Agreement shall also apply to companies affiliated ("Afilliates") with the Customer (cf. Sections 15 et seq. AktG, Section 271 (2) HGB).

b) The companies affiliated with the Customer shall bear the corresponding rights and obligations under this Agreement, as the party authorized to conclude the Agreement itself.

c) For Affiliates under this Agreement, the Party authorized to enter into the Agreement shall be liable to the Processor, as if it were at fault, pursuant to Clause 10 of this Agreement.

d) The Parties may specify a list of Affiliates entitled to order services governed by this Agreement in an Annex. If available, this Annex is attached to this Agreement as "Annex V".

11.4 Termination

a) This contract may be terminated at the end of each quarter, with a notice period of one month.

b) The right of termination according to clause 10 of this contract remains unaffected.

c) If this contract is terminated, the continuation of any processing of personal data is suspended until the terminated contract is replaced by a legally effective new contract.

11.5 Processing outside business premises

a) Unless otherwise agreed, the processing of data outside the premises of the processor is permitted. A meaningful document on the safeguarding of the processing shall be made available to the Controller upon request.

b) The Processor shall ensure and warrant that compliance with all necessary and adequate data protection measures within the meaning of Art. 32 GDPR is also ensured in cases of 11.5 (a).

11.6 Use of certificates as demonstration of compliant processing

Suitable and valid certificates for IT security and data protection (e.g. IT-Grundschutz, ISO 27001, etc.) can also be presented as proof of compliant processing, provided that the respective subject of the certification also applies to the corresponding service(s) and related processing. However, the presentation of a relevant certificate shall not substitute the Customer's right to verify nor the Contractor's obligation to document the security measures within the meaning of clause 7.6 of this Agreement.

11.7 Supplementary clause to 7.7 a) Use of sub-processors

In events of operational emergency such as server failures and cyber-attacks with massive impact on the maintenance of the business operations of the Controller(s) or the security of the Personal Data of the Data Subjects, the Processor shall be entitled to engage additional sub-processors for the limited period of the event. The notification period defined in clause 7.7 a) of this Agreement shall not apply, in favor of a short notice prior to the commencement of processing by the subcontractor.

11.8 Secrecy and confidentiality

a) The Processor is obligated to instruct and obligate its employees and vicarious agents involved in the processing of personal data or other confidential information or information requiring secrecy in accordance with the relevant legal provisions (including § 2 GeschGehG, § 3 TDDSG, § 53 BDSG, § 203 StGB, § 39 PostG) in a documented manner. Instruction and obligation shall continue after termination of the activity.

b) The Processor warrants to be aware of the applicable data protection regulations and to be familiar with the application thereof. The Processor further warrants to familiarize the employees engaged in the performance of the services with the relevant provisions of data protection regulation and that they are obligated to maintain confidentiality in the handling of personal data, unless they are already otherwise subject to an appropriate statutory duty of confidentiality.

11.9 Written form and severability clause

a) Amendments and supplements to this Agreement and all parts thereof - including any representations made by the Processor - must be agreed in writing and must expressly state that they are an amendment or supplement to these Terms and Conditions, which may also be in an electronic format.

b) Should individual provisions of this contract be invalid, this shall not affect the validity of the rest of the contract. The parties shall then replace this provision with a provision that achieves or comes as close as possible to the intended regulatory purpose of the invalid or unenforceable or infeasible provision - insofar as this is legally permissible. This applies in particular to loopholes in this contract.

ANNEX I LIST OF PARTIES

1. Name und Adress of Customer: Client party according to service agreement

- Contact info of the Data Protection Officer (DPO) : To be provided by the controler (e.g. via Website or E-Mail notification)
- Role: Customer
- (Accession) Date: Corresponds to the signature date of the service agreement

2. Name und Adress of Contractor: SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden, Germany

- Contact info of Data Protection Officer (DPO) and Data Protection Team (DPT):
    - DST: datenschutz@sva.de, +49 6122 536-0
    - DPO: dsb@sva.de, +49 6122 536-0
- Role: Contractor (Processor)
- (Accession) Date: *Corresponds to the signature date of the service agreement.*

ANNEX II: DESCRIPTION OF THE PROCESSING

For all listed categories of data subjects and personal data, the following shall apply: The controller/Customer shall notify the processor (Contractor) of any personal data that deviates from those listed in this Annex. The to be adjusted types of personal data and categories of data subjects listed in the notification shall become an integral part of this agreement as a supplement. This also includes personal data to which you grant Contractor access in connection with the provision of products or services. Unless otherwise agreed, the provisions of this contract on processing of personal data shall apply accordingly.

Categories of data subjects whose personal data is processed

Specifying, deviating from or supplementing the categories of data subjects defined in the service agreement, the processing may include any categories of data subjects whose data is processed by the controller to which the Contractor gains access to or hast to process otherwise in context of the agreed servcies (such as maintained it-systems). This may include:

- Employed persons of the Principal within the meaning of § 26 BDSG,

- end customers/customers of the client,

- suppliers of the client,

- Others (guarantors, other third parties, such as tax consultants, etc.).

Categories of personal data processed

Specifying, deviating from or supplementing the categories of personal data defined in the service agreement, the processing may include any categories of perosnal data, that is processed by the controller and to which the Contractor gains access to or hast to process otherwise in context of the agreed servcies (such as maintained it-systems). This may include:

- Master data (name, address, e-mail, tel. no., IP address, etc.),

- allocation data (customer no., employee no., member no., etc.),

- data from keyloggers (e.g. certain data of data loss prevention systems),

- telecommunications data (§ 3 TTDSG),

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- special types of personal data (Art. 9 GDPR),

Nature of the processing

The Contractor shall perform (IT) services on behalf of the Customer. The type of processing results from the correponding service agreements. In general, this includes incidental access and processing that cannot be excluded while providing (IT) services, as well as planned processing based on the service description.

Purpose(s) for which the personal data is processed on behalf of the controller

Support and (IT-)services, exemplarily within the scope of commissioning, installation and maintenance of hardware and software of the controller, hosting services as well as other services originating from the portfolio of the Processor.

Duration of the processing and contract term

The duration of the processing and term of this Agreement shall correspond to the duration of the corresponding agreed service(s).

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES

If the service to be provided by the Contractor is performed exclusively on the premises of the Controller/Customer, using exclusively the latter's technical systems or data processing equipment and under the instruction or supervision of the Controller/Customer, the technical and organizational protective measures set out in this Annex shall be replaced by those of the Controller/Customer.

The SVA has taken the technical and organisational protective measures documented below. Contractors and subcontractors may take alternative technical and organisational protective measures, provided that the following protective measures are not fallen short of. These shall be documented and attached to this agreement as an annex. If no annex to this agreement is attached, the following technical and organisational protective measures are deemed to have been fulfilled by the Contractor.

Considering the state of the art, the implementation costs and the type, scope, circumstances and purposes of processing as well as the varying probability of occurrence and severity of the risk to rights and freedoms of natural persons, SVA shall take appropriate technical and organisational measures to ensure a level of protection commensurate with the risk.

In assessing the appropriate level of protection, particular account must be taken of the risks inherent in processing, in particular those arising from destruction, loss, alteration or unauthorised disclosure or access, whether accidental or unlawful, to personal data transmitted, stored or otherwise processed.

1. Use of pseudonyms

When instructed by the controller the processed personal data may be processed in such a way that it is not allocated to one specific data subject without additional information, provided that this additional information is kept separately and is subject to technical and organisational measures which prevent unauthorized identification of the data subject.

2. Encrypting measures

- Encrypted storage of passwords
- Secure data transfer (e.g. SSL, FTPS, TLS)
- Secured WLAN

3. Measures to ensure confidentiality

a. Measures that deny access to unauthorized persons:

- Door security (electronic door openers, combination lock)
- Key management / documentation of key allocation
- Specific safeguards for the server room
- Specific safeguards for back-up storage and/or other data carriers
- Non-reversible destruction of data carriers
- Visitor regulation (Pick-up at reception, post-visit escort to the exit)

b. Measures, which prevent unauthorized persons from using the processing systems:

- Personal and individual user log-in when accessing the system or the corporate network
- Authorization process for access authorization
- Limitation of authorized users
- Electronic documentation of passwords and protection of these documents from unauthorised access
- Additional system log-in for specific applications
- Automatic blocking of clients after a certain course of time without user activity (also password protected screen savers or automatic pausing)
- Firewall

c. Measures, which guarantee that only authorized persons have access to the processing systems and that personal data cannot be read, copied, modified or removed without authorization:

- Administration and documentation of differentiated authorizations
- Evaluations/logging of data processing

- Authorisation process for authorisations
- Authorisation routines
- Profiles/roles
- Segregation of duties
- Non-reversible deletion of data carriers

d. *Measures, which guarantee that data collected for different purposes can be processed separately:*

- Access authorisations according to functional competence
- Separate data processing through differentiated access authorisations
- Multi-client capability of IT systems

4. Measures to secure integrity

- Access rights
- Logging of system-relevant data
- Document Management System (DMS) with modification history
- Security / logging software
- Functional responsibilities, organization-determined competences
- Logging of read-access, data copy, modification or removal

5. Measures to secure and recover availability

- Security concept for software and IT applications
- Back-up procedures and Storage procedures for back-ups (fire-proof safe, separate tape marks, etc.)
- Guaranteed data storage in secured network
- Demand-driven installation of security updates
- Hard disk mirroring
- Establishment of an uninterruptible power supply (UPS)
- Fire and/or extinguishing water protection for the server rooms and archive rooms
- Air-conditioned server room
- Virus protection
- Firewall
- Redundant, locally separated data storage (offsite storage)

6. Measures to ensure load bearing capacity

- Redundant power supply
- Sufficient capacity of IT systems and facilities
- Procedure to logistically steer the avoidance of power peaks
- Redundant systems/facilities
- Resilience and error management

7. Measures to regularly inspect, assess and evaluate the effectiveness of the technical and organisational measures

- Procedures for regular inspections/audits
- Policies for regular inspection, assessment, and evaluation

8. Instruction/order control

- Contract for order data processing pursuant to Art. 28 para. 3 GDPR with provisions on the rights and obligations of the order processor and responsible party
- Process for issuing and/or following instructions
- Determination of contact persons and/or responsible employees
- Control/verification of order execution according to instructions
- Training/instruction of all employees with access rights at the order processor's premises
- Commitment of all employees to confidentiality
- Appointment of a data protection officer pursuant to Art. 37 et seq. GDPR
- Keeping a list of processing activities pursuant to Art. 30 para. 2 GDPR

- Documentation and escalation process for violations of the protection of personal data
- Guidelines/provisions to ensure technical and organisational measures for the safety of processing
- Process for the forwarding of requests from data subjects

9. Information security policy and certificates

The SVA Information Security Policy is published on the SVA website. In addition, SVA has (or is in the process of implementing) the following certifications:

- ISO 27001:2013 (ISMS)
- ISO 9001:2015
- TISAX (planned for 2022)

ANNEX IV: LIST OF SUB-PROCESSORS

SVA shall not use the services of external parties for the processing of personal data of the Controller. Notwithstanding the foregoing, the Parties may agree on the involvement of additional parties (e.g. subcontractors, etc.) during the offer phase, whereby the Customer agrees to their engagement (if relevant under data protection regulation) as subprocessors within the meaning of this Agreement. An updated list according to this Annex IV will be provided upon request.

Should SVA engage subcontracted processors at a later point in time, the Parties shall adapt this Data Processing Agreement and Annex IV accordingly or replace this Data Processing Agreement with an updated, individual agreement.

ANNEX V: LIST COMPANIES AFFILIATED ("AFFILIATES")

The Controller or Customer authorizes the following companies affiliated with the Controller pursuant to clause 11.3 of this Agreement to directly engage the Contractor or Processor on the basis of this Agreement:

Company	Adress incl. country	Date added:	Optionally contact info of contact person
currently none	-	-	-