Preamble to the contract for data processing according to Article 28 (3) GDPR on the basis of the EU Standard Contractual Clauses (“data processing agreement”, “agreement" or “DPA”)

This Agreement applies between the respective contractual partner hereinafter referred to as “customer” or “controller”, in its role as a controller within the meaning of Article 4 No. 7 GDPR[1] and SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden, in its role as a processor within the meaning of Article 4 Nr. 8 GDPR, hereinafter referred to as “contractor”, “SVA” or “processor”

When SVA is commissioned by the customer to process personal data and/or a service agreement relevant to data protection legislation is concluded, the Parties simultaneously conclude this data processing agreement based on the (EU) Standard Contractual Clauses.

To minimize the audit effort for the involved Parties, but at the same time ensure fair and transparent contractual data protection provisions, the (EU) Standard Contractual Clauses between controllers and processors within the EU/ EEA pursuant to Article 28 (7) GDPR form the base of this Agreement. The (EU) Standard Contractual Clauses are an addition and not to be confused with the (EU) Standard Contractual Clauses for third country transfers. Both mentioned versions of the (EU) Standard Contractual Clauses were published by the EU Commission via the implementing decision (EU) 2021/915 of 4 June 2021. These inner EU Standard Contractual Clauses stipulate that the clauses may not be modified (Clause 2) but can be supplemented, provided that these supplements do not contradict the provisions and their regulatory integrity of the (EU) Standard Contractual Clauses (Clauses 1-10). Accordingly, the (EU) Standard Contractual Clauses remain unchanged. The aforementioned admissible supplements of these clauses are contained in Clause 11 and the respective Annexes to this agreement.

Scope of application

This agreement specifies the data protection obligations of the contracting Parties arising from the relevant services agreed upon. Therefore, this agreement includes all activities that are considered to be “Processing” in the meaning of Article 28 GDPR. According to the interpretation of the national supervisory authorities and the European Data Protection Board, this may also include activities where the processing of personal data is not directly the subject of the service agreement, but access to such data cannot be excluded during the provision of the service (e.g. in the case of (remote) maintenance of IT systems by SVA).

Adjustments, applicability and hierarchy

This agreement can be replaced, supplemented or specified at any time by an individual agreement negotiated between the Parties - in such cases, you can contact datenschutz@sva.de. If the contracting Parties already have concluded a valid data processing agreement in accordance with Article 28 (3) GDPR for the respective service/processing activity, it shall take precedence over this agreement.

If, due to the type, scope or nature of the relevant services, the categories of personal data or the processing activity, it is deemed necessary to conclude an individual agreement replacing this agreement, this will be decided by both Parties in consultation. This might be deemed necessary in particular due to legal requirements or in consideration of the risks to the rights and freedoms of the data subjects.

[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, and repealing Directive 95/46/EC).

EU 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[2] 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 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

[2] The term "racial origin" is derived from the original text of the European Union (EU) GDPR and its translation. It is important to clarify that neither the EU nor SVA endorses or tolerates theories that attempt to determine the existence of different human races. In this respect, the wording is not intended to imply a biological understanding of "racial origin" and "race," and its use is not intended to reproduce racist ideas. The EU also emphasizes this in Recital 51 of the GDPR.

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 EU Standard Contractual Clauses by the contracting Parties)

11.1 Choice of law and place of jurisdiction

a) This agreement and all legal transactions concluded in the context of its execution shall be governed by German law and, to the extent applicable, the GDPR.

b) The Parties agree for all legal disputes arising from or in connection with this agreement 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 out in this agreement shall apply to the commissioning processor (customer) who engages the other processor (contractor) in cases where both contracting Parties act as processors within the meaning of Article 4 No. 8 GDPR. In this case, references to the actual controller within the meaning of the GDPR, who is not a Party to this agreement, are identified below by the additional reference to “Article 4 No. 7 GDPR”.

b) If the agreement is concluded directly between a controller (customer) as defined under Article 4 No. 7 GDPR and a processor (contractor), the provisions set forth in this agreement shall apply according to the wording.

c) Furthermore, if both Parties to this agreement are processors within the meaning of Article 4 No. 8 GDPR, the following shall apply: In the event of insolvency, liquidation and discontinuation of the contractor's business activities or extraordinary termination of the contractual agreements, the contractor shall ensure that the customer has access to the processed data. In addition, the contractor shall ensure that the data is recovered and made available in an easily accessible format, unless the customer itself has access to this data. The contractor shall also contractually ensure the same obligations with any subcontractors within the meaning of Clause 7.7 of this agreement.

d) Specifying Clause 1 e), f) and Clause 7.4 of this agreement, it is the sole responsibility of the controller to assess whether

1) the technical and organizational measures of the processor for the processing on behalf of a controller are sufficient to adequately protect the processed data, and

2) the commissioning of the processor and its authorized sub-processors in accordance with Annex IV is lawful,

3) the processing is carried out in accordance with the instructions of the controller and in accordance with suitable contractual agreements within the meaning of Article 28 (3) GDPR.

Otherwise, the controller within the meaning of Article 4 No. 7 GDPR is responsible for ensuring compliance with the data protection regulations of all applicable legal provisions, in particular the lawfulness of the processing.

11.3 Supplementary provisions to Clause 7.1 (Instructions)

a) The obligation of documentation in accordance with Clause 7.1 of this agreement is incumbent on both Parties. Verbal instructions from the controller must be confirmed to the processor immediately and at least in text form.

b) It is the sole responsibility of the controller to ensure that the instructions given are lawful.

c) The right of the controller or customer to issue instructions is limited, to the extent permitted by law, to the processing activities and data operations resulting from the service agreement(s) and/or comparable documents pertaining to this agreement.

11.4 Regulation on Affiliates

a) The provisions of this agreement shall also apply to companies affiliated (“Affiliates”) 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".

e) If an Affiliate is included in Annex V with the mutual consent of the contracting Parties, the requirements of Clause 5 a) are deemed to be fulfilled. Accordingly and notwithstanding the compliance with the other provisions of this agreement a separate completion of Annexes I - IV and signing of Annex I for such Affiliates is not required.

11.5 Termination

a) This agreement may be terminated at the end of each quarter, subject to a notice period of one month.

b) The right of termination according to Clause 10 of this agreement remains unaffected.

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

11.6 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 related 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 Article32 GDPR is also ensured in cases of Clause 11.6 (a).

11.7 Use of certificates as demonstration of compliant processing

a) Suitable and valid certificates for IT security and data protection (e.g. (BSI) IT-Basic Protection, ISO 27001, TISAX 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 controller's right to inspect/audit the processor nor the obligation to document the security measures within the meaning of Clause 7.6 of this agreement.

b) Such an inspection/audit is subject to the following conditions:

- **Scope:** Audits shall be limited to the processor's data processing systems and personnel involved in the processing activities covered by this agreement.
- **Frequency:** Audits shall be carried out at most once a year or with such other frequency as required by applicable data protection legislation or by a competent supervisory authority, or immediately after a significant personal data breach affecting the personal data processed by the processor under this agreement.
- **Period:** The Audits shall, where possible, be carried out during normal business hours (Monday to Friday from 9 a.m. to 6 p.m.).
- **Advance notice:** Audits require regular advance notice of at least four weeks. In the event of justified suspicions of a significant personal data breach by the processor, audits may also be carried out without prior notice.

- **Operational disruption:** The audits must be carried out without disproportionate disruption to the processor's operations.
- **Confidentiality:** The audits must be carried out in strict compliance with trade and business secrets pursuant to Section 2 No. 1 GeschGehG (Trade Secrets Law) and all other relevant confidentiality and secrecy obligations to which the processor is subject.
- **Auditors appointed by the controller:** If the (third party) auditor appointed by the controller is in a competitive relationship with the processor, the processor shall have the right to object to this auditor. The controller shall bear the immediate costs of the appointed auditor.
- **Audit report(s):** The controller will prepare an audit report summarizing the findings and results of the audit of the processor. Such audit reports shall be confidential information of the processor, which the controller shall not disclose to third parties, except to its legal advisors and other consultants, its data protection officer, its employees and its affiliates, or if the controller is required to disclose under applicable data protection legislation or at the request of a competent supervisory authority, or if the processor has given consent to disclosure. The result of the audit shall be made available to the processor.

c) Audits of other processors commissioned: The audit of sub-processors commissioned in accordance with Annex IV of this agreement shall be the sole responsibility of the processor. Upon request, the processor shall provide the controller with suitable evidence (certifications, results of audits, etc.) demonstrating an adequate level of protection of the controller's data. The rights of the controller under this Clause 11.6 and Clause 7.6 of this agreement therefore only apply to the processor pursuant to Annex I of this agreement. The rights of the controller to request a copy of the contractual terms between the processor and (sub-)processor pursuant to Clause 7.7 (c) shall remain unaffected.

d) Third parties (e.g., other controllers) may only exercise the customer's audit rights under this agreement if they are entitled to do so under applicable law and if the customer authorizes and coordinates such audits. In order to avoid duplicate audits, the customer shall undertake all reasonable efforts to combine lawful audits by third parties.

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

The following shall apply in addition to or specify clause 7.7 a) of this contract: In the event of an operational emergency, such as server failures and cyber-attacks with a massive impact on the maintenance of the controller's business operations or the protection of the personal data of the data subjects, the processor shall be entitled, after informing the controller, to engage additional (sub-)processors for the limited period of the emergency. The notification period defined in Clause 7.7 a) of this agreement is thereby shortened in favor of a short-term announcement of the sub-processor to be commissioned prior to the start of processing. The right of objection to which the controller is entitled in this context remains unaffected.

No processing (on behalf of a controller) but transfer of data by the processor: A transfer of personal data processed by the processor on behalf of the controller to the manufacturers or distributors (hereinafter referred to as “manufacturers”) of the IT solutions distributed by the processor shall only take place insofar as this is necessary in the context of the execution of the order by the processor in accordance with instructions and:

- the data is limited to what is necessary,
- as far as necessary for the purposes of the independent implementation of registration, independent maintenance/support and the independent conclusion of EULAs, TOSs or other applicable contracts by the manufacturers.

In these cases, the manufacturers alone determine the purposes and means of the specified processing of the personal data transmitted to the manufacturers by the processor on behalf of the controller and are considered Third Parties for the processor within the meaning of Article 4 para. 10 GDPR and not processors in a subcontracting relationship. In this context, existing transparency

and other informational obligations pursuant to Article 13 para. 1 lit. e GDPR or Article 14 para. 1 lit. e GDPR must be fulfilled by the controller.

11.9 Secrecy and confidentiality

a) The processor shall 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 TDDDG, § 53 BDSG, § 203 StGB) in a documented manner. These instructions and obligations shall continue after termination of the (processing) activity.

b) The processor warrants that it is aware of the applicable data protection regulations and is familiar with their application. The processor further warrants that it will familiarize its employees and any other person acting under the authority of the processor within the meaning of Article 29 GDPR who are involved in the processing of personal data of the controller or have access to such data with the data protection provisions applicable to them and has obliged them to maintain confidentiality when handling personal data, unless they are already otherwise subject to an appropriate and sufficient statutory duty of confidentiality. The processor shall also contractually ensure the aforementioned obligations vis-à-vis any commissioned (sub-)processors listed in Annex IV to this agreement.

11.10 Amendments and adjustments

a) If a Party intends to change the agreed services or the conditions of this agreement (e.g. due to decisions by the authorities, changes in supplier relationships, legislative changes), this Party shall inform the other Party in text form (e.g. by letter or e-mail to the contact details provided in Annex I) at least 6 weeks before the changes take effect and, as far as possible, avoid disadvantages for the other Party. The Party is entitled to unilaterally amend the provisions of this agreement under the following conditions:

1) In the case of amendments exclusively in favour of the other Party,

2) in the event of merely insignificant changes that do not affect the essence of the rights and obligations but are necessary to be able to continue the services under this agreement, or

3) in the event of mandatory legal changes.

b) For any other changes, the other Party shall be entitled to terminate the affected services without observing a notice period as of the date on which the changes take effect. The other Party shall be expressly informed of the right of termination in the notification of change.

11.11 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.

11.12 Liability

a) **Liability in the external relationship:** Both the controller and the processor are liable in relation to data subjects in accordance with the provisions of Articles 82 et seq. GDPR.

b) **Liability in the internal relationship:** In the relationship between the Parties (controller and processor), the general legal provisions apply, in particular Article 82 GDPR.

c) **Liability for other processors:** In all other respects, the processor shall be liable for its (sub-)processors pursuant to clause 7.7 d).

d) **Recourse claims:** Any recourse (claims) of the controller or a data subject against (sub-)processors shall remain unaffected by the provisions of this agreement.

e) **Indemnification:** The Parties may be exempted from liability within the meaning of Article 82 GDPR, if necessary on a pro rata basis, if they can prove that they are only partially or not in any way responsible for the event giving rise to the damage. This allows for differentiated liability depending on responsibility.

f) **Exclusion and priority:** Any liability provision or limitations thereof agreed upon between the Parties in other contracts shall not apply to data protection issues and shall lapse in favour of the provisions of this agreement.

g) **Further liability claims:** Further liability claims deriving from legal provisions remain unaffected.

11.13 Supplementary provisions on data deletion

The provisions governing the deletion or return of processed and/or transferred personal data pursuant to Clause 10 (d) of this Agreement shall always be based

1) on the technical capabilities available to the Processor for data extraction and deletion,

2) the circumstances and nature of the respective processing, in particular whether the controller or customer is itself in a position to exercise the right to which it is entitled under Clause 10 (d), and

3) the description in the respective service description or comparable document(s) to which this agreement is linked.

ANNEX I – LIST OF PARTIES

1. Name and address of the controller/customer: Commissioning Party in accordance with the service agreement.
    - Contact info of the Data Protection Officer: To be provided by the client (e.g. via the website or e-mail notification)
    - Role: controller (customer)
    - (Accession) date: Corresponds to the date of commissioning based on the service agreement

2. Name and address of the processor/contractor: SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden
    - Contact info of SVA's Data Protection Team::
        - Data Protection Department: datenschutz@sva.de, +49 6122 536-0
        - Data Protection Officer: dsb@sva.de, +49 6122 536-0
    - Role: processor (contractor)
    - (Accession) date: Corresponds to the date of commissioning based on 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 services (such as maintained it-systems). This may include:

- Employees of the controller within the meaning of § 26 BDSG,
- End-customers/customers of the controller,
- Suppliers of the controller,
- Others (e.g. 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 personal data, that is processed by the controller and to which the processor gains access to or has to process otherwise in the context of the agreed servcies (such as maintained IT-systems). This may include:

- General personal data (e.g. first and last name, address, etc.),
- Organisational data (e.g. customer no., employee no., member no., etc.),
- Process data in IT service management (e.g. end user contact data, history data, etc.)
- Log data (e.g. user history, change history, account usage data, etc.)
- Telecommunication data (§ 3 TDDDG)

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 categories of personal data (Article 9 GDPR)

Nature of the processing

The processor shall perform (IT) services on behalf of the controller. The type of processing results from the corresponding service agreements. In principle, this includes incidental processing and processing that cannot be excluded when providing (IT) services, as well as processing on behalf of a controller 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 offered services of the processor's portfolio.

Duration of the processing

The duration of the processing shall correspond to the duration of the corresponding Agreed Service(s) according to the related service agreement.

Annex III – TECHNICAL AND ORGANIZATIONAL MEASURES

SVA has implemented technical and organizational security measures as described hereafter.

This is done taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. SVA implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

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.

Pseudonymization

In general, pseudonymization in the context of service provision is only possible if the data is processed or transmitted on systems for which SVA is responsible. SVA can use various pseudonymization methods. The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information is carried out on the instruction of the customer.

1 Physical access

Measures that prevent unauthorized persons from gaining physical access to data processing facilities.

Technical measures	Organizational measures
Perimeter protection depending on the object and the protective systems contained therein	Reception
Automatic access control system (personalized electronic locking cards)	Visitor book / visitors logging
Chip cards / transponder systems	Employee / visitor passes
SVA locking system	Obligation for visitors to be accompanied by SVA employees
Doorbell intercoms with cameras	Guideline for handling keys
24x7 video surveillance in the data center	Key regulation and list
Logging of access through the SVA locking card system	Different access security zones according to protection requirements
Access to the data center via 2 FA	Visitor and Supplier Handling Policy
24x7 video surveillance of the company premises (main site)	Individual assignment of access rights only to the extent required

2 Control of access

Preventing the use of data processing equipment by unauthorized persons.

Technical measures	Organizational measures
Login with personalized user accounts	Secure password assignment
Multi-factor authentication (system-dependent)	Policy on handling accesses and passwords
Automatic blocking of accounts in the event of too many failed login attempts	Policy „Clean Desk“
Logging of system logins	Policy on handling mobile devices
Anti-virus software server/clients	Policy „Deletion / Distruction“
Firewall	Separation of tasks / functions
Intrusion Detection Systems (IDS and IPS)	Roles and authorizations concept
Mobile device management for all mobile end devices	Rules and procedures for network segmentation are implemented
VPN for remote access	"Work and behavior in secure areas" policy
Provision of a password manager	Mobile working policy
Automatic screen lock during inactivity	Policy on handling printers
Patch management	
Protected printing	
Hardening measures are implemented for operating systems and applications	
Regular review of security measures through penetration testing	
Access control for clients at network level	

3 Data access control

Ensuring that those authorized to use an automated processing system have access only to the personal data covered by their access authorization.

Technical measures	Organizational measures
Tamper-proof access logging	Limiting the number of users with administrator rights to the necessary minimum
Separation and management of privileged access	Management of user rights by administrators
Secure deletion of data/carriers	Roles and rights concept
Secure destruction in accordance with DIN 66399	Approval procedure for the granting, changing and withdrawing of rights
Encryption of notebooks/smartphones	Documentation of all rights changes
System-dependent server encryption	Implementation of the "need-to-know" principle
Segmentation of the networks used is defined	
System-dependent access logging	

4 Separation control

Ensure that personal data collected for different purposes can be processed separately.

Technical measures	Organizational measures
Client separation	Segregation of duties / functions
Separation of productive and test data	
Logical separation of data	

5 Transfer control

Ensure that the confidentiality and integrity of personal data is protected during transmission and transport.

Technical measures	Organizational measures
Transport encryption (TLS, SSL, etc.)	Guideline on the classification and handling of information
E-mail encryption	Guideline "Handling mobile data carriers"
Use of VPN	Implementation of the "need-to-share" principle
Use of suitable protocols such as sftp, https, etc.	
Use of suitable encryption algorithms	
Use of signature procedures	

6 Input control

Ensuring that it is possible to check and establish retrospectively which personal data have been entered or modified in processing systems, at what time and by whom.

Technical measures	Organizational measures
System-dependent technical logging of the entry, modification and deletion of data	Approval procedure for assigning, changing and withdrawing rights
Login logging	Assignment of rights to enter, change and delete data on the basis of an authorization concept

7 Availability control

Ensure that personal data is protected against destruction or loss.

Technical measures	Organizational measures
Fire and smoke detection systems	Regular data recovery tests and logging of the results
Fire extinguisher in front of server room	Regular penetration tests
ServerrServer room monitoring: temperature, humidity, CO2	Emergency plan/regular DR tests
Redundant air conditioning in the server room	Restart concept (measures to restore availability in the event of system failure)
Redundant data centers and infrastructure	implemented BCM
Backups across multiple locations	
Patch management	
UPS per data center	
Load balancing	
Monitoring	
Appropriate measures to protect against malware	

8 Data protection measures

Technical measures	Organizational measures
Software solutions for data protection management in use	Designation of internal data protection officer
Central provision of all data protection-relevant information and documentation (procedures, processes, policies, etc.) for all SVA employees (including internal wiki)	Commitment of all employees to comply with data protection regulations, data secrecy, confidentiality and secrecy and other legal obligations to maintain secrecy and confidentiality (including GeschGehG, 203 StGB, TDDDG, etc.).
Database-supported records of processing activities in accordance with Art. 30 GDPR, in which all processing activities for which SVA acts as a controller or processor are documented and evaluated as necessary.	Regular awareness-raising and training of employees (at least annually) plus additional, area-specific and event-related measures
	Established process for carrying out data protection impact assessment (DPIA is carried out if required in accordance with Art. 35 GDPR)
	Established process for fulfilling transparency obligations to data subjects. SVA complies with the information obligations pursuant to Art. 13 and 14 GDPR
	Establishment and organization of internal data protection in accordance with the mission statement of the BvD e.V. including clear allocation of roles between the data protection department (data protection coordinators & management) and the DPO
	Documented and implemented processes to handle rights of the data subject.
	Established data protection policy and data protection concept
	Regular review of the effectiveness of technical protection measures (audit)
	Regular review of data protection implementation in SVA and activity report by DPO
	Initial and subsequent periodic audits of processors in terms of data protection compliance (due diligence and inspections)
	Documentation of a deletion concept for order processing

9 Incident-Response-Management

Support for security breach response.

Technical measures	Organizational measures
Intrustion Prevention System (IPS)	Documented process for the detection, processing and timely reporting of (also with regard to the obligation to report to supervisory authorities, clients (responsible parties) and data subjects)
Security Operations Center (SOC)	Involvement of data protection and information security in security incidents and data breaches Documentation of security incidents and data breaches Contingency concept and process with 24x7 manned incident distribution center for receiving and processing incidents Internal incident response team

10 Data protection by design and by default

Privacy by design / Privacy by default.

Technical measures	Organizational measures
Technical limitations for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed Technical measures to ensure that it shall be as easy to withdraw as to give consent. Possibilities for data subjects to configure programs in line with data protection requirements (depending on the use case)	Early involvement of the data protection team in product development

11 Order control (outsourcing to third parties)

Ensuring that personal data processed on behalf of the client are only processed in accordance with the client's instructions.

Technical measures	Organizational measures
	Conclusion of the necessary data processing agreements or EU standard contractual clauses Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality Arranging effective control rights towards the processors Regulation on the use of further processors Initial and after regularly audits of processors to demonstrate compliance with data protection regulation Careful selection of processors (especially regarding adequate guarantees for data protection and data security) Transfer of personal data to third countries only in compliance with appropriate safeguards pursuant to Art. 44 et seq. GDPR and, if necessary, implementation of Transfer Impact Assessments (TIA).

12 Information Security Policy

Technical measures	Organizational measures
Software-based Information Security Management System (ISMS) Ticket system for the processing of incidents	Internal information security officer Documented process for detecting, handling and reporting of information security incidents Information Security Management System Information security awareness and training for employee on a periodic basis Self-declaration on information security Guidelines for internal IT operations Established information security guidelines Regular internal audits

13 Quality Management Policy

Technical measures	Organizational measures
Complete process map of the SVA	Internal quality management representative Quality policy document Quality management system Regular internal audits

14 Control and use of AI systems

Technical measures	Organizational measures
	Internal AI responsible person Company-wide AI policy AI inventory overview Testing process for AI tools prior to deployment Regular awareness-raising and training for employees on the AI Regulation

15 Certificates

Certification according to ISO 27001:2013 (ISMS)
Certification according to TISAX
Certification according to ISO 9001:2015
Certification according to ISO 14001:2015
Certification according to ISO 22301 2020 BCM

ANNEX IV: LIST OF SUB-PROCESSORS

The controller/customer has authorized the use of the following sub-processors:

Note on international data transfer: If the controller/customer engages (sub)processors for whom a third-country transfer is carried out on the basis of EU standard contractual clauses, the corresponding "Transfer Impact Assessment" within the meaning of Clauses 14 and 15 of the EU standard contractual clauses can be requested by email.

Company	Address (incl. country)	Transfers on the basis of (Articles 44 ff. GDPR)	Name, role and contact info of contact person	Description of processing activities (including a clear delineation of responsibilities if multiple sub-processors are approved, duration of processing as well as countries in which the processing will take place):
currently none	-	-	-	Processing activity: Processing countries: Duration:

ANNEX V: LIST COMPANIES AFFILIATED ("AFFILIATES")

The controller/customer authorizes the following companies affiliated with the controller pursuant to Clause 11.4 of this agreement to directly engage the processor/contractor on the basis of this agreement:

Company	Address (incl. country)	Date added:	Optionally contact info of contact person
currently none	-	-	-