FEELESTATE

Contract for commissioned processing of personal data according to the EU General Data Protection Regulation (GDPR)

(Date: 24.05.2018)

§1 Area of application

(1) This contract stipulates the rights and obligations of the AVANTO VR Solutions GmbH (hereinafter referred to as "Processor") and its Customers (hereinafter referred to as "Controller") of the online applications "FEELESTATE CMS" and "PANOCREATOR®" (collectively referred to as "Software") in the context of processing personal data on behalf of the Controller.

(2) This contract applies to all activities of processing personal data, provided by the Controller, through the Processor and its subcontractors.

(3) The terms used in this contract are to be understood in accordance with their respective definitions in the EU General Data Protection Regulation (GDPR). Should it be necessary to make the following declarations 'in writing', the written form is meant, as prescribed by § 126 BGB (Bürgerliches Gesetzbuch [*German Civil Code*]). Furthermore, the declarations may be made in another form under the condition that suitable verification is ensured.

§2 Scope and duration of the data processing

(1) The Processor shall process personal data provided by the Controller and through online forms while using the Software.

(2) The processing is based on the Processors general terms and conditions as part of the license agreement, entered into by the Parties (referred to as the 'Master Contract').

(3) Processing shall begin immediately and be carried out for an unspecified period until either this contract or the Master Contract have been terminated by one of the Parties.

§3 Nature and purpose of collecting, processing or using the data

(1) Processing the data consists of the following: collecting, compiling, organising, sorting, saving, separating, recalling, using or transferring, distributing or any other form of provision, replication or linking, restricting, deleting or destroying data.

The data is processed for the following purpose:

- Authorizing access to certain functions or restricted parts of the Software
- Creating statistics of the behaviour of users of the Software

(2) The following data is processed:
- Name
- Lastname
- Address

- Phone Number
- E-Mail Address
- Company Name
- Position

(3) The following data subjects are affected by the data being processed:

- Customers of the Controller

- Employees of the Controller

§4 Obligations of the processor

(1) The Processor shall only process personal data as contractually agreed or as instructed by the Controller unless the Processor is legally obliged to carry out a specific type of data processing. Should the Processor be bound by such obligations, the processor is to inform the Controller thereof prior to processing the data, unless informing him/her is illegal. Furthermore, the Processor shall not use the data provided for processing for any another purpose, specifically his/her own.

(2) The Processor confirms to be aware of the applicable legal provisions on data protection. He is to observe the principles of correct data processing.

(3) The processor shall be obliged to maintain strict confidentiality when processing the data.

(4) Any individuals who could have access to the data processed on behalf of the Controller must be obliged in writing to maintain confidentiality unless they are already legally required to do so via another written agreement.

(5) The Processor shall ensure that its individuals employs, who are to process the data, have been made aware of the relevant data protection provisions as well as this contract before starting to process the data. The corresponding training and sensitisation measures are to be appropriately carried out on a regular basis. The Processor shall ensure that the individuals tasked with processing the data are adequately instructed and supervised on an ongoing basis in terms of fulfilling data protection requirements.

(6) In connection with the commissioned data processing, the Processor must support the Controller when designing and updating the list of processing activities and implementing the data protection assessment. All data and documentation required are to be provided and made immediately available to the Controller upon request.

(7) Should the Processor be subject to the inspection of supervisory authorities or any other bodies or should affected persons exercise any rights against the Processor, then the Processor shall be obliged to support the Controller to the extent required, if the data being processed on behalf of the Controller is affected.

(8) Information may be provided to third parties by the Processor solely with the Controller's prior consent. Inquiries sent directly to the Processor will be immediately forwarded to the Controller.

(9) If he/she is legally obliged to do so, the Processor shall appoint a professional and reliable individual as the authorised data protection officer. It must be ensured that the officer does

not have any conflicts of interest. In the event of any doubts, the Controller can contact the data protection officer directly. The processor is to then immediately notify the controller of the contact details of the data protection officer or provide a reason as to why a data protection officer has not been appointed. The Processor is to immediately inform the Controller of any changes to the status of the data protection officer or of any changes to his in-house tasks.

(10) Any data processing may only be carried out in the EU or EEC. Any change to a third-party country may take place with the Controller's consent and in accordance with the conditions stipulated in chapter V of the GDPR and this contract.

    a. If the Processor is not located in the European Union, then he/she is to appoint a responsible representative in the European Union in accordance with article 27 of the GDPR. The Controller is to be immediately informed of the contact details for the representative as well as any changes to the status of the representative.

§5 Technical and organisational measures

(1) The data protection measures described in Appendix 1 are binding. They define the minimum requirements to which the Processor is obligated.

(2) The data protection measures may be adjusted according to the continued technical and organisational advancement as long as the agreed upon minimum has been sufficiently met. The Processor shall immediately implement the changes required for the purposes of maintaining information security. The Controller is to be immediately informed of any changes. Any significant changes are to be agreed upon by the Parties.

(3) Should the security measures implemented by the Controller not, or no longer, be sufficient, the Processor is to inform the Controller immediately.

(4) The Processor shall ensure that the data processed on behalf of the Controller is kept strictly separate from any other data.

(5) Copies or duplicates are not to be created without the Controller's knowledge. Any technically necessary, temporary duplications are exempt, provided any adverse effects to the agreed upon level of data protection can be ruled out.

(6) Processing data in a private residence is only permitted with the Controller's prior written consent. Should the data be processed in this way, the Processor is to ensure that the sufficient level of data protection and data security is maintained and that the Controller's supervisory rights as determined in this contract can also be exercised without restriction in the private residence. Commissioned data processing on private devices is not permitted under any circumstances.

(7) Dedicated data media, which originate from the Controller or which are used for the Controller, are to be specifically marked and are subject to ongoing administration. They are to be appropriately stored at all times and must not be accessible to unauthorised persons. Any removals and returns are to be documented.

(8) The Processor shall provide regular proof of having fulfilled his/her obligations, especially for completely carrying out the agreed upon technical and organisational measures. This proof is to be

provided to the Controller every 12 months, at the latest, without it being requested, and at any time upon request. The proof may be provided by means of approved rules of conduct or by an approved certification procedure.

§6   Stipulations on correcting, deleting and blocking data

(1) In the scope of the data processed on behalf of the Controller, the Processor may only correct, delete or block the data in accordance with the contractual agreement or the Controller's instructions.

(2) The Processor shall comply with the respective instructions provided by the Controller at all times and also after the termination of this contract.

§7   Subcontracting

(1) Subcontractors may only be appointed on an individual basis with the Controller's written consent.

(2) Consent is only possible if the subcontractor is subject to a contractual minimum of data protection obligations, which are comparable with those stipulated in this contract. The Controller shall, upon request, inspect the relevant contracts between the Processor and the subcontractor.

(3) The Controller's rights must also be able to be effectively exercised against the subcontractor. In particular, the Controller must have the right to carry out inspections or have them carried out by third parties to the extent specified here.

(4) The Processor's and subcontractor's responsibilities must be clearly distinguished.

(5) Any additional subcontracting carried out by the subcontractor is not permitted.

(6) The Processor shall choose the subcontractor by specifically considering the suitability of the technical and organisational measures taken by the subcontractor.

(7) Any transfer of the data processed on behalf of the Controller to the subcontractor shall only be permitted after the Processor has provided convincing documentation that the subcontractor has met his/her obligations in full. The Processor must submit the documentation to the Controller without being requested to do so.

(8) Appointing any subcontractors, who are to process data on behalf of the Controller, who are not located and do not operate exclusively within the EU or EEC, is only possible in compliance with the conditions stipulated in chapter 4 (10) and (11) of this contract. Specifically, this shall only be permitted if the subcontractor provides appropriate data protection measures. The Processor is to inform the Controller of the specific data protection guarantees provided by the subcontractor and how evidence thereof can be obtained.

(9) The Processor must review the subcontractor's compliance with obligations on a regular basis, every 12 months at the latest. The inspection and its results must be documented such that they are understandable to a qualified third party. The documentation is to be submitted to the Controller without it being requested.

(10) Should the subcontractor fail to fulfil his/her data protection obligations, the Processor will be liable to the Controller for this.

(11) At present, the subcontractors provided in Appendix 2 with names, addresses and order content are involved in processing personal data to the extent specified therein and have been approved by the Controller. Any other obligations on the part of the Processor to subcontractors, which have been stipulated here, shall remain unaffected.

(12) Subcontracting, in terms of this contract, only refers to those services that are directly associated with rendering the primary service. Additional services, such as transportation, maintenance and cleaning, as well as using telecommunication services or user services, do not apply. The Processor's obligation to ensure that proper data protection and data security is provided in these cases remains unaffected.

§8 Stipulations on correcting, deleting and blocking data

(1) The Controller shall be solely responsible for assessing the admissibility of the processing requested and for the rights of affected parties.

(2) The Controller shall document all orders, partial orders or instructions. In urgent cases, instructions may be given verbally. These instructions will be immediately confirmed and documented by the Controller.

(3) The Controller shall immediately notify the Processor if he finds any errors or irregularities when reviewing the results of the processing.

(4) The Controller shall be entitled to inspect compliance with the data protection provisions and contractual agreements with the Processor to an appropriate extent, either personally or by third-parties, in particular by obtaining information and accessing the stored data and the data processing programs as well as other on-site inspections. The Processor must make it possible for all individuals entrusted with carrying out audits to access and inspect as required. The Processor is required to provide the necessary information, demonstrate the procedures and provide the necessary documentation for carrying out inspections.

(5) Inspections at the Processor's premises must be carried out without any avoidable disturbances to the operation of his/her business. Unless otherwise indicated for urgent reasons, which must be documented by the Controller, inspections shall be carried out after appropriate advance notice and during the Processor's business hours, and not more frequently than every 12 months. If the Processor provides evidence of the agreed data protection obligations being correctly implemented, as stipulated in chapter 5 (8) of this contract, any inspections shall be limited to samples.

§9 Notification Obligations

(1) The Processor shall immediately notify the Controller of any personal data breaches. Any justifiably suspected incidences are also to be reported. Notice must be given to one of the Controller's known addresses within 24 hours from the moment the Processor realises the respective incident has occurred. This notification must contain at least the following information:

    a. A description of the type of the personal data protection infringement including, if possible, the categories and approximate number of affected persons as well as the respective categories and approximate number of the personal data sets;

    b. The name and contact details of the data protection officer or another point of contact for further information;

    c. A description of the probable consequences of the personal data protection infringement;

    d. A description of the measures taken or proposed by the Processor to rectify the personal data protection infringement and, where applicable, measures to mitigate their possible adverse effects.

(2) The Controller must also be notified immediately of any significant disruptions when carrying out the task as well as violations against the legal data protection provisions or the stipulations in this contract carried out by the Processor or any individuals he/she employs.

(3) The Processor shall immediately inform the Controller of any inspections or measures carried out by supervisory authorities or other third parties if they relate to the commissioned data processing.

(4) The Processor shall ensure that the Controller is supported in these obligations, in accordance with Art. 33 and Art. 34 of the GDPR, to the extent required.

§10 Instructions

(1) The Controller reserves the right of full authority to issue instructions concerning data processing on his/her behalf.

(2) The Controller and the Processor shall appoint the individuals who have been exclusively authorised to issue and accept instructions in Appendix 3.

(3) In the event of a change to the above-mentioned individuals or if they are subject to long-term incapacitation, the other party shall be immediately informed of any successors or representatives.

(4) The Processor shall immediately inform the Controller if an instruction issued by the Controller violates, in his opinion, legal requirements. The Processor shall be entitled to forego carrying out the relevant instructions until they have been confirmed or changed by the party responsible on behalf of the Controller.

(5) The Processor is to document the instructions issued and their implementation.

§11 Ending the commissioned processing

(1) When terminating the contractual relationship or at any time upon the Controller's request, the Processor must either destroy the data processed as part of the commission or submit the data to the Controller at the Controller's discretion. All copies of the data still present must also be destroyed. The data must be destroyed in such a way that restoring or recreating the remaining information will no longer be possible, even with considerable effort. Any physical destruction shall be carried out in accordance with DIN 66399.

(2) The Processor is obligated to immediately ensure the return or deletion of data from subcontractors.

(3) The Processor must provide proof of the data being properly destroyed and immediately submit this proof to the Controller.

(4) Any documentation that serves the purpose of providing proof of proper data processing, shall be kept by the Processor according to the respective retention periods, including the statutory period after the contract has expired. The Processor may submit the respective documentation to the Controller once his/her contractual obligations have ended.

§12 Remuneration

(1) The Processor's remuneration is conclusively stipulated in the Master Contract. There is no separate remuneration or reimbursement provided in this contract.

§13 Liability

(1) The Controller and the Processor shall be jointly liable for compensation to anyone for damage caused by any unauthorised party or for incorrect data processing within the scope of the contract.

(2) The Processor shall bear the burden for proving that any damage is not the result of circumstances that he/she is responsible for insofar as the relevant data have been processed under this agreement. If this proof has not been provided, the Processor shall, when initially requested to do so, release the Controller from all claims that are levied against the latter in connection with the data processing.

(3) The Processor shall be liable to the Controller for any damages culpably caused by the Processor, his/her employees or appointed subcontractors or the contract-executing agency in connection with rendering the contractual service requested.

(4) Sections 13 (2) and 13 (3) shall not apply if the damage occurred as a result of correctly implementing the service requested or an instruction provided by the Controller.

§14 Contractual penalty

(1) In the event that the terms of this contract are breached, a contractual penalty of 1.500€ per individual case will apply. The contractual penalty shall, in particular, be forfeited in the case of deficiencies implementing the agreed upon technical and organisational measures. In the event of permanent infringements, every calendar month in which the infringement is wholly or partly present shall be considered an individual case. Any exemption to the offence deemed as continuing shall be ruled out.

(2) The contractual penalty shall have no impact on any of the Controller's other claims.

§15 Right to extraordinary termination

(1) The Controller may, at any time, terminate the Master Contract and this contract without notice ('extraordinary termination') if a serious infringement of data protection regulations or the provisions of this contract exists on part of the Processor, if the Processor cannot or will not execute the client's legal instructions or if the Processor refuses to accept the Controller's supervisory rights, in violation of this contract.

(2) A serious breach shall, in particular, be deemed to have occurred if the Processor has not substantially fulfilled or failed to fulfil the obligations laid down in this agreement, in particular the technical and organisational measures.

(3) For insignificant breaches, the Controller shall provide the Processor with a reasonable period of time to remedy the situation. Should the situation not be remedied in good time, the Controller shall be entitled to extraordinary termination as stipulated here.

(4) The Processor shall reimburse the Controller all costs arising from the premature termination of the Master Contract or this contract as a result of the Controller exercising his/her right to an extraordinary termination.

§16 Miscellaneous

(1) Both Parties are obligated to treat all knowledge of trade secrets and data security measures, which have been obtained by the other party within the scope of the contractual relationship, confidentially, even after the contract has expired. If there is any doubt as to whether information is subject to confidentiality, it shall be treated confidentially until written approval from the other party has been received.

(2) Should the Controller's property be threatened by the Processor by third-party measures (e.g. by seizure or confiscation), by insolvency or settlement proceedings or by other events, the Processor shall immediately notify the Controller.

(3) Any ancillary agreements must be in writing.

(4) An exemption to the right of retention in terms of § 273 BGB is ruled out with regard to the data processed and the associated data carriers.

(5) Should any parts of this agreement be invalid, this will not affect the validity of the remainder of the agreement.