Terms and conditions

1 Preamble

1.1 Unless otherwise agreed in writing between the Licensee and SynergyXR, the following General Terms and Conditions ('GTC') apply to all free trials, services, subscriptions and deliveries by SynergyXR ApS, a Danish corporation with its principal place of business at Silkeborgvej 261-263, DK-8230, Åbyhøj, Denmark ("**SynergyXR**"), and any contracting party (individual or entity) to which SynergyXR provides the SynergyXR Software ("**Licensee**") (each a "**Party**" jointly the "**Parties**"). The Licensee' explicitly agrees, that the Licensee's purchasing conditions, customary practice etc., or any conflicting, contrary or additional terms and conditions contained in any communication from Licensee to SynergyXR shall not apply unless such additional terms and conditions are expressly accepted in writing by SynergyXR.

1.2 SynergyXR provides the Licensee as a subscription service access to 3D, augmented reality and virtual reality software, systems, plug-ins and services (hereinafter referred to as "the SynergyXR Software"). Licensee wishes to gain access to the SynergyXR Software and related services.

1.3 Any changes and amendments to the Agreement must be agreed in writing. In case of any discrepancies in the terms of the Agreement, the commercial terms of the Scope of Works shall take precedence over the GTC and its appendices.

2 Definitions

"**Affiliate**" means, with respect to a party, any entity that directly or indirectly Controls, is Controlled by, or is under common Control with that party, where "Control," "Controlled by," and "under common Control with" mean possession, directly or indirectly, through one or more intermediaries, of the power to direct or cause the direction of management or policies of such entity, whether through ownership of equity, voting or other interests, by contract, or otherwise.

"**The Agreement**" means these GTC and its schedules, respectively Schedule 1 (Data Processing Agreement) and Schedule 2 (Service Level Agreement) as well as a Scope of Works indicating the parties and the commercial terms of the arrangement.

"**Data Processing Agreement"** means the content of Schedule 1 to these GTC.

"**Effective Date**" means the date that SynergyXR make SynergyXR Software available to Licensee (whether as free trial or payable).

"**Intellectual Property Rights**" means any and all patents, utility models, rights to inventions, copyright and neighbouring and related rights, moral rights, trademarks and service marks, business names and domain names, rights in get up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, confidential information (including Know-How and trade secrets) and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

"**Know How**" means all technology, source code, object code, local area network manager code, technical information, procedures, processes, trade secrets, methods, practices, techniques, information, logic/flow charts, sketches, drawings, specifications, application- and modification manuals and data relating to the design, manufacture, inspection, and testing of the SynergyXR Software, which are from time to time in SynergyXR's possession.

"**Licensee**" any customer or free trial user of the SynergyXR Software.

"**Service Level Agreement"** or **"SLA"** means the content if Schedule 2 to these GTC.

"**SynergyXR Software**" means the 3D, augmented reality and virtual reality software (including associated services) developed and provided by SynergyXR to Licensee.

"**Term**" and "**Renewal Term**" has the meaning provided in Section 10 of these GTC.

3 Use of SynergyXR Software

3.1 Subject to the Agreement and during the Term, SynergyXR grants Licensee a limited, revocable, non-exclusive, non-transferable, non-sublicensable license to utilize SynergyXR Software for the purpose of the Agreement.

3.2 The Licensee shall be entitled to use the SynergyXR Software only for its own use. Licensee is not permitted to sub-license, rent, sell or in any form transfer the rights to use SynergyXR Software without prior written approval from SynergyXR. All licenses acquired by Licensee shall be personal on user-level and cannot be shared.

3.3 SynergyXR may make any alterations to the SynergyXR Software that are required to ensure compliance with all relevant laws and regulations. SynergyXR reserves the right at any time to make changes in the SynergyXR Software by removing, adding, modifying features or functions or to provide fixes, updates and upgrades, provided that such

changes do not materially alter the core features or functionality of the SynergyXR Software. Such changes may also involve SynergyXR changing subcontractors or sub-processors of personal data. To the extent that there is a change of sub-processors, such change shall be handled in accordance with Schedule 1 (Data Processing Agreement).

3.4 SynergyXR will provide support in accordance with Schedule 2 (Service Level Agreement).

4 Intellectual Property Rights

4.1 Licensee acknowledges and agrees that SynergyXR owns all Intellectual Property Rights, title, Know How, and interest in and to the SynergyXR Software (including any and all deployed associated services). SynergyXR reserves all rights not expressly granted to Licensee under the Agreement.

4.2 No rights or licenses are granted to disclose, to distribute, or to disseminate the SynergyXR Software or any part of hereof.

4.3 SynergyXR confirms that it has all the rights in relation to the SynergyXR Software (including any and all deployed associated services) to fulfill the terms of this Agreement, including any third-part software included in the SynergyXR Software. SynergyXR shall defend, indemnify, and hold Licensee harmless from and against any claims brought by a third party alleging that the Licensee's use of the SynergyXR Software infringes or violates any third party Intellectual Property Rights

4.4 The Licensee warrants that the Licensee's information, material and trademarks uploaded to the SynergyXR Software does not infringe any third-party rights. The Licensee must indemnify SynergyXR against any third-party claims or any damages caused by any actions by Licensee in the Synergy XR Software. The Licensee hereby grants to SynergyXR a royalty-free, non-exclusive and unrestricted license to use, copy, adapt, transmit and display Licensee's Intellectual Property Rights in the SynergyXR Software solely for the purposes of fulfilling the Agreement with Licensee.

4.5 Each Party shall retain all Know-How and Intellectual Property Rights, owned by the respective Party.

5 Licensee's obligations

5.1 Licensee is not allowed and shall not allow any third party to: (a) make modifications, translations, dissemble, decompile or reverse engineer, or create derivative works based on or (wholly or partially) by copying any coding embodied in the SynergyXR Software; (b) circumvent limits or other timing or use restrictions that are embodied in the SynergyXR Software; (c) remove proprietary notices or marks from or in the SynergyXR Software; (d) frame or mirror any content forming part of the SynergyXR Software, other than as necessary for the permitted use of the SynergyXR Software according to the Agreement and these GTC (e) access the SynergyXR Software to try to build a competitive product or service, or to copy any ideas, features, functions or graphics of the SynergyXR Software; or (f) use the SynergyXR Software (wholly or partially) for any hazardous or illegal purposes nor any purpose in which the failure of the SynergyXR Software could lead to death, personal injury, or severe physical or environmental damage.

5.2 The Licensee shall take reasonable steps to prevent unauthorized access to the SynergyXR Software, by protecting its passwords and other log-in information. The Licensee shall notify SynergyXR immediately of any known or suspected unauthorized use of the SynergyXR Software or breach of its security and shall use best efforts to stop said breach.

5.3 The Licensee shall not access, store, distribute or transmit any viruses or any material during its use of the SynergyXR Software that is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive.

6 Licensee's data

6.1 Licensee exclusively owns all rights, title and interest in and to all Licensee's own data. SynergyXR shall not access Licensee's data, except to respond to service or technical problems or at Licensee's request or as necessary for the operation of the SynergyXR Software. Licensee hereby grants SynergyXR a royalty-free, non-exclusive, non-transferable, license for the Term (and for ninety (90) days thereafter) to host, process, transmit, copy, display, use and otherwise exploit Licensee's data to the extent reasonably required for SynergyXR to perform its obligations pursuant to the Agreement and to comply with legal requirements or as expressly permitted in writing by the Licensee. This license shall inter alia include the right to use and copy Licensee's data with the purpose of creating anonymized statistical analytics with respect to the SynergyXR Software, and such statistical analytics shall be owned by SynergyXR.

6.2 The Licensee warrants that the Licensee's collection and use of any personal information or data provided while using the SynergyXR Software complies with all applicable data protection laws, rules, and regulations.

6.3 SynergyXR does not screen content uploaded to the SynergyXR Software but reserves the right (but not the obligation) to remove any content that violates the Agreement or otherwise violates third parties' Intellectual Property Rights or any applicable laws. The Licensee acknowledges and agrees that SynergyXR does not verify, adopt, ratify, or sanction Licensee's content and the Licensee agrees that the Licensee is solely responsible for and must bear all risks associated with the Licensee's use of the SynergyXR Software.

6.4 Licensee warrants that the content uploaded to the SynergyXR Software does not violate any intellectual property rights of third party. The Licensee shall hold SynergyXR harmless against any expense, judgement, or loss for alleged infringement of any rights of third party related to uploaded content.

7 Personal data protection

7.1 SynergyXR processes personal data of the users of the SynergyXR Software. Information on how SynergyXR process the personal data is further described in the applicable privacy policy available at the SynergyXR website. By entering into the Agreement, Licensee confirms to have read and accepted the terms comprised by SynergyXR' privacy policy and to make such information available to any of its designated users.

7.2 If Licensee uploads content which includes personal data to the SynergyXR Software SynergyXR is assessed to be a data processor of the Licensee. Thus, the parties have agreed to the Data Processing Agreement attached as Schedule 1 governing the processing of personal data by SynergyXR on behalf of Licensee. The Licensee is advised not to upload any special categories of personal data (including criminal convictions and offences) to the SynergyXR Software.

8 Compliance audit

8.1 To ensure Licensee's compliance with the Agreement and these GTC, Licensee agrees that upon SynergyXR' request, Licensee shall within 20 days provide all records and information reasonably requested by SynergyXR in order to verify that Licensee's installations and use of the SynergyXR Software (including any and all deployed associated services) are in compliance with the Agreement.

9 Confidentiality

9.1 Both parties undertake to keep confidential any and all information exchanged by the parties which is either indicated as confidential or, due to its nature, should be kept confidential, including but not limited to SynergyXR's Intellectual Property Rights, Know How and information about prices with the exception of those instances where the disclosure of such information is necessary in order for the party to fulfil its obligations under the Agreement.

9.2 The confidentiality obligation of the parties shall continue to apply after the termination of the Agreement. It shall not apply to the extent that the information exchanged is or subsequently becomes publicly available, unless such public availability is the result of a breach of the Agreement.

10 Term and Termination

10.1 The Term of the Agreement will commence on the Effective Date and continue in effect until the free trial has ended or in accordance with the provisions of the Scope of Works (whichever is the latest) ("Term").

10.2 Excluding any free trials, the Agreement shall be automatically renewed at the end of the Term for a further period of equal to the Term (the "Renewal Term") and shall be automatically renewed on the same basis at the end of each subsequent Renewal Term unless either Party gives to the other Party notice in writing to terminate this Agreement no less than 30 days the Term, or the Renewal Term, as the case may be.

10.3 Unless otherwise agreed in writing, the subscription charges applicable to Licensee's subscription to the SynergyXR Software (including any and all deployed associated services) for any Renewal Term shall continue as fixed in previous Term or Renewal Term, safe for any regulation pursuant to clause 10.4.

10.4 By providing a written notice of 30 days to Licensee, SynergyXR shall have the right to adjust the subscription charges each year, as of the first day of January, in proportion to the increase in the Danish Net Price Index in the preceding 12 months or to account for any increase in the costs charged by SynergyXR's suppliers to the extent such costs forms part of the charges payable by the Licensee for the SynergyXR Software.

10.5 SynergyXR reserves the right to restrict functionality, suspend or terminate the services to the SynergyXR Software (or any part thereof including any and all deployed associated services), remove, disable and quarantine any data provided through the SynergyXR Software (or any part thereof including any and all deployed associated services) in case of Licensee's breach of the Agreement. Unless legally prohibited from doing so, SynergyXR will use commercially reasonable efforts to contact Licensee directly via email to notify Licensee when taking any of the foregoing actions. SynergyXR shall not be liable to Licensee or any other third party for any such modification, suspension or discontinuation of Licensee's rights to access and use the SynergyXR Software (or any part thereof including any and all deployed associated services).

10.6 Both SynergyXR and the Licensee may terminate the Agreement for cause (a) upon written notice to the other Party of a material breach if such breach remains uncured at the expiration of thirty (30) days from the date of the breaching party's receipt of such notice; or (b) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. If the Agreement is terminated by Licensee in accordance with this section, SynergyXR will, to the extent permitted by applicable law, refund Licensee any prepaid subscription charges for the period after the effective date of termination. If the Agreement is

terminated by SynergyXR in accordance with this section, Licensee is obliged to pay any unpaid subscription charges covering the remainder of applicable Term. In no event will termination relieve Licensee's obligation to pay any subscription charges payable to SynergyXR for the period prior to the effective date of termination.

10.7 In the event of any termination of the Agreement by either party, Licensee must cease all use of the SynergyXR Software.

11 Limitation of Liability

11.1 The SynergyXR Software is provided as is. Under no circumstances and under no legal theory (whether in contract, tort, negligence or otherwise) shall either Party to this Agreement, or their respective affiliates, officers, directors, employees, agents, service providers, suppliers or licensors, be liable to the other Party or its affiliates for any lost profits, lost sales or business, lost data (where such data is lost in the course of transmission through Licensee's systems or over the internet through no fault of SynergyXR), business interruption, loss of goodwill, costs of cover or replacement, or for any other type of indirect, incidental, special, exemplary, consequential or punitive loss or damages, or for any other indirect loss or damages incurred by the other party or its affiliates in connection with this Agreement, regardless of whether such party has been advised of the possibility of or could have foreseen such damages.

11.2 Notwithstanding anything to the contrary in this Agreement, SynergyXR's aggregate liability arising out of this Agreement shall in no event exceed the subscription charges paid by Licensee during the twelve (12) months prior to the first event or occurrence giving rise to such liability. Licensee acknowledge and agree that the essential purpose of this section 11.2 is to allocate the risks under this Agreement between the Parties and limit potential liability given the subscription charges, which would have been substantially higher if SynergyXR were to assume any further liability other than as set forth herein. The limitations set forth in section 11.2 shall not apply to claims or damages resulting from third party claims subject to clause 4.3 of the GTC.

11.3 In no event shall SynergyXR be responsible for remedying damages caused by (a) the incorrect or unauthorized use of SynergyXR Software, (b) unauthorized repairs carried out by the Licensee or third parties, or (c) any act or omission by the Licensee or a third party.

11.4 SynergyXR shall be entitled to suspend provision of the SynergyXR Software if the Licensee is in material breach of its obligations under this Agreement and such breach is not remedied (or reasonably demonstrated not to constitute a breach) within 30 days of SynergyXR's written notice to the Licensee specifying the alleged breach.

12 Force Majeure

12.1 SynergyXR shall not be liable for any delay or non-performance of its obligations where such delay or non-performance is attributable to circumstances beyond SynergyXR's control, including but not limited to industrial disputes (including global and local strikes and/or lockouts), fires, wars, uprisings, civil unrest, acts of terrorism, natural disasters, currency restrictions, computer viruses, worms etc., import or export bans, breakdowns or disruptions in telecommunication or electricity or, as well as any similar conditions affecting a sub supplier's performance vis-à-vis SynergyXR.

12.2 In case the consequences of a force majeure event extend for a period of more than one (1) month, either party shall be entitled to terminate the Agreement by giving fourteen (14) days' written notice for expiry at the end of a month.

13 Marketing

13.1 Any free trial subscription to the SynergyXR Software is conditioned upon the Licensee providing its consent to receive marketing material and emails from SynergyXR. Any such consent can be withdrawn.

13.2 SynergyXR shall be allowed to – at all times acting loyal and in good faith – disclose or permit disclosure of the existence of this Agreement to any third party, disclose that the Licensee is its customer to any third party; and use the Licensee's name and/or brand in any promotion or marketing related to the SynergyXR Software.

14 Miscellaneous

14.1 Licensee shall have no right to assign its rights or obligations in full or in part without the prior written approval from SynergyXR.

14.2 The Agreement constitute the entire, final and exclusive understanding and agreement between the Parties pertaining to the subject matter hereof, and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions whether oral or written, of the Parties. The provisions of the Agreement may not be amended or supplemented unless such amendment or supplement is agreed in writing between the Parties.

14.3 The Parties have the status of independent contractors, and nothing in the Agreement shall be deemed to place the parties in the relationship of principal-agent, partners or joint ventures, nor to confer on either Party any express or implied right, power or authority to enter into any agreement or commitment on behalf of the other Party, nor to impose any obligation upon the other Party.

14.4 Should any provision of the Agreement be held to be void, invalid or inoperative, the remaining provisions

of the Agreement shall not be affected and shall continue in effect.

14.5 All notices under the Agreement by Licensee shall be made in writing and sent by email to contact@synergyxr.com or to SynergyXR ApS, at Silkeborgvej 261-263, DK-8230, Åbyhøj, Denmark.

15 Governing Law and Venue

15.1 Any dispute arising out of or in connection with this contract, including any disputes regarding its existence, validity or termination, which the Parties have been unable to settle amicably, shall be finally settled by arbitration administered by the Danish Institute of Arbitration in accordance with the Rules of Arbitration adopted by the Board of the Danish Institute of Arbitration. The arbitration shall take place in Aarhus, Denmark. The language of the arbitral proceedings shall be English.

15.2 The laws of Denmark, excluding any choice of law rules, shall govern the Agreement and the settlement of disputes. The United Nations Convention on Contracts for the International Sale of Goods (CISG) shall not apply.

Schedule 1
Data processing agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) between Licensee (the data controller) and SynergyXR ApS (the data processor) have on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1 Preamble

1.1 These Contractual Clauses set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

1.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 (General Data Protection Regulation).

1.3 In the context of the provision of 3D, augmented reality and virtual reality software, systems and services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

1.4 The Clauses shall take priority over any similar provisions contained in other agreements between the Parties.

1.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.

1.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

1.7 Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

1.8 Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

1.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

1.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

1.11 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2 The rights and obligations of the data controller

2.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State1 data protection provisions and the Clauses.

2.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

2.3 The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3 The data processor acts according to instructions

3.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

3.2 The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4 Confidentiality

4.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

4.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5 Security of processing

5.1 Article 32 GDPR stipulates that, 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, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

5.2 The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

5.2.1 Pseudonymisation and encryption of personal data;

5.2.2 the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.3 According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

5.4 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

5.5 If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6 Use of sub-processors

6.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

6.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

6.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 4 weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

6.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

6.5 The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

6.6 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6.7 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR

– against the data controller and the data processor, including the sub-processor.

7 Transfer of data to third countries or international organisations

7.1 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

7.2 In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

7.3 Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

7.3.1 transfer personal data to a data controller or a data processor in a third country or in an international organization;

7.3.2 transfer the processing of personal data to a sub-processor in a third country;

7.3.3 have the personal data processed by the data processor in a third country.

7.4 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

7.5 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8 Assistance to the data controller

8.1 Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

8.2 This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

8.2.1 the right to be informed when collecting personal data from the data subject;

8.2.2 the right to be informed when personal data have not been obtained from the data subject;

8.2.3 the right of access by the data subject;

8.2.4 the right to rectification;

8.2.5 the right to erasure ('the right to be forgotten');

8.2.6 the right to restriction of processing;

8.2.7 notification obligation regarding rectification or erasure of personal data or restriction of processing;

8.2.8 the right to data portability;

8.2.9 the right to object;

8.2.10 the right not to be subject to a decision based solely on automated processing, including profiling.

8.3 In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

8.3.1 The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

8.3.2 the data controller's obligation to without undue delay communicate 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;

8.3.3 the data controller's 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);

8.3.4 the data controller's obligation to consult the competent supervisory authority, 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 data controller to mitigate the risk.

8.4 The Parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

9 Notification of personal data breach

9.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

9.2 The data processor's notification to the data controller shall, if possible, take place within 36 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

9.3 In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

9.3.1 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;

9.3.2 the likely consequences of the personal data breach;

9.3.3 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.

9.4 The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10 Erasure and return of data

10.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

11 Audit and inspection

11.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

11.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

11.3 The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12 The parties' agreement on other terms

12.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13 Commencement and termination

13.1 The Clauses shall become effective on the date of both parties' signature.

13.2 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

13.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

13.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

13.5 This data processing agreement form an appendix to the GTC between the Parties and shall be considered duly signed and valid upon the commencement of the GTC.

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The data processor provides the data controller private access to 3D, augmented reality and virtual reality software, systems and services. The data controller gain access to servers, applications, plug-ins and related software and services in order to use the opportunity and feasibility to change work-related procedures, instructions, collaboration and support across multiple work situations or any purpose considered relevant by the data controller. Insofar any personal data will be submitted by the data controller to such systems and

services, this personal data in question will be subject to this data processing agreement. Consequently, any data (and processing hereof) not considered personal data subject to the GDPR shall be excluded from the terms of this data processing agreement.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The data controller will have access to a dedicated, private 3D, augmented reality and virtual reality software in which the data controller may – at its own discretion – upload and interact with personal data of the data controller's choice. The data controller will make decisions on the nature of the processing of personal data upon the submission of such and the interactions within the software, such processing activities may consist of (but is not limited to) storage, back-up, presentation and systematization.

A.3. The processing includes the following types of personal data about data subjects:

The processing includes all types of personal data that the data controller provides to the data processor. Any decision from the data controller to submit, provide, make available or in any other manner to share or transfer personal data to the data processor shall be considered an instruction to process such personal data.

Personal data may consist of (but is not limited to) name, e-mail address, telephone number, address, portrait- or other photos and/or videos containing persons.

A.4. Processing includes the following categories of data subject:

The processing includes all categories of personal data that the data controller provides to the data processor. Any decision from the data controller to submit, provide, make available or in any other manner to share or transfer personal data to the data processor shall be considered an instruction to process personal data on the applicable categories of data subjects.

The categories of data subjects may include (but is not limited to) employees, independent contractors, customers or suppliers.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The processing is not time-limited and is carried out during any applicable Term or Renewal Term.

Appendix B Authorised sub-processors

B.1. Approved sub-processors
On the Effective Date, the data controller authorises the engagement of the following sub-processors:

A Microsoft Ireland Operations Limited, IE256796, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Irland. Providing system hosting (Azure).

B Exit Games GmbH, Hongkongstr. 7, 20457 Hamburg, Germany. Providing service hosting (Photon multi-player)

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor gives the data controller a notice of 28 days (4 weeks) prior to the replacement or addition of a sub-processor. From the receipt of the data processor's notice, the data controller must object to the change within 14 days, otherwise the addition or replacement of the sub-processor in question shall be deemed to have been accepted. Any objection from the data controller must be factual and reasoned.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing
The data processor shall perform the processing activities required to provide the services as described in the main agreement to which these Clauses form an appendix.

The data processor may anonymize personal data and process such anonymized data for statistical purposes and further development of the data processor's offerings.

C.2. Security of processing

The level of security shall take into account that the processing does not involve a large volume of personal data nor personal data as defined in Article 9 GDPR on 'special categories of personal data'. The Parties agree that a medium level of security is sufficient in order to protect the personal data processed.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security. The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Access control of processing areas

Data processor implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas,
- protection and restriction of access paths,
- establishing access authorizations for employees and third parties, and
- the data center where personal data are hosted is secured by appropriate security measures.

Access control to data processing systems

Data processor implements suitable measures to prevent their data processing systems from being accessed or used by unauthorized persons, including:

- use of adequate encryption technologies,
- identification of the terminal and/or the terminal user to the data processor and processing systems,
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen, and
- access to data content is logged, monitored, and tracked.

Access control to use specific areas of data processing systems

Data processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data,
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions,
- monitoring capability in respect of individuals who delete, add or modify the personal data,
- release of data only to authorized persons, including allocation of differentiated access rights and roles,
- use of adequate encryption technologies, and
- control of files, and controlled destruction of data.

Availability control

Data processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy,
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission control

Data processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels; and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input control

Data processor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel,
- utilization of unique authentication credentials or passwords,
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked,
- automatic log-off of user ID's that have not been used for a substantial period of time,
- proof established within data processor's organization of the input authorization, and
- electronic recording of entries.

Separation of processing for different purposes

Data processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users,
- modules within the data processor's database separate which data is used for which purpose, i.e. by functionality and function, and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this appendix C.2.

Monitoring

Data processor shall implement suitable measures to monitor access restrictions to data processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators,
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months, and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The rights of data subjects:

Following specific instructions from the data controller, the data processor must obtain or submit personal data, delete personal data (including backup, if possible) or rectify personal data about a data subject, and limit the processing of personal data about a data subject.

If the data processor transmits personal data to the data controller, this must be done in a structured, commonly used and machine-readable format.

The data processor instructs employees in the handling of the data subjects' rights and has implemented procedures for how the data processor assists the data controller in answering requests from data subjects.

Notification of personal data breach

The data processor must notify the data controller of any personal data breach.

If the data processor discovers a personal data breach, the data processor must take the necessary measures to limit the negative consequences of the breach and to limit its recurrence.

The data processor has a procedure for handling security breaches, which ensures that the data processor informs the data controller about security breaches and supports the parties' cooperation to deal with the breach.

The data processor shall assist the data controller in providing the information necessary to report the personal data breach to the relevant supervisory authority. The data processor shall not report a breach to the relevant supervisory authority on behalf of the data controller.

C.4. Storage period/erasure procedures

Personal data is stored for the duration of the Term or Renewal Term or until the data controller decides to erase the personal data from the SynergyXR Software. The data controller is able and authorized to erase personal data at its own discretion.

If the data processor is not instructed to erase or return the personal data within ninety (90) days after the termination of Agreement, the data processor will be entitled to delete the data controller's data and all copies thereof. The data processor sends confirmation of the erasure to the data controller upon request.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

- Any sub-processor's location
- The data processor's location and home workspaces

C.6. Instruction on the transfer of personal data to third countries

Data controller approves the sub processors and third country data transfers set out in B.1 above. The legal basis for the third country data transfers are the EU Standard Contractual Clauses.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, e.g. by approval of a new or changes to a sub-processor, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data controller or a representative of the data controller may, at appropriate intervals, carry out supervision regarding the data processor's performance of this data processing agreement.

The Parties agree that in the view of the nature of the processing and the content of the personal data provided, the supervision may be carried out by the data processor confirming its compliance with this data processing agreement upon request from the data controller. If the data controller provides a risk assessment providing for a more detailed supervision, written supervision may be carried out using statements or questionnaires. The data controller has the right

to carry out a physical inspection of it is deemed necessary in accordance with the data controller's risk assessment.

Any expenses of the data controller in connection with a physical inspection are paid by the data controller itself. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the data controller to carry out its supervision.

If the data processor decides (without any obligation hereto) to obtain an auditor's report from a state authorised public accountant concerning the data processor's general compliance with the data protection regulation, such report shall be considered an adequate supervision of the data processor's activities and these Clauses.

The parties have agreed that an SOC2, ISAE 3402 or ISAE 3000 report or any other auditing standards which may be alternative to or supersede said standards is adequate.

The reports will be generic and relate to multiple clients supported by the data processor.

Based on the results of an audit/inspection or the certification, the data controller may request further measures to be taken to ensure compliance with the data protection legislation, the applicable EU or Member State data protection provisions and the Clauses, safe for the remuneration agreed in Appendix D.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor or a representative of the data processor shall, at appropriate intervals, carry out written or physical supervisions of the sub-processors related to the agreement in order to establish the sub-processor's compliance with the data protection legislation and these Clauses. Such supervision may take place in writing by obtaining independent audit reports, obtaining information through questionnaires, written confirmation of the sub-processor's compliance or the like.

In addition to the planned supervision, the data processor may carry out an inspection with the sub-processor when the data processor (or the data controller) deems it necessary.

Documentation of the data processor's supervision is upon request forwarded to the data controller for information.

If the results of the supervision clearly demonstrates non-compliance to material provisions of the data protection regulation, the data controller is entitled to request the implementation of additional measures to ensure compliance with the data protection regulation, data protection provisions of other Union law or the national law of the Member States and these Clauses safe for the remuneration agreed in Appendix D.

Appendix D The parties' terms of agreement on other subjects

Remuneration

Within a cap of 30 minutes per request, the data processor shall provide, free of charge, the assistance to the data controller that may reasonably be required of a data processor under the data protection legislation, such as the time spent in connection with the data controller's supervision and the data processor's assistance pursuant to Article 32 – 36 of the GDPR. Any time exceeding the cap will be invoiced at the standard hourly rates of the data processor.

If the data controller requests the provision of services or assistance from the data processor, which is outside the requirements of data protection legislation, the data processor is entitled to separate remuneration for this in accordance with the data processor's standard hourly rates and reimbursement of positive expenses.

If the data controller requires the data processor to take specific measure to ensure a higher level of technical and organisational security, the data processor is entitled to claim payment for the costs associated with this if the measures cannot be considered a general requirement under the data protection legislation. The costs may be, but is not limited to, the hourly rate of time spent, the costs of IT systems, security measures or physical measures.

Schedule 2
Service Level Agreement

1 Background

1.1 This Service Level Agreement describe the Service Levels that SynergyXR shall provide for operation of the SynergyXR Software to Licensee.

1.2 Licensee is responsible for any hardware, local infrastructure, operating systems and basic software necessary to acquire services from SynergyXR as well as the operability hereof.

2 Definitions

The following supplementary definitions shall apply to this SLA:

"Availability" is the percentage of time that the SynergyXR Software shall be operational and can be used by Licensee and its End-Users. This excludes any time used for maintenance activities ("Maintenance Windows").

"End-User" is the permitted users of the Licensee.

"Incident" is any event that is not part of the standard services, and which causes or may cause disruption to or reduction in the quality of SynergyXR Software.

"Maintenance Windows" means 1) Saturday from 9:00 to Sunday 22:00 CET and 2) any other times needed for urgent updates. Downtime may be required in the Maintenance Windows.

"Incident Closure" means by solving the problem, solving the problem temporarily or establishing a workaround considered acceptable by SynergyXR with regards to an Incident

"Response Time" is the time taken for SynergyXR to respond to an Incident following notification by Licensee to SynergyXR

"Resolution Time" is defined as the time taken for SynergyXR from reacting to an Incident and until Incident Closure excluding any pauses at set out in clause 5.3(b).

"Service Incident Levels" are the definition of levels as set out in the table in clause 4.1

"Service Levels" is the targets set out in the tables in section 3 which SynergyXR's performance will be measured against.

"Target" is the minimum percentage of Incidents that will be resolved within the resolution time. The target is set to allow some leeway for certain Incidents that take longer than the prescribed amount of time due to their nature.

"Update" Changes that update, upgrade, or alter the behavior of the SynergyXR Software or fixes specific problems, modify or introduce new functionalities or any other change that alter the SynergyXR Software

"Working Day" means Danish business days, 8 a.m. to 5 p.m. Monday to Friday CET.

"Working Hours" means the hours in a Working Day.

3 Service Levels

3.1 SynergyXR will use best efforts to ensure that the SynergyXR Software meets below Availability, measured on a monthly basis.

Service Level	Availability
Scheduled up time on Working Days	98,5%

3.2 The scheduled Availability is calculated on a quarterly basis excluding downtime during Maintenance Windows.

4 Service Incident definition

4.1 Incidents effect on business operations are based on a combination of the impact on the business as defined in clause 4.2 - 4.4 and the urgency of the Incident as defined in clause 4.5 - 4.7. and is categorized in the following Incident matrix with the specified levels (1-4):

Service Incident Level Definition		Urgency		
		High	Medium	Low
Impact	High	1	2	3
	Medium	2	3	4
	Low	3	4	4

Impact levels

4.2 High

4.2.1 There is a possibility of personnel getting injured.

4.2.2 A large number of End-Users are affected and/or not able to utilize the SynergyXR Software at all.

4.2.3 The financial impact of the Incident is likely to increase rapidly if not solved.

4.2.4 The damage to the reputation of the business is likely to increase rapidly if not solved.

4.2.5 The damage to the reputation of the business is likely to be very high.

4.3 Medium

4.3.1 A moderate number of End-Users are affected and/or not able to utilize the SynergyXR Software properly.

4.3.2 The financial impact of the Incident is increasing, but not rapidly.

4.3.3 The damage to the reputation of the business I likely to be moderate.

4.4 Low

4.4.1 A minimal number of End-Users are affected and/or able to utilize the SynergyXR Software but this requires extra effort.

4.4.2 The financial impact of the Incident is not likely to increase.

4.4.3 The damage to the reputation of the business is likely to be minimal.

Urgency levels

4.5 High

4.5.1 The damage caused by the Incident increases rapidly.

4.5.2 Work that cannot be completed by End-Users is highly time sensitive.

4.5.3 A medium impact can be prevented from becoming a high impact by acting immediately.

4.6 Medium

4.6.1 The damage caused by the Incident increases considerably over time.

4.6.2 Work that cannot be completed by End-Users is somewhat time sensitive

4.6.3 A medium or low impact is not likely to become a high impact.

4.7 Low

4.7.1 The damage caused by the Incident only marginally increases over time.

4.7.2 Work that cannot be completed by staff is not time sensitive

4.7.3 A low or medium impact that will not become a high impact.

4.8 Any Impact Level and Urgency Level shall be decided by SynergyXR in good faith and based on the general applicability of the SynergyXR Software.

4.9 An Incident shall be reported to SynergyXR by e-mail to the following e-mail address: support@synergyxr.com

5 Response and Resolution Time

5.1 SynergyXR Response Time

(a) Support Working Hours
SynergyXR shall provide support during the Working Hours.

(b) Response Time
SynergyXR shall provide Response Time at least in accordance with the time set forth in the following table in accordance with the Service Incident Level Definition:

Incident Level	Response Time (Target)
1-2	within 24 Working Hours of at least 85% of the Incidents
3-4	within 72 Working Hours of at least 85% of the Incidents

(c) Resolution Time
SynergyXR does not guarantee any specific Resolution Time. If the Resolution Time is likely to exceed the Target Response Time, SynergyXR shall use its best endeavors to keep the Customer informed on the Incident and expected Incident Closure during the Resolution Time.

5.2 SynergyXR may decide to restore the SynergyXR Software and seek Incident Closure by rolling back to a previous version and recall an Update.

5.3 In section 5.1 the following shall apply in the assessment of the response, answering, reaction and Resolution Times referred to therein:

(a) The response, answering, reaction or resolution time starts when the Incident giving rise to the response, answering, reaction or Resolution Time is reported to SynergyXR as set out in clause 4.9.

(b) The response, answering, reaction or Resolution Time is paused:

(i) pending information requested by SynergyXR to be provided by Customer regarding the End-User, or

(ii) pending third party assistance where necessary (for instance Microsoft or any other service provider)

(iii) time outside Working Day, and

(iv) during any Maintenance Windows