Appendix to the Terms of Service of SynergyXR ApS

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Any SynergyXR customer subject to the general Terms of Service of SynergyXR to which this data processing agreement form an integrated appendix

(the data controller)

and

SynergyXR ApS
CVR 31177626
Silkeborgvej 261 – 263
8230 Åbyhøj
Denmark
(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED 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. Table of Contents

2. Preamble

1. These Contractual Clauses (the 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.

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).

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.

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

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

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.

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.

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.

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

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

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.

3. The rights and obligations of the data controller

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 State[1] data protection provisions and the Clauses.

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

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

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.

4. The data processor acts according to instructions

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.

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.

5. Confidentiality

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 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.

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.

6. Security of processing

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.

   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:
   - Pseudonymisation and encryption of personal data;
   - the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

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

2. 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.

3. 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.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require 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.

7. Use of sub-processors

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).

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.

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.

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.

   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.

5. 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. 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.

8. Transfer of data to third countries or international organisations

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.

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.

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

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

    b. transfer the processing of personal data to a sub-processor in a third country

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

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.

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.

9. Assistance to the data controller

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.

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

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. 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:

   a. 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;

   b. 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;

   c. 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);

   d. 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.

3. 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.

10. Notification of personal data breach

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.

2. The data processor's notification to the data controller shall 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.

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:

    a. 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;

    b. the likely consequences of the personal data breach;

    c. 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.

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.

11. Erasure and return of data

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.

12. Audit and inspection

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.

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.

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.

13. The parties' agreement on other terms

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.

14. Commencement and termination

1. The Clauses form an appendix to the Terms of Service of SynergyXR shall become effective on the commencement of the services from SynergyXR.

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.

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.

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.

5. Signature

   This data processing agreement form an appendix to the main service agreement and SynergyXR's Terms of Service and shall be considered duly signed and valid upon the commencement of the services.

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 wishes to provide 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. 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.

Reference is made to the main agreement entered into between the parties.

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, video, portrait- or other photos 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 as long as the main agreement between the Parties remain in force.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	COMPANY REG. NO	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft Ireland Operations Limited	IE256796	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Irland	System hosting (Azure)
Exit Games GmbH		Hongkongstr. 7 20457 Hamburg Germany	Service hosting (Photon multiplayer)

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned 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 and a minimum of (if any) personal data as defined in Article 9 GDPR on 'special categories of personal data'. The parties agree that a security level in compliance with article 32 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
- all 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:

<u>The rights of data subjects:</u>

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.

<u>Notification of personal data breach</u>

The data processor must notify the data controller of any personal data breach within 36 hours.

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

C.4. Storage period/erasure procedures

Personal data is stored for the duration of the main agreement or until the data controller decides to erase the personal data. 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 3 months after the termination of the main 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 shall, 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. 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 at any stage decides (without any obligations hereto) to obtain an auditor's report from a state authorised public accountant concerning the data processor's gen-

eral compliance with the data protection regulation, such report shall be considered an adequate supervision of the data processor's activities and these Clauses. Such report may be subject to the ISAE3402, ISAE3000, SOC2 or similar standards. A report will be generic and apply to multiple clients supported by the data processor.

Based on the results of an audit, 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 give rise to this, 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

Please refer to the main agreement between the Parties.

Remuneration

Within a cap of two hours 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 ordinary hourly rates of the data processor.

If the data controller demands 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 regular 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.