Data processing agreement

(Standard Contractual Clauses)

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

between

Publisher/ Customer/User

Hereinafter the "Data Controller"

and

Veo Technologies ApS

Rovsingsgade 68

2100 København Ø Danmark

Company registration number: 37240834 hereinafter 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. Content

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 the services associated with the use of the Veo camera and the related Veo Platform, incl. the Veo Website and Veo App, to the Data Controller as specified in the Data Processor's General Terms and Product Terms (collectively the "Main Agreement"), the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses. Unless otherwise defined herein, capitalised terms used in these Clauses shall have the same meanings as those defined in the Main Agreement.

   No processing of personal data is performed by any other Veo group companies than the Data Processer. Thus, no other Veo group companies than the Data Processer undertake any role or responsibility in relation to the data processing activities defined in the Clauses.

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

5. The appendices attached to the Clauses 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. Appendix E contains the Data Controller's instructions with regards to transfer of personal data to third countries where the Data Controller is established.

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

12. 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 data protection provisions and the Clauses.

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.

3. To ensure the further development and optimization of the Data Processor's products and features as well as systems, incl. algorithm tools, that are useful to the Data Controller, the Data Controller permits the Data Processor to use

the recordings for the purpose of developing such new products, features and systems. In this regard, the Data Processor will be considered Data Controller when utilizing the recordings for these purposes.

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.

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:

    a. Pseudonymisation and encryption of personal data;
    b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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.

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.

   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) in the 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 10 days 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.

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. 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.

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.

8. Transfer of data to third countries or international organizations

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, the Danish Data Protection Agency, 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, the Danish Data Protection Agency, 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, if possible, take place within immediately and no later than 24 hours after the Data Processor has become aware of the breach of the personal data security 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 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 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.

4. The Data Controller will be obliged to pay the Data Processor for any assistance under this Clause 12. Any payment under this Clause 12 must be in accordance with market standards.

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.

2. The Data processors liability under these Clauses cannot exceed DKK 100,000.

14. Commencement and termination

1. The Clauses shall become effective in connection with entering into the Main Agreement.

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. The Data Processor is bound by the Data Processor Agreement without the Parties' signatures. The Data Processor Agreement is thus concluded without physical / digital signatures, as the Data Processor Agreement is binding in accordance with the requirement of GDPR, article 28(3), first sentence.

15. Data Controller and Data Processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points

2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Contact information for the Data Controller:

Reference is made to the Main Agreement for contact information.

Contact information for the Data Processor:

Reference is made to the Main Agreement for contact information.

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 following purposes form the basis of the Data Processor's processing of personal data on behalf of the Data Controller:

As further described in the Main Agreement, the purpose of the processing is to assist the Data Controller in recording or live streaming various sporting events with the Veo camera and making these recordings and live streaming sessions available live or on demand to others by using and storing those on the Veo platform, incl. the Veo Website and Veo App. The purpose is also to assist the Data Controller in making these recordings and livestreaming sessions available on other external websites and platforms at the choice of the Data Controller, including e.g., social media platforms, channels, or similar. The purpose is also to assist the Data Controller in analysing, editing and storing the recordings. Further, the purpose is to assist the Data Controller in administering relations to other Data Controllers (Veo League Exchange), as creating highlights of such recordings in relation to the Data Controllers or affiliated users designated as players associated with the Data Controllers (Veo Player Profiles) as well as assisting users of the Data Controller in creating short highlights of such recordings (Snipping Tool).

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 Processor will provide the Veo camera and software which the Data Controller will use to record, upload, and publish sound and video from various sporting events such as games, training sessions etc. Consequently, the Data Processor will process these recordings on behalf of the Data Controller. The Data Processor will further provide a platform where recordings may be uploaded and made available (live and on-demand) by the Data Controller. Moreover, the Data Processor will provide a technical solution which enables the Data Controller to make recordings and livestreaming available on other external websites and platforms at the choice of the Data Controller, including e.g., social media platforms, channels, or similar.

Additionally, the Data Processor will provide a League Exchange service on the platform where the Data Controller and other customers of the Data Processor are able to create a collective group specifically connected to the Data Controller's leagues. The Data Processor will process recordings shared in the collective groups and contact information on the Data Controllers' appointed admin users.

Moreover, the Data Processor will provide a Player Profile service which allows the Data Controller to designate its affiliated players. By designating a player, the Data Controller provides the player the opportunity to create a player profile where the player can create, save, and publish highlights concerning the user him-/herself from the Data Controller's recordings as well as additional information about the player him-/herself.

The Data Processor will on the platform further provide an analysis and editing tool to the Data Controller. Consequently, the Data Processor will also process the recordings when the Data Controller uses the tool.

In addition to the analysis and editing tool for the Data Controller, the Data Processor will provide the Data Controller's users with a "snipping tool" feature, which – when allowed by the Data Controller through privacy settings – will enable viewers to create and download short highlights (10-20 seconds) from the recordings. Finally, the Data Processor will store recordings on the platform on behalf of the Data Controller which enable the Data Controller to offer recordings on-demand to its fans, athletes etc.

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

The Data Processor will only process non-special category data in form of video recordings of different sporting events and contact information (name, club association, e-mail, telephone number) on the Data Controller's admin users re. the League Exchange service. Further, the Data Processor will process similar personal data on other users or data subjects associated with or otherwise related to the Data Controller or the Data Controller's recorded activities.

In relation to the Player Profile service, the Data Processor will process additional personal data if a designated player chooses to provide and publish this information. The personal data will pertain to jersey number, preferred position on the field, strong foot, specific highlights from recordings of and chosen by the designated player and other similar non-sensitive personal data.

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

(i) Sport players playing at a sport event at the Data Controller, (ii) Spectators to the sport event, (iii) Fans and (iv) Employees/persons of contact of the Data Controller.

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 of personal data shall be performed until the Data Processor's services has been terminated, after which the personal data is either returned or erased in accordance with Clause 11. The Data Processor's processing of personal data is performed as long as the underlying Main Agreement(s) consists.

Appendix B. Authorised Sub-processors

1. Approved sub-processors

1.1 On commencement of the Clauses, the Data Controller authorises the engagement of the following sub-processors as stated at https://www.veo.co/subprocessors.

1.2 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 authorization – 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.

Appendix C. Instruction pertaining to the use of personal data

1. The subject of/instruction for the processing

1.1 The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor to assist the Data Controller in recording and/or live streaming various sporting events on the Veo platform. Further, the Data Processor assists the Data Controller in making recordings and/or live streaming available through a technical solution to other external platforms or websites at the choice of the Data Controller, including, e.g., social media platforms, channels, or similar. Moreover, the Data Processor will assist the Data Controller in analysing and editing recordings from various sporting events, including the snipping tool feature providing the League Exchange service, and storing recordings in order to make recordings available on demand on the Veo Platform.

2. Security of processing

2.1 The level of security shall take into account:

Taking into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the Data Processor must implement an appropriate level of security.

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:

Physical security

The Data Processor shall implement the following physical security measures:

a) The Data Processor's office space can be locked.

b) The Data Processor uses alarm systems to detect and prevent burglary.

c) The Data Processor uses fire alarms and smoke detectors to detect and prevent fires.

d) The Data Processor's devices (including PCs, servers, etc.) are secured behind locked doors.

Organizational security

The Data Processor shall implement the following organizational security measures:

a) All employees of the Data Processor are subject to confidentiality obligations that apply to all processing of personal data.

b) The employee access to personal data is limited, so that only the relevant employees have access to the necessary personal data.

c) The processing of personal data done by the employees of the Data Processor is logged and can be checked as required.

d) The Data Processor has documentable process descriptions for breaches of the personal data security, which are reviewed at least annually.

e) The Data Processor's employees regularly document and report breaches of personal data security or risks thereof.

f) The Data Processor has established procedures that ensures proper deletion or continuous confidentiality when hardware is repaired, serviced or disposed.

Technical security: Access to personal data

The Data Processor shall implement the following technical security measures regarding access to personal data:

a) The Data Processor uses logical access control with username and password or other unique authorization.

b) The Data Processor uses antivirus programs that are updated regularly.

c) The Data Processor requires employees to use individual passwords.

d) There are procedures for granting authorizations to IT systems when hiring new employees.

e) There are procedures for revoking permissions when an employee stops or switches department.

f) The Data Processor has policies for password composition, including minimum requirements.

g) The Data Processor logs and controls unauthorized or repeated failed login attempts.

Technical security: Access to and protection of it systems

The Data Processor shall implement the following technical security measures regarding access to and protection of it systems:

a) The Data Processor regularly reviews system controls.

b) The Data Processor grants authorizations to individuals or groups of users to access, change and delete processed personal data.

c) The Data Processor regularly reviews and verifies user authorizations for specific systems.

d) The Data Processor logs and controls unauthorized or repeated failed attempts to access data.

Technical security: Availability and robustness

The Data Processor shall implement the following technical security measures regarding availability and robustness:

a) There are rules and guidelines for restoring data from backup.

b) There are rules and guidelines for data backup.

c) Backups are made regularly (either in-house or at supplier).

3. Assistance to the Data Controller

3.1 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:

3.1.1 If the Data Controller receives a request for the exercise of one of the rights of the data subjects in accordance with applicable data protection law, and a proper reply to the request requires assistance from the Data Processor, the Data Processor shall assist the Data Controller with the necessary and relevant information and documentation as well as appropriate technical and organizational security measures.

3.1.2 If the Data Controller needs the Data Processor's assistance in order to reply to a request from a data subject, the Data Controller must send a written requst for assistance to the Data Processor and the Data Processor shall in response provide the necessary help or documentation as soon as possible and no later than 7 calendar days after receiving the request.

3.1.3 If the Data Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Data Controller, and the request concerns personal data processed on behalf of the Data Controller, the Data Processor shall without undue delay forward the request to the Data Controller.

4. Storage period/erasure procedures

4.1 Upon termination of the provision of personal data processing services, the Data Processor shall either delete or return the personal data in accordance with Clause 11.1 unless the Data Controller – after the signature of the contract – has modified the Data Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

5. Processing location

5.1 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:

At the Data Processor's own headquarter or at the headquarters of approved sub-processors as specified in Appendix B.

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

6.1 Personal data is only being processed by the Data Processor on the locations specified in Clause C.5. As part of compliance with the Regulations, the Data Processor transfers personal data to the United States at locations specified in Section C.5. As part of complying with the Clauses, the Data Processor transfers mainly the personal data to the following countries: Denmark US, Canada. Such transfers are based on decisions of the European Commission, which generally ensure a sufficient level of protection, either through legislation or through other measures.

6.2 Transfer of personal data can in all cases only be done in accordance with these Clauses, on the instructions of the Data Controller and to the extent permitted by the applicable data protection law.

6.3 If the Data Controller does not provide a documented instruction in these Clauses or subsequently with regards to the transfer of personal data to a third country, the Data Processor is not entitled to carry out such transfers within the scope of these Clauses.

6.4. Personal data transfers to a third country may also occur if the Data Controller is established outside the EU/EEA. These transfers of personal data from the Data Processor to the Data Controller placed in a country outside the EU/EEA must only take place in accordance with Appendix E.

7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

7.1 The Data Processor shall, upon the Data Controller's written request, document to the Data Controller that the Data Processor

7.1.1 is complying with his obligations under these Clauses and the Instruction, and

7.1.2 with the relevant articles in the GDPR in regards to the personal data being processed on behalf of the Data Controller.

7.2 According to Clause C.7.1 the Data Processor's documentation shall be sent to the Data Controller within a reasonable time after receiving the request.

7.3 The Data Processor must provide the data Controller with documentation of continuous compliance with the provisions. The documentation can consist of self-audit reports prepared by the Data Processor and will be prepared once a year. The self-audit will follow the principles and control objectives of the ISAE 3000 auditing standard. The Data Processor is not obligated to initiate and undertake external audits of its compliance with the Clauses on its own initiative.

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

8.1 The Data Processor shall at least once a year, at their own expense, conduct an audit of the Data Processor's sub-processors.

Appendix D. The Parties' terms of agreement on other subjects

D.1 - Liability

Liability in connection with these Clauses shall follow the terms on liability in the Main Agreement.

Appendix E. Transfer of personal data to third countries where the Data Controller is established

If the Data Controller is established in a country outside the EU/EEA, the Parties will ensure that a legal transfer basis is established for the transfer of personal data from the Data Processor to the Data Controller based outside the EU/EEA.

The legal transfer basis will be either the European Commission's applicable adequacy decisions or the European Commission Decision 914/2021/EU of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 ("SCC's").

1. Transfers based on adequacy decisions

The European Commission has so far recognised the following countries as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, the United States (solely commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay.

Consequently, the adequacy decision applicable for the relevant country, will form the legal transfer basis for transfer of personal data from the EU (and Norway, Liechtenstein and Iceland) to that relevant third countries, provided that the relevant Data Controller to whom personal data is to be transferred, is covered by the adequacy decision.

If the Data Controller is not covered by the adequacy decision, the transfer of personal data will be based on SCC's as set out in section D.3.

2. Transfers based on the SCC's

In the event that the Data Controller is established in a country where the European Commission has not adopted an adequacy decision, the legal transfer basis will be the SCC's (Module 4 – Processor to Controller) which can be found in section E.3.

3. Standard Contractual Clauses (SCC's)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data[2], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

[2] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

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

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[3] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party

[3] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

N/A

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(d) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(e) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred

personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(f) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(g) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(h) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(i) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(j) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(k) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(l) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(m) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(n) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(o) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(p) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(q) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(r) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(s) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(t) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(u) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(v) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Denmark.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Veo Technologies ApS

Address: Rovsingsgade 68, 2100 København Ø Danmark

Contact person's name, position and contact details: Reference is made to the Main Agreement for contact information.

Activities relevant to the data transferred under these Clauses: The Data Processor's activities include the Data Processor to assist the Data Controller in recording, live stream, various sporting events, analysing and editing recordings from various sporting events, including the snipping tool feature providing the League Exchange service, and storing recordings in order to make recordings available on demand.

Signature and date: This Annex II shall be deemed executed upon execution of the Clauses and subscription to the services governed by the Data Processor's General Terms and Product Terms ("Main Agreement").

Role (controller/processor): Data Processor

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Publisher/ Customer/User of the subscription services governed by the Main Agreement

Address: As stated when subscribing to services governed by the Main Agreement

Contact person's name, position and contact details: As stated when subscribing to services governed by the Main Agreement

Activities relevant to the data transferred under these Clauses: Processing necessary to provide the services pursuant to the Main Agreement

Signature and date: This Annex II shall be deemed executed upon execution of the Clauses and subscription to the services governed by the Main Agreement

Role (controller/processor): Data Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Appendix A.4 of the Clauses.

Categories of personal data transferred

See Appendix A.3 of the Clauses.

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

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

On a continuous basis until the Data Processor's services have been terminated.

Nature of the processing

See Appendix A.2 of the Clauses.

Purpose(s) of the data transfer and further processing

See Appendix A.1 of the Clauses.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Appendix A.5 of the Clauses.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

N/A

C. COMPETENT SUPERVISORY AUTHORITY

The Danish Data Protection Agency, Datatilsynet.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Appendix C of the Clauses.

ANNEX III – LIST OF SUB-PROCESSORS

See Appendix B of the Clauses.