DATA PROCESSING AGREEMENT

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

between

The Customer

Hereinafter the “Controller”

and

Veo Technologies ApS

Business reg. no. DK37240834
Rovsingsgade 68
DK2100 Copenhagen
Denmark
privacy@veo.co

Hereinafter the “Processor”

each a “Party”; together the “Parties”

HAVE AGREED on the following Data Processing Agreement (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subjects.

Last updated: 18 August 2026

SECTION I

1. Purpose and scope

1.1. The purpose of this Data Protection Agreement (the "Clauses") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "GDPR").

1.2. The Controllers and Processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of the GDPR.

1.3. These Clauses apply to the processing of personal data as specified in Annex II.

1.4. Annexes I to V are an integral part of the Clauses.

1.5. These Clauses are without prejudice to obligations to which the Controller is subject by virtue of the GDPR.

1.6. These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of the GDPR.

2. Invariability of the Clauses

2.1. The Parties acknowledge that these Clauses, including Annex I-IV, do not constitute standard contractual clauses as referred to in Article 28(7) of the GDPR, due to the deviations from the EU Commission's original document agreed between the parties. The Standard Contractual Clauses adopted by the EU Commission pursuant to Article 46(2)(c), as included in Annex V, remain unchanged and thus constitute Standard Contractual Clauses within the meaning of Article 46(2)(c) of the GDPR.

2.2. With reference to Clause 2.1, the Parties continue to undertake to ensure that the Clauses do not directly or indirectly contradict obligations of the GDPR or detract from the fundamental rights or freedoms of data subjects.

3. Interpretation

3.1. Where these Clauses use the terms defined in the GDPR, those terms shall have the same meaning as in that Regulation.

3.2. These Clauses shall be read and interpreted in the light of the provisions of the GDPR.

3.3. These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. Hierarchy

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

5. Docking clause

The docking clause shall not apply.

SECTION II: OBLIGATIONS OF THE PARTIES

6. Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Annex II.

7. Obligations of the Parties

7.1. Instructions

7.1.1. The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

7.1.2. The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the GDPR or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the Controller.

7.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

7.4.1. The Processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

7.4.2. The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

7.6.1. The Parties shall be able to demonstrate compliance with these Clauses.

7.6.2. The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with these Clauses.

7.6.3. The Processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from the GDPR. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller will take into account the risk and nature of the processing activities carried out by the Processor.

7.6.4. The Controller may, at its own expense, choose to conduct the audit by itself or mandate an independent auditor.

7.6.5. The Processor is entitled to charge a reasonable fee for assistance provided to the Controller in Accordance with this Clause 7.6.

7.6.6. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

7.7.1. The Processor has the Controller's general authorisation for the engagement of sub-processors from an agreed list. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.

7.7.2. Where the Processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor similar data protection obligations as the ones imposed on the Processor in accordance with these Clauses. The Processor shall ensure that the sub-processor complies with the obligations to which the Processor is subject pursuant to these Clauses and to the GDPR.

7.7.3. At the Controller's request, the Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secrets or other confidential information, including personal data, the Processor may redact the text of the agreement prior to sharing the copy.

7.7.4. The Processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor, but to the extent permitted by law, with any limitations of liability included in the General Terms and Conditions.

7.8. International transfers

7.8.1. Any transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of the GDPR.

7.8.2. The Controller agrees that where the Processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, the Processor and the sub-processor can ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of the GDPR, provided the conditions for the use of those standard contractual clauses are met.

8. Assistance to the Controller

8.1. The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the Controller.

8.2. The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with 8.1. and 8.2., the Processor shall comply with the Controller's instructions.

8.3. In addition to the Processor's obligation to assist the Controller pursuant to Clause 8.2., the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of the GDPR.

8.4. The Parties shall set out in Annex III the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

9. Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 of the GDPR, where applicable, taking into account the nature of processing and the information available to the Processor.

9.1. Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

9.1.1. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

9.1.2. in obtaining the following information which, pursuant to Article 33(3) of the GDPR, shall be stated in the Controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

9.1.3. in complying, pursuant to Article 34 of the GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

(1) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(2) the details of a contact point where more information concerning the personal data breach can be obtained;

(3) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of the GDPR.

SECTION III: FINAL PROVISIONS

10. Non-compliance with the Clauses and termination

10.1. Without prejudice to any provisions of the GDPR, in the event that the Processor is in breach of its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with these Clauses, for whatever reason.

10.2. The Controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the Processor has been suspended by the Controller pursuant to point 10.1. and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the Processor is in substantial or persistent breach of these Clauses or its obligations under the GDPR;

(3) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to the GDPR.

10.3. The Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1.2, the Controller insists on compliance with the instructions.

10.4. Following termination of the contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

ANNEXES:

ANNEX I: LIST OF PARTIES

See page 1 of these Clauses.

ANNEX II: DESCRIPTION OF THE PROCESSING

See page 8 of these Clauses.

ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES

See page 12 of these Clauses.

ANNEX IV: LIST OF SUB-PROCESSORS

The Controller has authorised the use of the sub-processors presented at: https://www.veo.com/legal/subprocessors.

ANNEX V: STANDARD CONTRACTUAL CLAUSES (MODULE 4)

See page 14 of these Clauses.

ANNEX II: DESCRIPTION OF THE PROCESSING

VEO EDITOR (BASE SUBSCRIPTION)
Purpose of the processing
The purpose of the processing of personal data is to deliver our base subscription, Veo Editor, in accordance with the Controller's subscription. As part of this provision of service the Processor will process personal data for the purpose of deploying the AI pipeline, including to stitch the recording, apply follow-cam and interactive mode, and detect game events. In addition, personal data is processed for the purpose of allowing the Controller's users to use the available features, including to create clips, tag and comment on clips, download, draw on recordings, mark player of the match, assign assists, view recordings in different views and speeds, register which users viewed the recording, and to allow users to take notes in their journals. The purpose is also to allow the Controller to send email invites to users and share links to recordings via e-mail.
Nature of the processing
When the Controller has recorded a game with a Veo camera, the camera will upload the recording to the Veo Platform, when the camera is connected to a device and to wifi. The recording is transferred to the Processor's cloud infrastructure, where it is processed to deploy the AI pipeline. All recordings and subsequent personal data are hosted and stored in the Processor's platform infrastructure. The personal data contained in video recordings are available for view (in different formats), download, sharing and for the Controller's users to deploy any feature available in the Veo Editor subscription and as described above under the purpose of processing. Other personal data processed as part in the services will be generated by the Controller's users. Such personal data will be processed, including stored and made available, in accordance with the Controller's and its users' instructions.
Categories of data subjects whose personal data are processed
The Processor will process personal data of players, coaches, spectators, referees, and users.
Categories of personal data processed
The Processor will process the following categories of personal data: - Players: Video recordings, game events (goals, freekicks, corners, etc.), age group, game events, name, clip tags, pictures. - Coaches: Video recordings, pictures. - Referees: Video recordings. - Spectators: Video recordings. - Users: Username, comments, mentions, journal notes, viewed recordings, clip tags.
Special categories of personal data processed
n/a
Duration of the processing
The processing will be carried out on an ongoing basis in accordance with the Controller's subscription to the Veo Platform.

VEO ANALYTICS 2 (ADD-ON)
Purpose of the processing
The purpose of processing is to provide the service Analytics 2 to the Controller, who has purchased Analytics 2 as an add-on. As part of Analytics 2 the purpose of the processing is to detect information regarding the players on the pitch, including distance covered by players, as well as average and maximum speed, i.e., speed at any moment during the game, distance to ball, time on ball, number of sprints, tackles, duels, dribbles, interceptions, loose ball recoveries, passes (attempted/completed), and conversion rate. All data is made available to the Controller's users. The Processor also detects distance between players and enables the Controller to make comparisons of individual player stats. The individual player stats are made available per event and aggregated over a specific period of time. The Processor also provides a tool to link jersey numbers with individual players, who have been invited as users to the platform, and allows the Controller to create formations and line-ups connecting specific players to jersey numbers and positions on the pitch. The rosters and line-ups are available for both match level and team level with users and jersey numbers. The Processor also allows the users to take notes relating to specific clips and recordings and save them with different privacy settings, and to create highlight reels based on jersey number tracking, and player moments are made available based on players' distance to and time on ball.
Nature of the processing
The nature of the processing entails using the Processor's AI model to detect all events during the recordings uploaded to the Processor's platform. All recordings and all data derived from the recordings are hosted and stored in the Processor's platform infrastructure. The personal data derived from video recordings are available for view (in different formats), download, sharing and for the Controller's users to deploy any feature available in the Analytics 2 subscription and as described above under the purpose of processing. Other personal data processed as part in the services will be generated by the Controller's users. Such personal data will be processed, including stored and made available, in accordance with the Controller's and its users' instructions.
Categories of data subjects whose personal data are processed
The Processor will process personal data of players and users.
Categories of personal data processed
The Processor will process the following categories of personal data: - Players: Video recordings, game events (goals, freekicks, corners, sprints, tackles, duels, passes, interceptions, saves, loose ball recoveries, etc.), age group, name, clip tags, pictures, distance to ball, run speed, distance run, position on field, jersey number, time on ball. - Users: Notes, comments, tags, mentions, username.
Special categories of personal data processed
N/A
Duration of the processing
The processing will be carried out on an ongoing basis in accordance with the Controller's subscription to the Veo Platform.

COACH ASSIST (REQUIRES ENABLING ON TEAM LEVEL)
Purpose of the processing
The purpose of the processing of personal data is to deliver the Coach Assist chat, which can be enabled on a team basis for all users of a specific team. The Coach Assist chat makes available an AI chat function based on an LLM, which enables users to ask questions regarding a game, including questions regarding strategy, performance, tactics, and suggested improvements. For the purpose of providing output based on the users prompts, the LLM will process the player specific statistics and game statistics related to recorded games that have been uploaded to the Veo Platform and allocated to the team for which the Coach Assist chat is enabled. Personal data about the users engaging with the Coach Assist chat are processed for the purpose of providing output to the user. The third party AI provider(s) are obligated to not use the personal data for training of their AI model(s).
Nature of the processing
When the Controller has enabled the Coach Assist chat for a team, the Processor will enable an LLM-based chat set up with API integration(s) to one or more LLM provider(s), as described in the list of sub-processors. The processing will entail analysis of game statistics for the purpose of providing output based on prompts created by users with access to the team. Logs of the chat history will be stored with the Processor, in its infrastructure. The logs are not stored with the third party provider(s).
Categories of data subjects whose personal data are processed
The Processor will process personal data of players and users.
Categories of personal data processed
The Processor will process the following categories of personal data: - Players: Game events (goals, freekicks, corners, sprints, tackles, duels, passes, interceptions, saves, loose ball recoveries, etc.), name, jersey number, distance to ball, run speed, distance run, position on field, time on ball. - Users: Name, date of user creation, preferred language, user bio (if applicable), age (if applicable), nationality, team membership(s).
Special categories of personal data processed
n/a
Duration of the processing
The processing will be carried out on an ongoing basis in accordance with the Controller's subscription to the Veo Platform.

VEO LIVE (ADD-ON)
Purpose of the processing
The purpose of the processing of personal data is to deliver the add-on subscription, Veo Live, in accordance with the Controller's subscription. As part of this provision of service, the Processor will process personal data to enable the Controller's users to live stream matches in real time to the Veo mobile application, and to external streaming platforms such as Youtube, Facebook, and Twitch via RTMP, or to other destinations selected by the Controller. The Controller specifically instructs the Processor to stream to third-party platforms as part of the livestreaming setup. In addition, personal data is processed to provide the Controller with viewership and engagement insights in relation to their streams.
Nature of the processing
When the Controller is live streaming, the real-time transmission of video recordings containing personal data, is processed through to the Veo mobile application or to external streaming platforms selected by the Controller. This includes the delivery of live video streams, the application of overlays to the stream, and the collection and storage of views and engagement data associated with each stream.
Categories of data subjects whose personal data are processed
The Processor will process personal data of players, referees, coaches, and spectators.
Categories of personal data processed
The Processor will process video recordings of all data subjects.
Special categories of personal data processed
n/a
Duration of the processing
The processing will be carried out throughout the duration of the livestreaming.

VEO LEAGUE EXCHANGE
Purpose of the processing
The purpose of the processing of personal data is to deliver the Veo League Exchange, in accordance with the Controller's subscription. As part of this provision of service, the Processor will process personal data to enable the Controller to create a league and share match recordings with other teams within the same league, allowing users to access and import recordings to Veo Editor for analysis and opponent scouting. The purpose is also to allow the Controller to send email invites to users and share links to recordings via e-mail in accordance with the Controller's instructions. Where the Controller is part of a League Exchange for which another Customer is the data controller, the purpose of the processing is for the Processor to facilitate the disclosure of the personal data to the owner of the League Exchange. In that case, the Controller is instructing the Processor to disclose this personal data.
Nature of the processing
Where the Controller is the owner of a League Exchange, the nature of the processing is the storing of recordings shared to the League Exchange and making them available to the members of the League Exchange. Where the Controller is a member and not the owner of the League, the nature of the processing is to allow the Controller to share recordings to the League.
Categories of data subjects whose personal data are processed
The Processor will process personal data of players, referees, coaches, spectators, and users.
Categories of personal data processed
The Processor will process the following categories of personal data: - Players: Video recordings, game events. - Coaches: Video recordings. - Referees: Video recordings. - Spectators: Video recordings. - Users: Access rights, name, email address
Special categories of personal data processed
n/a
Duration of the processing
The processing will be carried out on an ongoing basis in accordance with the Controller's subscription to the Veo Platform.

ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES
INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the Processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

The technical and organisational measures set out in this Annex are implemented by the Processor pursuant to Article 32 of the GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. The measures are designed to ensure a level of security appropriate to the risk, including as regards the pseudonymisation and encryption of personal data, the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Encryption and pseudonymisation

Personal data at rest is encrypted using AES-256 server-side encryption across the Processor's primary storage services (Amazon S3, Amazon RDS and Amazon DynamoDB). AWS Key Management Service (KMS) customer-managed keys are used for selected services, including AWS Backup vaults. Personal data in transit is protected using TLS across all application, API and authentication endpoints. Camera authentication tokens are hashed.

Access control and authentication

Access to systems processing personal data is controlled through a central identity provider, with multi-factor authentication enforced for all personnel. If a system does not support federated authentication, access is governed by the Processor's access management controls. Where shared credentials are used, they are managed through a dedicated enterprise password-management solution. Application access is provisioned and de-provisioned through an access-management process. Access is granted on a need-to-know basis in accordance with the Processor’s Access Management Policy.

Logging and monitoring

Infrastructure activity is logged through the Processor's cloud provider's native audit logging service. System-level access logs are maintained per application. System-specific logs are available upon reasonable request to support the Controller's compliance obligations.

Backup and recovery

Personal data is backed up using AWS-native backup services on a per-service basis. Backup and recovery procedures are maintained by the Processor. Detailed backup schedules and recovery time objectives are available upon written request.

Confidentiality obligations

All employees of the Processor are bound by confidentiality obligations contained in their employment contracts. Contractors and third-party personnel with access to personal data are subject to non-disclosure agreements prior to engagement.

Physical security

The Processor’s premises are secured with key-chip access control and per-user entry logging. All production personal data are hosted within AWS infrastructure, which operates under the AWS shared responsibility model for physical and environmental security.

Asset disposal

The Processor's IT Equipment Standards require that all devices are securely wiped prior to repair, recycling or disposal. Device management and wipe procedures are enforced through a centralised mobile device management solution.

Awareness training

All employees of the Processor are required to participate in mandatory IT security and Privacy awareness training at appropriate intervals and in accordance with their roles.

Description of the specific technical and organisational measures to be taken by the Processor to be able to provide assistance to the Controller.

Procedures for the Controller's audit rights in accordance with Clause 7.6

The Processor shall, upon the Controller's written request, document to the Controller that the Processor complies with its obligations under these Clauses. Requests for documentation shall be made to privacy@veo.co.

The Processor must, upon request, provide the Controller with documentation of continuous compliance with the provisions. The documentation may consist of selfaudit reports prepared by the Processor, an independent auditor's report or other appropriate documentation. The Processor is not obligated to initiate and undertake external audits of its compliance with the Clauses.

The Processor shall, at its own expense, conduct appropriate audits of the Processor's sub-processors taking into account the risk of the processing activities carried out by the sub-processor in question.

The Processor's assistance to the Controller in accordance with Clauses 8.1 and 8.2

The Processor has implemented a procedure on handling data subjects' rights, including any assistance to be provided to the Controller. Where the Controller receives a request from a data subject which requires assistance from the Processor, the Controller may request assistance at privacy@veo.co.

The Processor will provide the necessary assistance, where the Controller itself is not able to facilitate the fulfillment of a request.

Where the Processor receives a request directly from a data subject relating to personal data processed on behalf of the Controller, the Processor will, without undue delay, forward the request to the Controller, or refer the data subject to the Controller, depending on the nature of the request. Besides confirming the receipt of the request, the Processor shall only handle requests from data subjects in accordance with instructions from the Controller.

The Processor's assistance to the Controller in accordance with Clause 9

The Processor has implemented an Incident Response Plan for handling personal data breaches. The Processor will notify the Controller without undue delay and within 48 hours of becoming aware of a personal data breach relating to personal data processed on behalf of the Controller.

Where the Controller experiences a personal data breach for which the Processor's assistance is required, the Controller may request assistance at privacy@veo.co.

Where possible, the Processor will assist the Controller with handling and investigating the personal data breach and provide available documentation to assist the Controller with notifying relevant authorities.

ANNEX V: STANDARD CONTRACTUAL CLAUSES (MODULE 4)
PROCESSOR TO CONTROLLER

INTRODUCTION
If the Data Controller is established in a country outside the EU/EEA, which is not subject to an adequacy decision adopted pursuant to Article 45 of the GDPR, the Parties will conclude module 4 of the standard contractual clauses based on the European Commission Decision 914/2021/EU of 4 June 2021 as set out in this Annex V.

SECTION I

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) 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')

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.

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 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.

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.

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.

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.

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.

7. Docking clause (Optional)

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

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, 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

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.

9. Use of sub-processors

[Intentionally left blank]

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.

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.

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 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.

13. Supervision

[Intentionally left blank]

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

14. Local laws and practices affecting compliance with the Clauses

a) 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.

b) 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;

(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.

c) 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.

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

e) 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).

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

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

15.1. Notification

a) 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.

b) 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.

c) 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.).

d) 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.

e) 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

a) 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).

b) 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.

c) 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

16. Non-compliance with the Clauses and termination

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

b) 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).

c) 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 of 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.

d) 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.

e) 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.

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.

18. Choice of forum and jurisdiction

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

ANNEX V.I

A: LIST OF PARTIES

DATA EXPORTER	
Name	Veo Technologies ApS
Address	Rovsingsgade 68, DK2100 Copenhagen, Denmark
Contact information	privacy@veo.co
Role	Data processor
Relevant processing activities	As described in Annex II.

DATA IMPORTER	
Name	Customers established outside the EU/EEA
Role	Data controller

B: DESCRIPTION OF PROCESSING

As part of the services provided by the Data Processor and set out in Annex II, the Data Processor imports the personal data to EU/EEA, and makes it available, i.e., re-exports the data to the country in which the Customer is established.

C: COMPETENT SUPERVISORY AUTHORITY

The Danish Data Protection Agency, Datatilsynet.

ANNEX V.II: TECHNICAL AND ORGANISATIONAL MEASURES

As set out in Annex III.

ANNEX V.III: LIST OF SUB-PROCESSORS

As set out in Annex IV.