Veo information notice regarding data protection (incl. the GDPR)

To help our customers better understand and comply with data protection legislation in connection with the use of the Veo camera and Veo Platforms as well as the related features and services, we have prepared this information notice for our customers.

When using the Veo camera and Veo Platforms etc. personal data in form of especially video recordings of different sport events will be collected and processed. Any customer initiating such data processing activities must comply with the relevant data protection legislation and other applicable legislation.

For European customers this means that special attention must be paid to the EU General Data Protection Regulation, also known as the GDPR. The GDPR includes a set of rules that must be complied with when processing personal data. In addition, it may also be necessary to take supplementary national rules on data protection into account.

In this information notice we highlight central rules in the GDPR, which you should be aware of when recording sport events and processing personal data in general. As the GDPR in general impose very strict obligations, we assume most of our customers may benefit from this notice.

Please be aware that we do not exhaustively describe the requirement and obligations in relation to processing of personal data and data protection. The information notice cannot constitute or substitute legal advice. We also note that all customers are independently responsible and liable for ensuring compliance with the GDPR, any applicable supplementary national legislation on privacy and data protection, and any other relevant national legislation such as rules about CCTV-surveillance.

For any further information on relevant data protection legislation etc., we encourage our customers to seek guidance or contact local data protection agencies or similar authorities.

Is recording sport events processing of personal data?

The concept of "personal data" is very broad and includes **any information** relating to an identified or identifiable natural person. Personal data can for example be a name, a person's age, physical characteristics, a person's voice, a picture, or video recordings showing individuals.

According to the GDPR, information constitutes personal data if it is possible to identify a person from the data (e.g., from picture or video recording) or in combination with other data.

This means that video recordings showing individuals playing or watching various sports will be considered personal data. The individuals who appear from the video recordings are called "data subjects".

Who is responsible for complying with data protection legislation?

According to the GDPR, it is important to identify who acts as so-called *data controller* and who acts as *data processor* in relation to any data processing activity to determine which obligations the concerned parties have.

With regards to customers use of the Veo camera and Veo Platforms as well as the related features and services (which include recording, live-streaming on the Veo Platforms or external sites and platforms (including sharing of personal data by the use of the Veo Partner Program), on-demand accessibility, League-Exchange, Player Profile, analysis and editing of recordings, including the snipping tool), the customer will act as the data controller and Veo Technologies ApS will act as data processor.

The relationship between our customers and Veo in connection with the processing of personal data is governed by a data processing agreement, which is accessible at veo.co. More information on the customers' and Veo's data protection roles and responsibilities are also available at veo.co.

Given this split of roles and responsibilities, the customer is primarily responsible for complying with the data protection legislation, including the GDPR. Therefore, Veo will in general refer questions, comments, or enquiries in relation to the data processing activities and recording of sport events to the relevant customer.

How do you as customer and data controller comply with data protection legislation?

According to the GDPR, the data controller has many different responsibilities and obligations when processing personal data. Below we have highlighted selected important points of attention regarding compliance with the GDPR.

1) **Documentation of data processing activities**
   The data controller must maintain records of its data processing activities. Such records must, inter alia, include descriptions of what personal data is processed, concerning whom and for which purposes. Consequently, the processing of personal data in connection with the use of the Veo camera Veo Platforms must be documented and described in such records.

2) **Legal basis and principles relating to processing of personal data**
   The data controller must be able to establish a legal basis such as consent, contract, legal obligation, or legitimate interests in relation to all data processing activities. What legal basis to use depends on the type of personal data you process and the situation in which processing of personal data is necessary. The use of the Veo camera and Veo Platforms etc. will normally require one of the legal bases set out in article 6 of the GDPR.

   A data controller relying on legitimate interest must balance the data controllers interests against the data subject's. If they would not reasonably

expect the processing, or if it would cause unjustified harm, their interests are likely to override the data controller's legitimate interests.

A data controller relying on legitimate interest or consent must ensure that the legitimate interest or consent extends to all elements of the processing including recording, live-streaming on the Veo Platforms or external sites and platforms such as YouTube ("External Media Platforms"). If a legitimate interest assessment or consent has not originally considered live-streaming on External Media Platforms or disclosure under the Veo Partner Program, the data controller may need to renew their legitimate interest assessment or consent before initiating live-streaming on External Media Platforms.

Further, the data controller must comply with the fundamental principles relating to processing of personal data. This for instance means that the processing of personal data must be fair, transparent, limited to what is strictly necessary and in general comply with good data protection practice.

3) **Inform data subjects about the processing of personal data**

To ensure sufficient transparency, the data controller must provide certain information regarding the processing of personal data to the data subjects. In relation to the use of the Veo camera this basically entails that the persons (e.g., players, referee, spectators, and fans) appearing in the recordings must be informed.

This information is usually provided in a privacy policy and should, inter alia, include contact information, description of the purpose of the processing of personal data (e.g., why are sport events recorded and shared?), what personal data is processed (e.g., video recordings and user information), and how long personal data is kept (e.g., when are video recordings deleted?).

As Veo may use the video recordings for Veo's own development and optimization purposes, it is also necessary to inform the data subjects of the disclosure of video material to Veo Technologies ApS. Find more information on how Veo process personal data for these and other purposes at veo.co.

If the data controller chooses to make use of the Veo Partner Program, which enables video material to be accessed via various third-party applications (Veo API) specifically selected by the data controller, it is additionally necessary that the data controller inform the data subjects of the disclosure of video material to any such third party (Veo API Partner) and the purpose of any such disclosure. Information on any processing for the purpose(s) of the receiving Veo API Partner with whom the video material is shared must also be provided to the data subjects. This means that the data controller must carefully consider which Veo API Partner to disclose video materials to and documents all disclosures sufficiently.

The information must be easily accessible for the data subjects. Therefore, it is a good idea to make a privacy policy available on a website or fan page and inform of any recording on posters at club houses and other warning signage.

4) **The data subject's rights**
The data subjects have certain data protection rights. These include, inter alia, the right of access (copies), the right to rectification, the right to erasure, the right to restriction, and the right to object against processing of the personal data.

The data controller must be able to properly handle a request from a data subject regarding the exercise of its rights. It is e.g., a requirement that a request is answered for free and without undue delay, and at the latest one month from the date the request was received.

5) Storage of personal data
Personal data shall not be stored for a longer period than necessary for the purposes for which the personal data is processed. This means that the data controller shall give thought to how long it is necessary to process the personal data (recordings, etc.), and when the personal data shall be deleted.

6) **Data protection and security**
Personal data must be handled with integrity and adequate confidentiality. This entails that appropriate technical and organizational security measures must be implemented to mitigate any risks in relation to the processing of personal data.

This for instance means that the data controller must consider who (and how many) has access to personal data, the Veo camera, and other features such as administration profiles on the Veo Platforms, etc. Further, it is important to implement minimum standards for admin-user passwords, only create the necessary number of admin-users, and generally take care of the personal data processed.

If a security incident takes place, such incident may negatively impact the confidentiality, integrity, or availability of the personal data. This is for instance the case if personal data such as video material is shared, made public or leaked accidentally. If so, the data controller may be obligated to report the so-called personal data breach to the relevant data protection agency. Under certain circumstances, the data controller may also have to notify the data subjects.

If Veo experiences any personal data breaches within the Veo platforms etc., Veo will to the extent required provide information on such incidents without undue delay in accordance with the data processing agreement.

7) **Awareness of data protection**
It is important to share information to your employees and other people who works within your organization, regarding data protection and how to handle personal data. In this way, your employees, etc., can act in a fitting manner in relation to data protection matters, e.g., handle a personal data breach situation or handle a request from a data subject regarding the exercise of its rights under the GDPR.

8) Data protection for children and young people
The GDPR prescribes specific protection to children and young people with regards to processing of personal data concerning such data subjects, as they may be less aware of the risks and consequences associated with such processing. Further, they may pay less attention to how to safeguard their privacy and exercise their rights in relation to processing of personal data.

For this reason, we encourage any customers intending to use Veo's products and services in relation to children and young people, for example in case the Veo camera is used to stream and/or record sporting events where children or young people participate or compete, to pay special attention to the protection of personal data concerning these data subjects.

Further, we recommend carefully considering and assessing whether any such processing complies with the fundamental principles and whether sufficient legal basis can be established. In this regard, providing the data subjects with information on the processing in an intelligible and transparent manner adjusted to the age and perception of the data subjects is vital. For more information on how to generally comply with the GDPR, please see the above sections.

Veo also encourage customers to seek professional legal advice or other guidance from e.g. data protection authorities or relevant sport associations, if planning to process personal data involving children and young people or other more vulnerable data subjects.

9) Utilization of the Veo Partner Program
The Veo Partner Program generally enables customers to make video material accessible from or via specifically selected third-party applications. The customers decide – via the privacy settings – whether specific video material may be disclosed by use of the Veo Partner Program and what third-party applications may access the video material.

If customers decide to activate and make use of the Veo Partner Program to share video material outside the Veo Platforms, it is important to be aware and consider that allowing the specifically selected third-party applications to access video material from the Veo Platform will entail disclosure of personal data to the third parties at the choice of the specific customer.

Such disclosure of personal data to third parties constitutes an individual data processing activity and requires an independent legal basis to be established (please see the above information concerning legal basis and principles relating to processing of personal data (point 2)) and considerations in relation to data protection for children and young people (point 8)).

Additionally, we recommend that customers and users carefully consider what specific third-party applications they choose to share video material via to ensure that all disclosure are relevant, necessary and proportionate, and that customers re-visit those selections regularly.

Veo will in this regard, as data processor, facilitate the sharing of video material only when specifically and explicitly instructed by the customers as data controllers. Instructions are provided by the customer to Veo via the privacy settings and the specific choices of third-party applications by the customer.

If customers choose to share video material via selected third-party applications and disclose such to any third parties established in a non-EU/EEA country, customers must be aware that such sharing and disclosure of personal data constitute a transfer of personal data under the GDPR. Special requirements apply for transfer of personal data to such countries outside the EU/EEA, and the customers must, therefore, additionally establish a legal basis for the transfer of the personal data. A legal basis for such transfer could be the reliance of an adequacy decision made by the EU-Commission or entering into EU Standard Contractual Clauses with the relevant third party.

More information on restrictions and requirements in relation to transfer of the personal data from EU/EEA-countries to countries outside the EU/EEA can be found in guidance available on the website of the Dan-ish Data Protection Agency, Datatilsynet (datatilsynet.dk), as well as guidelines available on the website of European Data Protection Board, EDPB (https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en). Veo especially recommend customers transferring personal data to third parties outside the EU/EEA to pay close attention to the following important guidance from the EDPB:

- EDPB Recommendations 01/2020 (https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en)on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and

- EDPB Recommendations 02/2020 (https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en) on the European Essential Guarantees for surveillance measures

Further, more country-specific legal and regulatory guidance can be found on other local data protection agencies. In general, we recommend all our customers to seek such guidance and if neccesary professional legal advice to ensure compliance with the applicable data protection legislation.

10) External Media Platforms

When streaming to External Media Platforms, Veo will no longer be responsible for or participate in the processing of personal data. If the customers decide to carry out such streaming, Veo urges its customers to consult Veo's General Terms and Conditions as well as Veo's User Terms which both can be found on veo.co before initiating the streaming to External Media Platforms.

Further, Veo emphasizes that the customers must ensure to establish a legal basis for the processing as described in Section 2), Legal basis and principles relating to processing of personal data.

11) Data Protection Impact Assessment ("DPIA")

It follows from the GDPR that a data controller is required to conduct a DPIA prior to initiating a processing activity if the processing activity includes the use of new technologies or is likely to result in a high risk to the rights and freedoms of natural persons.

The Danish Data Protection Agency has issued guidelines on the DPIA requirements. (https://www.datatilsynet.dk/Media/2/6/Konsekvensanalyse.pdf and https://www.datatilsynet.dk/Media/4/1/Datatilsynets%20liste%20over%20behandlinger%20der%20altid%20er%20underlagt%20kravet%20om%20en%20konsekvensanalyse%20(2).pdf)Veo recommends that the customers in particular consider the following factors, which may entail a requirement to conduct a DPIA:

- Whether the processing entails the use of new technologies
- Whether personal data is processed on a large scale
- Whether the personal data concerns vulnerable data subjects

Veo urges its customers to carefully consider whether they are required to conduct a DPIA before using Veo Platforms including live-streaming on External Media Platforms in particular in cases of streaming events where children or young people participate or compete.

Check list (for inspiration)

We note that this checklist is solely a tool for inspiration and can never stand alone in relation to ensuring compliance with data protection legislation, including the GDPR.

#1	**Do you have an overview of your processing of personal data, including categories of personal data and data subjects (e.g. do you record, process and share video material concerning children and young people or other vulnerable data subjects) as well as categories of recipients of the personal data (e.g. third parties recipients of the video material and personal data in connection with for instance your use of the Veo Partner Program or other streaming solutions)?**	✔
#2	**Have you identified the purpose of the processing of personal data and chosen an appropriate legal basis (and have you considered whether it is possible to establish a legal basis for the use of personal data related to children and young people, if relevant)?**	✔
#3	**Have you prepared a "record" concerning the data processing activities in relation to which you are data controller?**	✔
#4	**Have you ensured that you comply with the fundamental principles relating to the processing of personal data (lawfulness, fairness and transparency, purpose limitation, data minimization, etc.)?**	✔
#5	**Have you provided clear and intelligible information about the processing of personal data to the data subjects, and made the information available and easily accessible, e.g., in a privacy policy on your website and signage?**	✔
#6	**Do you have sufficient knowledge on the "data subject rights" to identify a request regarding the exercise of the rights, and have you drafted a plan to handle any such request?**	✔
#7	**Have you considered how long it is necessary for you to process and store personal data, and have you remembered to delete personal data when it is no longer necessary for you to process and store such data?**	✔

#8	Do you have sufficient knowledge on what a personal data breach is, and do you have a plan to handle such breaches?	✔
#9	Have you implemented technical and organizational security measures (e.g., instructions on who and how many may have access to personal data, storing of technical equipment, etc.), and prepared an internal security guideline/policy?	✔
#10	Have you made your employees, etc., aware of data protection in general?	✔
#11	Have you considered whether you are required to conduct a DPIA?	✔