DATA PROCESSING AGREEMENT

between

Pupil Labs GmbH
Sanderstraße 28,
12047 Berlin,
Germany
(hereinafter referred to as the **"Company"**)

and

_____
(hereinafter referred to as the **"Client"**)

Each of the Company and the Client are also referred to hereinafter, individually as a **"Party"** and collectively as the **"Parties"**.

Preamble

(a) The Company is the designer and manufacturer of Pupil Invisible, a state-of-the-art spectacle-like eye-tracking device. The device is worn like a pair of glasses, and it is used for determining where in the surrounding world the wearer of the device is looking.

(b) The Client is a user of the device who, in the course of using the device, records, stores and processes visual images and other information relating to identified or identifiable natural persons.

(c) The Parties have concluded a main contract for the use of Pupil Invisible.

(d) The Client in some cases transmits some of these information to the Company or to the Company's appointed Sub-Processors. However, the Client shall at all times, determine the ultimate purpose and means for processing any and all information.

(e) The Parties have agreed to enter into this Agreement for the purpose of regulating the Processor's handling of the said information, and complying with the applicable Data Protection Laws.

1. Definitions

1.1 In this Agreement, unless the context otherwise requires, the following expressions shall have the following meanings:

1.1.1 **"Agreement"** means this Agreement.

1.1.2 **"Controller"** means the person or entity that determines the purposes and means of the processing of Personal Data.

1.1.3 **"Data Protection Laws"** means all data protection and privacy laws and regulations applicable to the processing of Personal Data under the Agreement, including, where applicable, the GDPR.

1.1.4 **"Data Subject"** means any individual person who can be identified, directly or indirectly, via an identifier such as a name or location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

1.1.5 **"GDPR"** means the European Union General Data Protection Regulation, Regulation (EU) 2016/679.

1.1.6 **"Joint Controllers"** are entities that jointly determine the purposes and means of the processing of Personal Data.

1.1.7 **"Main Contract"** means the contract for the use of Pupil Invisible concluded by the Parties.

1.1.8 **"Personal Data"** means any information relating to a Data Subject.

1.1.9 **"Processor"** means the person or entity that processes Personal Data on behalf of the Controller.

1.1.10 **"Processing"** has the meaning given to it in the GDPR, and the words **"process"**, **"processes"** and **"processed"** shall be interpreted accordingly.

1.1.11 **"Product"** means Pupil Invisible, a state-of-the-art spectacle-like eye-tracking device, designed and manufactured by the Company, see https://www.pupil-labs.com/products/invisible.

1.1.12 **"Pupil Cloud"** means the cloud storage and cloud computing solution provided by the Company whereby customers can access data storage and data processing capabilities via multiple servers on the internet.

1.1.13 **"Security Incident"** means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.

1.1.14 **"Sub-Processor"** means the Processor engaged by another Processor to assist in fulfilling the latter's processing obligation.

1.1.15 **"Wearer"** is a Data Subject on whose head the Product is mounted.

2. Nature of Personal Data and Processing

2.1 The types of Personal Data envisaged under this Agreement include visual images (pictures, videos), cell phone ID, location data, timestamps, audio data, contact data (first, last name), shipping address, bank account information and other payment information, registration data, and order data.

2.2 The types of processing will include recording, collection, storage, disclosure by transmission, use, and analysis of data.

2.3 Categories of Data Subjects include the Wearer, persons being observed, passers-by, customers, representatives and employees of the Client.

2.4 The Product is marketed and distributed to individuals, private and public institutions, who may use the Product for a variety of purposes. The Client as an individual may wear the Product or give the Product to another person who then wears the Product. The Client as a private or public institution may distribute the Product to several persons who then wear the Product. Whenever the Product is mounted on the head of the Wearer and recording is switched on, it begins to record and store pictures, videos and other information of the Wearer, and if the world camera is connected, it also records and stores pictures, videos and other information of other natural persons, animate and inanimate objects.

3. Relationship between Parties

3.1 As between the Company and the Client, the Client is the Controller of Personal Data and the Company shall process Personal Data as a Processor on behalf of, and at the direction of the Client (Art. 28 GDPR). However, nothing in this Agreement shall prevent the Company from processing or otherwise using any Personal Data that the Company would otherwise collect and process independently of Client's use of the Product.

3.2 In general, the Client shall issue orders and instructions for processing, and the Company shall accept and execute orders and instructions for processing. The order and instructions shall be in writing or in a documented electronic format.

3.3 The Client is responsible under this Agreement for compliance with the applicable data protection and data privacy laws, including but not limited to ensuring that any recording, storage and processing, as well as the disclosure or transmission of Personal Data to the Company, is lawful. If the Company determines that an act or instruction of the Client is contrary to the Data Protection Laws, the Company will notify the Client to that effect as soon as possible. The Company is also entitled to suspend the implementation of an instruction until it is confirmed or adjusted by the Client.

3.4 The Company shall only use the Personal Data collected, in the manner agreed with the Client, and it shall not use the Personal Data for any unauthorized or illegitimate purposes.

3.5 The Client shall have unfettered access to any and all information which it stores with the Company. In fulfilling the rights of the Data Subjects, in compiling the lists of processing activities, and in necessary data protection impact assessments by the Client, the Company shall cooperate to the extent necessary and support the Client as far as possible. However, the Company is entitled to refuse the disclosure of any information which would constitute a violation of statutory or contractual regulations.

3.6 Each Party shall be entitled to satisfy itself before the start of processing and then regularly in an appropriate manner that the technical and organizational measures taken by the other and the obligations specified in this Agreement are complied with.

3.7 Each Party shall immediately inform the other party if it detects errors or irregularities in the examination of the results of the other.

3.8 Changes to the object of processing and procedural changes must be agreed jointly between the Parties, and must be specified in writing or in a documented electronic format.

4. Duration and Termination

4.1 This Agreement ends with the termination of the Main Contract.

4.2 A separate termination of this Agreement is possible only for good cause.

5. Sub-Processors

5.1 The Company has currently appointed Digital Ocean, LLC (https://www.digitalocean.com), Hetzner Online GmbH (https://www.hetzner.de), and and Amazon Web Services Inc. (https://aws.amazon.com) as its Sub-Processors providing the necessary infrastructure and support for the Company's Pupil Cloud service. Thus, in the majority of cases, the Company does not directly receive any of the information recorded by the Product. Instead, the information is routed directly to said Sub-Processors, and the information remains accessible through the Sub-Processors.

5.2 The Client agrees that the Company engages Digital Ocean LLC, Hetzner Online GmbH, and Amazon Web Services Inc., and that the Company may engage other Sub-Processors in the future, to store and process Personal Data and other information on the Client's behalf. In the latter case the

Company will inform the Client in writing and give the Client the right to object against the new processor for good cause.

5.3 The Company shall enter into written agreements with any appointed Sub-Processors, imposing data protection terms that require the Sub-Processor to protect Personal Data to the standard required by the Data Protection Laws. Also, the Company shall remain responsible for its compliance with the obligations of this Agreement and for any acts or omissions of the Sub-Processor that cause the Company to breach any of its obligations under this Agreement.

5.4 The Company shall provide the Client with reasonable advance notice (for which email shall suffice) if it adds or removes Sub-Processors.

6. Security and Confidentiality of the Personal Data

6.1 The Company shall implement and maintain appropriate technical and organisational security measures to protect Personal Data from security incidents and to preserve the security and confidentiality of the Personal Data (Art. 32 GDPR).

6.2 The Company and Company's Sub-Processors, which process the Client's Personal Data directly, have currently taken the technical and organizational measures described in Annex 1. The Company and/or the Sub-Processors may amend the measures described as long as the legally required overall security level is not reduced.

6.3 The Company undertakes to maintain confidentiality when processing the Personal Data of the Client, the Wearers and other Data Subjects. This shall continue to apply even after termination of the Agreement.

6.4 The Company shall ensure that any person who is authorised by the Company to process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality.

6.5 The Company shall not transfer Personal Data to any third party provider or location outside the European Economic Area except in accordance with the safeguards required under the GDPR.

6.6 Upon becoming aware of a Security Incident, the Company shall notify the Client without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Client.

6.7 The Client acknowledges that the security measures taken by the Company, are subject to technical progress and development and that the Company may update or modify the security measures from time to time

provided that such updates and modifications do not result in the degradation of the overall security of the Product.

6.8 The Client acknowledges that the Company takes all required technical and organizational measures, and documents the results. When necessary, the Client may request information from the Company about its practices and seek reasonable documentation about such practices.

6.9 If the data stored by the Client should be endangered by any seizure or attachment of the Company's property or by insolvency or composition proceedings or other events or measures taken by third parties, the Company will be obliged to inform the Client without undue delay. The Company will inform all responsible persons and bodies without undue delay to the effect that the Client is the Controller of, and has exclusive responsibility for and control over the data.

7. Data Subjects' Rights

7.1 The Data Subjects shall have and exercise the full range of rights provided under the Data Protection Laws, and the Client shall inform the Data Subjects of this fact.

7.2 Prior to recording, storing or processing a Data Subject's Personal Data, the Data Subject must have either consented to the processing or the processing is necessary for performance of a contract, compliance with a legal obligation, protection of the Data Subject's vital interests, protection of public interest or other legitimate interests. Processing must be fair and transparent, and Data Subjects should be aware of any potential risks.

7.3 The Client shall inform Data Subjects about the purpose of processing, the retention period and who the data will be shared with. The information and notification provided to the Data Subjects must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

7.4 The Data Subject shall have the right to obtain from the Client as well as the Company, confirmation as to whether or not Personal Data concerning them are being processed, and, where that is the case, have the right to access or obtain a copy of the Personal Data.

7.5 The Data Subject shall have the right to obtain from the Client as well as the Company, the erasure of Personal Data concerning them without undue delay and the Parties shall have the obligation to erase personal data without undue delay.

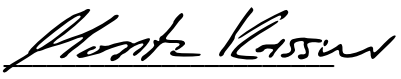
8. Final Provisions

8.1 In the unexpected event that the Parties become Joint Controllers, the Company shall only exercise controllership and be primarily responsible for the Personal Data which the Company solely introduced into the system. The Company may anonymise or deny the Client access to such Personal Data.

8.2 Should any provision of this Agreement be or become ineffective, the effectiveness of the other provisions of this Agreement shall not be affected thereby. The ineffective provision shall be replaced by a legally admissible provision which most effectively serves the purpose and intent of the ineffective provision.

8.3 This Agreement shall be governed by the laws of the Federal Republic of Germany without regard to its conflict of law provisions. To the extent legally possible, all disputes arising out of or in connection with this Agreement shall be brought before the courts of Berlin, Germany, which shall have exclusive jurisdiction.

IN WITNESS WHEREOF, the Parties, intending to be legally bound, have caused this Agreement to be executed by their authorized representatives as follows

Signed for and on behalf of:	Signed for and on behalf of:
Pupil Labs GmbH	_____
Signature: 	Signature: _____
Name: Moritz Kassner	Name:
Designation: CEO	Designation:
Place, Date: Berlin, 20.01.2020	Place, Date: _____

Annex 1

Description of the technical and organisational security measures implemented by the Company and the Company's Sub-Processor(s) in accordance with Art. 32 GDPR

I. Technical and organisational security measures implemented by the Company

- physical entry restrictions to the property and the facilities
- company-wide two-factor authentication
- internal access control to data and infrastructure
- company wide back-up implementations
- use of secure communication protocols (SSL, SSH etc.)
- data is only stored in EU Data Centers
- all handling of personal data is in accordance with GDPR law and best practices

II. Technical and organisational security measures implemented by the Company's Sub-Processor(s)

https://www.digitalocean.com/legal/data-security/

https://www.hetzner.com/unternehmen/rechenzentrum/
https://www.hetzner.com/assets/Uploads/downloads/Sicherheit-en.pdf