Data Processing Agreement

between

_____

as Controller (hereinafter “**Controller**”),

and

RooflineAI GmbH, Tunisstraße 19-23, 50667 Köln, Deutschland

as Data Processor (hereinafter “**Data Processor**”,
Controller and Data Processor jointly the “**Parties**”)

Preamble

The Controller has commissioned the Data Processor in a contract already concluded (hereinafter referred to as the "**Main Contract**") for the services specified therein. Part of the execution of the contract is the processing of personal data. In particular, Art. 28 GDPR imposes specific requirements on such commissioned processing. To comply with these requirements, the Parties enter into the following Data Processing Agreement (hereinafter referred to as the “**Agreement**”), the performance of which shall not be remunerated separately unless expressly agreed.

§ 1 Definitions

(1) Pursuant to Art. 4 (7) GDPR, the Controller is the entity that alone or jointly with other Controllers determines the purposes and means of the processing of personal data.

(2) Pursuant to Art. 4 (8) GDPR, a Data Processor is a natural or legal person, authority, institution, or other body that processes personal data on behalf of the Controller.

(3) Pursuant to Art. 4 (1) GDPR, personal data means any information relating to an identified or identifiable natural person (hereinafter "**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(4) Personal data requiring special protection are personal data pursuant to Art. 9 GDPR revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of Data Subjects, personal data pursuant to Art. 10 GDPR on criminal convictions and criminal offenses or related security measures, as well as genetic data pursuant to Art. 4 (13) GDPR, biometric data pursuant to Art. 4 (14) GDPR, health data pursuant to Art. 4 (15) GDPR, and data on the sex life or sexual orientation of a natural person.

(5) According to Article 4 (2) GDPR, the processing is any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) Pursuant to Article 4 (21) GDPR, the supervisory authority is an independent state body established by a Member State pursuant to Article 51 GDPR.

§ 2 Subject of the contract

(1) The Data Processor provides the services specified in the Main Contract for the Controller. In doing so, the Data Processor obtains access to personal data, which

the Data Processor processes for the Controller exclusively on behalf of and in accordance with the Controller's instructions. The scope and purpose of the data processing by the Data Processor are set out in the Main Contract and any associated service descriptions. The Controller shall be responsible for assessing the admissibility of the data processing.

(2) The Parties conclude the present Agreement to specify the mutual rights and obligations under data protection law. In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the Main Contract.

(3) The provisions of this contract shall apply to all activities related to the Main Contract in which the Data Processor and its employees or persons authorized by the Data Processor come into contact with personal data originating from the Controller or collected for the Controller.

(4) The term of this Agreement shall be governed by the term of the Main Contract unless the following provisions give rise to further obligations or termination rights.

§ 3 Right of instruction

(1) The Data Processor may only collect, process or use data within the scope of the Main Contract and in accordance with the instructions of the Controller. If the Data Processor is required to carry out further processing by the law of the European Union or the Member States to which it is subject, it shall notify the Controller of these legal requirements prior to the processing.

(2) The instructions of the Controller shall initially be determined by this Agreement. Thereafter, they may be amended, supplemented, or replaced by the Controller in writing or text form by individual instructions (Individual Instructions). The Controller shall be entitled to issue such instructions at any time. This includes instructions with regard to the correction, deletion, and blocking of data.

(3) All instructions issued shall be documented by the Controller. Instructions that go beyond the service agreed in the Main Contract shall be treated as a request for a change in service.

(4) If the Data Processor is of the opinion that an instruction of the Controller violates data protection provisions, it shall notify the Controller thereof without undue delay. The Data Processor shall be entitled to suspend the implementation of the relevant

instruction until it is confirmed or amended by the Controller. The Data Processor may refuse to carry out an obviously unlawful instruction.

§ 4 Types of data processed, group of Data Subjects, third country

(1) Within the scope of the implementation of the Main Contract, the Data Processor shall have access to the personal data specified in more detail in **Annex 1**.

(2) The group of Data Subjects affected by the data processing is listed in **Annex 2**.

(3) A transfer of personal data to a third country may take place under the conditions of Art. 44 et seq. GDPR.

§ 5 Protective measures of the Data Processor

(1) The Data Processor shall be obliged to observe the statutory provisions on data protection and not to disclose information obtained from the Controller's domain to third parties or expose it to their access. Documents and data shall be secured against disclosure to unauthorized persons, taking into account the state of the art.

(2) The Data Processor shall organize the internal organization within its field of responsibility in such a way that it meets the special requirements of data protection. It shall have taken the technical and organizational measures specified in **Annex 3** to adequately protect the Controller's data pursuant to Art. 32 GDPR, which the Controller acknowledges as adequate. The Data Processor reserves the right to change the security measures taken while ensuring that the contractually agreed level of protection is not undercut.

(3) The persons employed in the data processing by the Data Processor are prohibited from collecting, processing or using personal data without authorization. The Data Processor shall oblige all persons entrusted by it with the processing and performance of this contract (hereinafter "**Employees**") accordingly (obligation of confidentiality, Art. 28 (3) lit. b GDPR) and shall ensure compliance with this obligation with due care.

(4) The Data Processor has appointed a data protection officer. The Data Processor’s data protection officer is heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Information obligations of the Data Processor

(1) In the event of disruptions, suspected data protection violations or breaches of contractual obligations of the Data Processor, suspected security-related incidents or other irregularities in the processing of personal data by the Data Processor, by persons employed by it within the scope of the contract or by third parties, the Data Processor shall inform the Controller without undue delay. The same shall apply to audits of the Data Processor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

(a) a description of the nature of the personal data breach, including, to the extent possible, the categories and the number of Data Subjects affected, the categories affected and the number of personal data records affected;

(b) a description of the measures taken or proposed by the Data Processor to address the breach and, where applicable, measures to mitigate its possible adverse effects;

(c) a description of the likely consequences of the personal data breach.

(2) The Data Processor shall immediately take the necessary measures to secure the data and to mitigate any possible adverse consequences for the Data Subjects, inform the Controller thereof and request further instructions.

(3) In addition, the Data Processor shall be obliged to provide the Controller with information at any time insofar as the Controller's data are affected by a breach pursuant to paragraph 1.

(4) The Data Processor shall inform the Controller of any significant changes to the security measures pursuant to Section 5 (2).

§ 7 Control rights of the Controller

(1) The Controller may satisfy itself of the technical and organizational measures of the Data Processor prior to the commencement of data processing and thereafter regularly on a yearly basis. For this purpose, the Controller may, for example, obtain information from the Data Processor, obtain existing certificates from experts, certifications or internal audits or, after timely coordination, personally inspect the

technical and organizational measures of the Data Processor during normal business hours or have them inspected by a competent third party, provided that the third party is not in a competitive relationship with the Data Processor. The Controller shall carry out checks only to the extent necessary and shall not disproportionately disrupt the operations of the Data Processor in the process.

(2) The Data Processor undertakes to provide the Controller, upon the latter's verbal or written request and within a reasonable period of time, with all information and evidence required to carry out a check of the technical and organizational measures of the Data Processor.

(3) The Controller shall document the results of the inspection and notify the Data Processor thereof. In the event of errors or irregularities which the Controller discovers, in particular during the inspection of the results of the inspection, the Controller shall inform the Data Processor without undue delay. If facts are found during the control, the future avoidance of which requires changes to the ordered procedure, the Controller shall notify the Data Processor of the necessary procedural changes without delay.

§ 8 Use of service providers

(1) The contractually agreed services shall be performed with the involvement of the service providers named in **Annex 4** (hereinafter "**Sub-processors**"). The Controller grants the Data Processor its general authorization within the meaning of Article 28 (2) s. 1 GDPR to engage additional Sub-processors within the scope of its contractual obligations or to replace Sub-processors already engaged.

(2) The Data Processor will maintain a current list of Sub-processors on its website. The Controller acknowledges that the Data Processor may add or replace Sub-processors from time to time by updating such list. The Controller may object to an intended engagement or replacement of a Sub-processor for good cause under data protection law.

(3) Any objection must be raised in writing within thirty (30) days after the publication of the updated Sub-processor list. If the Controller does not object within this period, the addition or replacement shall be deemed approved.

(4) When engaging Sub-processors, the Data Processor shall oblige them in accordance with the provisions of this Agreement.

(5) A Sub-processor relationship within the meaning of these provisions does not exist if the Data Processor commissions third parties with services that are regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services provided by the Data Processor to the Controller and guarding services. Maintenance and testing services constitute Sub-processor relationships requiring consent insofar as they are provided for IT systems that are also used in connection with the provision of services for the Controller.

§ 9 Requests and rights of Data Subjects

(1) The Data Processor shall support the Controller with suitable technical and organizational measures in fulfilling the Controller's obligations pursuant to Articles 12-22 and 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as the right of access, correction or deletion with regard to his or her data, directly against the Data Processor, the latter shall not react independently but shall refer the Data Subject to the Controller and await the Controller's instructions.

§ 10 Liability

(1) In the internal relationship with the Data Processor, the Controller alone shall be liable to the Data Subject for compensation for damage suffered by a Data Subject due to inadmissible or incorrect data processing under data protection laws or use within the scope of the commissioned processing.

(2) The Data Processor shall have unlimited liability for damage insofar as the cause of the damage is based on an intentional or grossly negligent breach of duty by the Data Processor, its legal representative or vicarious agent.

(3) The Data Processor shall only be liable for negligent conduct in the event of a breach of an obligation, the fulfillment of which is a prerequisite for the proper performance of the contract and the observance of which the Controller regularly

relies on and may rely on, but limited to the average damage typical for the contract. In all other respects, the liability of the Processor - including for its vicarious agents - shall be excluded.

(4) The limitation of liability pursuant to § 10.3 shall not apply to claims for damages arising from injury to life, body, health or from the assumption of a guarantee.

§ 11 Termination of the Main Contract

(1) After termination of the Main Contract, the Data Processor shall return to the Controller all documents, data and data carriers provided to it or - at the request of the Controller, unless there is an obligation to store the personal data under Union law or other applicable national law - delete them. This shall also apply to any data backups at the Data Processor. The Data Processor shall on request provide documented proof of the proper deletion of any data.

(2) The Controller shall have the right to control the complete and contractual return or deletion of the data at the Data Processor in an appropriate manner.

(3) The Data Processor shall be obligated to keep confidential the data of which it has become aware in connection with the Main Contract even beyond the end of the Main Contract. The present Agreement shall remain valid beyond the end of the Main Contract as long as the Data Processor has personal data at its disposal which have been forwarded to it by the Controller or which it has collected for the Controller.

§ 12 Final provisions

(1) To the extent that the Data Processor does not expressly perform support actions under this Agreement free of charge, it may charge the Controller a reasonable fee therefore, unless the Data Processor's own actions or omissions have made such support directly necessary.

(2) Amendments and supplements to this Agreement must be made in writing. This shall also apply to any waiver of this formal requirement. The priority of individual contractual agreements shall remain unaffected.

(3) If individual provisions of this Agreement are or become wholly or partially invalid or unenforceable, this shall not affect the validity of the remaining provisions.

(4) This agreement is subject to German law.

Annex

Annex 1 - Description of the data/data categories

Email, password, name, IP address, Login times, independently uploaded and provided files

Annex 2 - Description of affected Data Subject/groups of affected Data Subjects

Controllers and their employees who have access to the software within the scope of the collaboration.

Annex 3 - Technical and organizational measures of the Data Processor

Introduction

This document summarizes the technical and organizational measures taken by the processor in accordance with Art. 32 para. 1 GDPR. These are measures that the processor uses to protect personal data. The purpose of the document is to support the processor in fulfilling their accountability obligation under Art. 5 para. 2 GDPR.

Confidentiality (Art. 32 para. 1 lit. b GDPR)

Entry Control

The following implemented measures prevent unauthorized entry to data processing facilities:

- Chip card/transponder locking system

Admission control

The following implemented measures prevent unauthorized access to data processing systems:

- Authentication with username and password
- Use of firewalls
- Use of VPN technology for remote access
- Encryption of data carriers
- Encryption of smartphones
- Encryption of notebooks/tablets
- Management of user permissions
- Creation of user profiles
- Use of 2-factor authentication
- Person control at the concierge or reception
- Key management/key book
- General instruction to manually lock the desktop when leaving the workplace

Access control

The following implemented measures ensure that unauthorized persons do not have access to personal data:

- Implementation of an authorization concept
- Number of administrators kept as small as possible
- Management of user rights by system administrators

Separation control

The following measures ensure that personal data collected for different purposes is processed separately:

- Physically separate storage on separate systems or data carriers
- Separation of production and test system
- Creation of an authorization concept
- Container apps when using private devices for business purposes (BYOD)

Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control

It is ensured that personal data cannot be read, copied, altered, or removed without authorization during transmission or storage on data carriers and that it can be verified which persons or entities have received personal data. The following measures are implemented to ensure this:

- Setup of VPN tunnels
- WLAN encryption (WPA2 with strong password)
- Provision of data via encrypted connections such as SFTP or HTTPS
- Prohibition of uploading business data to non-company servers

Input control

The following measures ensure that it can be verified who processed personal data in data processing systems at what time:

Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Fire extinguishers in server rooms
- Fire and smoke detection systems
- Air conditioning in server rooms
- Protected power strips in server rooms
- RAID system / disk mirroring
- Alarm notification for unauthorized access
- Regular backups

- Creation of a backup & recovery concept
- Monitoring of the backup process
- Storage of data backup in a secure, outsourced location
- Regular tests for data recovery and logging of results
- Hosting (at least the most important data) with a professional hoster

Procedures for regular review, assessment, and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Data protection management

The following measures are intended to ensure that an organization meeting the basic requirements of data protection law is in place:

- Use of the heyData platform for data protection management
- Appointment of heyData as the data protection officer
- Obligation of employees to data secrecy
- Regular training of employees in data protection
- Keeping a record of processing activities (Art. 30 GDPR)

Incident-Response-Management

The following measures ensure that reporting processes are triggered in the event of data protection violations:

- Reporting process for data protection violations according to Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR)
- Reporting process for data protection violations according to Art. 4 No. 12 GDPR to the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches
- Use of firewalls

Privacy-friendly default settings (Art. 25 para. 2 GDPR)

The following implemented measures take into account the principles of "Privacy by design" and "Privacy by default":

- Training of employees in "Privacy by design" and "Privacy by default"
- No more personal data is collected than necessary for the respective purpose.

Order control

By the following measures, it is ensured that personal data can only be processed according to instructions:

- Written instructions to the contractor or instructions in text form (e.g., via data processing agreement)

- Ensuring the destruction of data after the end of the contract, e.g., by requesting corresponding confirmations

- Confirmation from contractors that they obligate their own employees to data secrecy (typically in the data processing agreement)

Annex 4 – Current Sub-processors

Name	Function	Server location
Hetzner Online GmbH	Server provider and data center	EU (Germany)
Microsoft Ireland Operations Ltd.	Email, productivity and collaboration software	EU
GitHub, Inc.	Source code hosting and development collaboration	USA
Attio Ltd.	Customer relationship management (CRM)	UK/EU
Linear Orbit, Inc.	Issue and project tracking	USA
Slack Technologies (Salesforce, Inc.)	Internal messaging and communication	USA