Data Processing Agreement

between

a Customer (as defined in Levity AI’s Terms of Service)

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

and

Levity AI GmbH, Schoenhauser Allee 43A, 10435 Berlin

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 offences 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; this applies in particular with regard to the transfer of personal data to a third country or to an international organization. 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

(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**.

§ 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, Gormannstr. 14, 10119 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 quarterly 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 subcontractors

(1) The contractually agreed services shall be performed with the involvement of the subcontractors named in **Annex 4** (as 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 shall inform the Controller in advance by e-mail newsletter of any intended change regarding the involvement or replacement of a sub-processor. The email newsletter will be received by the Processor after signing up for the newsletter via https://levity.ai/signup. The Controller may object to an intended enlistment or substitution of a sub-processor for good cause under data protection law.

(3) The objection to the intended involvement or replacement of a subcontracted processor must be raised within 2 weeks of the information being sent in the email newsletter. If there is a good cause under data protection law and a mutually agreeable solution cannot be found between the Controller and Data Processor, the Controller shall have a special right of termination at the end of the month following the objection.

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

(5) A subcontractor 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 subcontractor 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 Responsible Party 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 the law of the Federal Republic of Germany - 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.

§ 11 Final provisions

(1) 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.

(2) 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.

(3) This agreement is subject to German law.

<u>Annex</u>

Annex 1 - Description of the data/data categories

all data that customers insert into Levity AI’s services such as customer support data (names, email addresses, addresses, messages) and messenger data (names, email addresses, content of messages)

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

Controllers, employees of Controllers, customers of Controllers, third parties

Annex 3 - Technical and organizational measures of the Data Processor

1. This Annex describes the technical and organizational measures of Levity AI GmbH.

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

2.1 Access control

The following implemented measures prevent unauthorized persons from gaining access to data processing facilities:

- Alarm system
- Securing of building shafts
- Manual locking system (e.g. key)
- Bell system with camera
- Key control / key book
- Careful selection of security personnel
- Visitors only accompanied by staff
- Careful selection of cleaning personnel
- Instruction to employees not to work in premises accessible to the public (e.g., cafés)
- Work in home office: unauthorized persons have no access to employees' homes
- Work in home office: instruct employees, if possible, to work in workrooms separated from living quarters

2.2 Access control

The following implemented measures prevent unauthorized persons from accessing data processing systems:

- Authentication with user and password
- Use of firewalls
- Automatic desktop lock
- Management of user permissions
- Creation of user profiles
- Use of 2-factor authentication
- General instruction to lock desktop manually when leaving the workplace

2.3 Access control

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

- Logging of access to applications (especially when entering, changing and deleting data).
- Use of an authorization concept
- Number of administrators kept as small as possible
- Secure storage of data media
- Management of user rights by system administrators
- Instruction to employees that only absolutely necessary data is printed out
- Instruction to employees that data is deleted only after consultation

2.4 Separation control

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

- Separation of productive and test system
- Logical client separation (on the software side)
- Creation of an authorization concept
- Definition of database rights
- Internal instruction to anonymize/pseudonymize personal data in the event of disclosure or after expiry of the statutory deletion period, if possible.

2.5 Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

Pseudonymization is the processing of personal data in such a way that it can no longer be assigned to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organizational measures. For this purpose, the data is linked to unique pseudonyms before further processing and additional personal data is removed. The following measures are implemented:

- Internal instruction to anonymize/pseudonymize personal data in case of disclosure or after expiration of the legal deletion period, if possible.

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

3.1 Transfer control

It is ensured that personal data cannot be read, copied, modified or removed without authorization during transfer or storage on data carriers and that it is possible to verify which persons or bodies have received personal data. The following measures are implemented to ensure this:

- E-mail encryption
- WLAN encryption (WPA2 with strong password)
- Logging of accesses and retrievals
- Provision of data via encrypted connections such as SFTP or HTTPS
- Prohibition of uploading business data to servers outside the company

3.2 Input control

The following measures ensure that it is possible to check who has processed personal data in data processing systems and at what time:

- Logging of the input, modification and deletion of data
- Retention of forms whose data have been transferred to automated processing systems
- Creation of an overview of which applications can be used to enter, change and delete which data
- Traceability of the input, modification and deletion of data through individual user names (not user groups)
- Assignment of rights for entering, changing and deleting data on the basis of an authorization concept
- Clear responsibilities for deletions
- Instruction to employees to delete data only after consultation

4. 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 and smoke detection systems
- Regular backups
- Storage of data backups in a secure, off-site location
- Separation of operating systems and data
- Hosting (at least of the most important data) with a professional hoster

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

5.1 Data Protection Management

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

- Use of the heyData platform for data protection management
- Appointment of the data protection officer heyData
- Obligation of employees to maintain data secrecy
- Regular training of employees in data protection
- Keeping an overview of processing activities (Art. 30 GDPR)
- Conducting data protection impact assessments, if required (Art. 35 GDPR).

5.2 Incident Response Management

The following measures are intended to ensure that notification processes are triggered in the event of data protection breaches:

- Notification process for data protection breaches pursuant to Art. 4 no. 12 GDPR vis-à-vis the supervisory authorities (Art. 33 GDPR).
- Notification process for data protection breaches pursuant to Art. 4 no. 12 GDPR vis-à-vis the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data mishaps
- Use of firewalls

5.3 Data protection-friendly default settings (Art. 25 para. 1 GDPR)

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

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

5.4 Order control

The following measures ensure that personal data can only be processed in accordance with instructions:

- Written instructions to the contractor or instructions in text form (e.g. by order processing contract).
- Ensuring that data is destroyed after completion of the order, e.g. by requesting appropriate confirmations

- Confirmation from contractors that they commit their own employees to data secrecy (typically in the order processing contract)
- Careful selection of contractors (especially with regard to data security)

Annex 4 – Current subcontractors

No.	Name of the further processor	Description of processing via this further processor
1	Ahrefs Pte. Ltd. (201227417H) 16 Raffles Quay, #33-03 Hong Leong Building, Singapore 048581	Analytics software
2	Auth0, Inc., 10800 NE 8th Street Suite 600, Bellevue, WA 98004, USA	Authentication software
3	Amazon Web Services Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, USA.	Secure cloud service platform for database storage
4	Asana, Inc., 1550 Bryant Street, Suite 200, San Francisco, CA 94103	Project management software
5	Blendr NV. Grauwpoort 1, 9000 Gent, Belgium	3rd party integration provider
6	Calendly LLC. 1315 Peachtree St NE, Atlanta, GA 30309, USA	Meeting booking software
7	APIHub, Inc. (Clearbit) 90 Sheridan St San Francisco, CA 94103 United States	Customer data enrichment
8	Clubhouse Software Inc. 79 Madison Avenue, 2nd Floor, New York, NY 10016 United States	Project and product management software
9	Facebook Ireland Ltd. 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Republic of Ireland	Ads, retargeting, lead generation
10	Figma Inc. 142 Minna Street, Floor 2, San Francisco, CA 94105 United States	Product design and prototyping software
11	Flatfile Inc. 1624 Market Street, Suite 202, PMB 9138, Denver CO 80202	Handling certain customer data uploads
12	Formagrid, Inc. (Airtable) 769 Dolores Street, San Francisco, CA 94110, United States	Data storage software
13	Frontegg Ltd. Rokach Boulevard 97, Tel Aviv 6902064, Israel	Authentification and permissioning software
14	Google Ireland Ltd (Google Drive), Gordon House, Barrow Street, Dublin 4, Ireland	Cloud storage for documents
15	Google Ireland Ltd (Google Mail), Gordon House, Barrow Street, Dublin 4, Republic of Ireland	Cloud-based email client
16	Google Ireland Ltd (Google Meet), Gordon House, Barrow Street, Dublin 4, Republic of Ireland	Video conferencing software
17	Google Ireland Ltd (Google Analytics) Gordon House, Barrow Street, Dublin 4, D04E5W5 Ireland	Website tracking and analytics
18	Google Ireland Ltd (Google Search Console) Gordon House, Barrow Street, Dublin 4, D04E5W5 Ireland	Search-related analytics
19	Google Ireland Ltd (Google Cloud Platform) Gordon House, Barrow Street, Dublin 4, D04E5W5 Ireland	Secure cloud service platform for database storage
20	Heap Inc. 460 Bryant Street, 3rd Floor, San Francisco, CA 94107 United States	Analytics
21	Hotjar Ltd	Users’ behavior visualization software

	Level 2, St Julian's Business Centre, 3, Elia Zammit Street, St Julian's STJ 1000, Malta	
22	Intercom R&D Unlimited Company 2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Republic of Ireland	Help and support widget in app
23	LinkedIn Ireland Unlimited Co. Gardiner House, Wilton Plaza, Dublin 2, Dublin, Ireland	Ads, retargeting, lead generation
24	Mailchimp, The Rocket Science Group, LLC 675 Ponce de Leon Ave NE, Suite 5000 Atlanta, GA 30308, USA	Email marketing automation software
25	A Medium Corp 760 Medium Street, San Francisco, CA 94102 United States	Blogging
26	Miro Technologies Inc. 5643 Copley Drive, San Diego, CA 92111 United States	Design and brainstorming software
27	Notion Labs, Inc. 2948 20th St, Apt. 300 San Francisco, CA 94110, USA	Documentation and notes storage software
28	Optimizely Inc. 631 Howard Street, Suite 100, San Francisco, CA 94105 United States	Analytics, content experiments
29	Paddle Ltd. Core B, Block 71, The Plaza, Park West, Dublin 12, Ireland	Online payment processing and billing software
30	SendinBlue SAS 47, Rue de la Chaussee d'Antin, Paris, 75009 France	Email marketing
31	Slack Technologies Inc. 500 Howard Street, San Francisco, CA 94105, USA	Team communication and collaboration software
32	Stripe Inc. 510 Townsend Street San Francisco, CA 94103, USA	Online payment processing and billing software
33	Twitter Inc. 1355 Market Street, Suite 900, San Francisco, CA 94103 United States	Ads, retargeting, lead generation
34	TYPEFORM SL. C/Bac de Roda, 163 (Local), 08018 – Barcelona (Spain)	Survey software
35	Segment.io, Inc. 101 15th St., San Francisco, CA 94103, USA	Data Analysis Service
36	Semrush Inc. 800 Boylston Street, Suite 2475, Boston, MA 02199 United States	Data Analysis Service
37	Valohai Oy Linnankatu 16, 4th Floor, Turku, 20100 Finland	MLOps software
38	Webflow Inc. 36889 North Tom Darlington Drive, Carefree, AZ 85377	Website design and hosting software
39	YouTube Inc. 1000 Cherry Avenue, San Bruno, CA 94066 United States	Ads, retargeting, lead generation
40	Zapier Inc. 548 Market St. 62411, San Francisco, CA 94104-5401	Process automation, information transmission
41	Zoom Video Communications, Inc. 55 Almaden Blvd. Suite 600, San Jose, CA 95113, USA	Video conferencing software