Data Processing Agreement

Customer

herein the **"Data Controller"**

and

MeisterLabs GmbH
Zugspitzstraße 2
85591 Vaterstetten
Germany

herein the **"Data Processor"**

individually referred to as a **"Party"** and jointly referred to as the **"Parties"**

enter into the following Data Processing Agreement (**"DPA"**)
governing the processing of personal data in possession of the Data Controller by the Data Processor.

1 Preamble

1.1 This DPA forms an annex to the Terms and Conditions, which are also applicable to this agreement, unless otherwise stated in this DPA.

1.2 With the acceptance of the Terms and Conditions, the Data Controller and the Data Processor have also accepted this this DPA as part of the click-through agreement to ensure that the processing of personal data by the Data Processor, as commissioned by the Data Controller, is carried out in compliance with the applicable data protection laws.

2 Definitions

2.1 "Data protection laws" include the EU's General Data Protection Regulation (EU/2016/679) (**"GDPR"**) as well as any national data protection acts and provisions governing the data processing activities under this DPA.

2.2 "Personal customer data" include all personal data the Data Processor, and any sub-processors used by the Data Processor, process on behalf of the Data Controller under the present DPA.

2.3 Any terms used in this DPA are to be interpreted within the meaning of the EU's GDPR, unless expressly agreed otherwise.

3 Rights and obligations of the Data Controller

3.1 The Data Controller undertakes to process the personal customer data that have been disclosed to the Processor and any sub-processors, in accordance with the relevant and applicable laws and regulations (in particular the data protection laws).

4 Rights and obligations of the Processor

The Data Processor is obliged

4.1 to process personal customer data only upon documented instructions of the Data Controller . The instructions for all processing steps necessary for performance of the contract are deemed to have been given upon conclusion of the contract.

4.2 to notify the Data Controller immediately if the Data Processor is of the opinion that the instructions of the Data Controller violate applicable data protection laws. However, this does not infer any obligation for the Data Processor to seek legal advice. Similarly, the fulfillment of this obligation does not constitute the provision of legal advice to the Data Controller.

4.3 as far as this is possible, to inform the Data Controller without undue delay of any inquiry, complaint, notification, request or other communication (herein referred to as **"Request"**) received from any regulatory or governmental authority, or other third party with regard to the processing of personal customer data by the Data Processor. The Data Processor will assist the Data Controller appropriately to enable him to respond to such a request in accordance with applicable data protection laws. Answers are given by the Data Controller exclusively unless the Data Processor is obliged under mandatory law to answer directly.

4.4 to assist the Data Controller, taking into account the nature of the processing, to comply with his obligation to reply to requests to exercise the rights set out in Chapter III of the General Data Protection Regulation (EU/2016/679) (right of access, right of rectification and erasure, right to be forgotten, right of data portability, right to restriction of processing and right to object) relating to the processing of personal customer data.

4.5 to assist the Data Controller, taking into account the nature of the processing and the information at their disposal, in complying with the obligations set out in Articles 32 to 36 (security of processing; notification of personal data breach to the supervisory authority and to data subjects; data protection impact assessment and consultation of the data protection authority) in relation to the processing of personal customer data, in particular

a) to notify the Data Controller in writing as soon as possible if the Processor becomes aware of any personal data breach relating to personal customer data;

b) to provide the Data Controller with information on the personal data breach as soon as possible.

4.6 to delete all personal customer data upon termination of this DPA or the Main Agreement, irrespective of the grounds for termination, or upon completion of the processing services under this DPA. If required by legal obligations to which the Data Processor is bound, the Data Processor may, in accordance with these obligations, keep a copy of the data of the Data Controller. Furthermore, the Data Processor is entitled to keep all necessary records and information (which may include personal customer data) required to prove compliance with his obligations under the Main Agreement and this DPA, in accordance with applicable statutory periods of limitation.

4.7 The Data Processor will, upon request, provide the Data Controller with all information necessary to demonstrate compliance with the obligations set out in this DPA, the Main Agreement or the data protection laws.

5 Sub-processors

5.1 The Data Controller hereby grants general consent to the commissioning of sub-processors in connection with the processing of data.

5.2 The Data Processor undertakes to inform the Data Controller of any change regarding the involvement or replacement of further sub-processors. Provided that the Data Controller does not object within two weeks, the involvement or replacement will be deemed approved. In the case of an objection, the Data Processor may terminate the DPA subject to no less than two weeks' notice. In this case, the Data Processor is no longer obligated to provide those services that involve the processing of personal customer data on behalf of the Data Controller. The remaining provisions of the Main Agreement remain unaffected by the termination of the DPA.

5.3 Furthermore, the Data Processor is obliged

a) to ensure, by written agreement, that all sub-processors are in substance bound by the same obligations that apply to the Processor under this DPA.

b) to assume liability to the Data Controller if a sub-processor fails to comply with his data protection obligations under the written agreement within the meaning of section a).

6 International data Transfers

6.1 The Data Processor may process personal data within the European Economic Area (**"EEA"**) or in countries where the European Commission decided that they ensure an adequate level of protection.

6.2 The Data Processor may only transfer personal data to sub-processors established in countries that the European Commission does not deem to ensure an adequate level of data protection if the Data Processor ensures that the requirements set forth in Chapter V of the GDPR are complied with, in particular by concluding Module 3 of the Standard Contractual Clauses adopted by the EU Commission (Decision 2021/914/EU) with the sub-processor.

6.3 Should the Standard Contractual Clauses adopted by the EU Commission (Decision 2021/914/EU) be invalidated, replaced, annulled or otherwise designed in such a way that they no longer constitute adequate safeguards for data transfers to third countries, the Parties undertake to find an alternative solution that complies with the applicable data protection laws and ensures the lawfulness of transferring the personal data to third countries.

7 Technical and organizational measures

7.1 The Data Processor undertakes to take the necessary technical and organizational measures to ensure compliance with the applicable data protection laws and this DPA. An overview of technical and organizational measures taken by the Processor is included in Annex 2. The Data Controller confirms that the technical and organizational measures provided in Annex 2 are adequate.

7.2 The Data Processor is obliged to notify the Data Controller of any significant changes to the technical or organizational measures. The Processor will ensure that such changes will not result in a lower level of protection.

8 Audit

8.1 The Data Processor will permit the Data Controller or an independent external auditor commissioned by the Data Controller and acting on the instructions of the Data Controller to conduct audits and inspections with regard to data protection and/or data security of personal customer data (**"Audit"**) in order to audit the data protection and data security procedures under this DPA. The Data Processor has the right to reject an auditor provided that he raises justified objections to the auditor's appointment. An objection is deemed justified in particular if the auditor has close ties to a competing company, or if there are other reasons which cast doubt on the professional qualification or independence of the auditor.

8.2 The Data Controller must, without exception, notify the Data Processor in writing of any audits relating to the processing of personal customer data with a reasonable lead time (usually no less than twenty-one days), stating the time, date, intended duration and the names of the persons conducting the audit. The audit may only be carried out during the Data Processor's regular

business hours and without disrupting the Data Processor's business operations. The Data Controller must bear the cost of audits.

8.3 The Data Controller may carry out audits no more than once per calendar year, unless there is reasonable cause for additional audits.

9 Confidentiality of data

The Data Processor warrants that the persons authorized by him to process the personal customer data have committed themselves to confidentiality or are bound to secrecy by law.

10 Term and termination

10.1 This DPA will enter into force as specified in 1.2. and will apply for as long as the Data Processor processes personal data on behalf of the Data Controller in connection with the provision of services under the Main Agreement.

11 General provision

11.1 Ancillary agreements must be made in writing. The above also applies to waiving the requirement of the written form.

11.2 Should the Data Controller and the Data Processor enter into additional agreements that are in conflict with this DPA, the provisions of this DPA relating to processing personal customer data shall take precedence over any conflicting provisions.

Annex 1

If Data Controller wishes to engage Data Processor with the processing of additional personal data than the personal data mentioned below, it is in the responsibility of the Data Controller to notify the Data Processor. Data Processor will then review the request and - if possible - confirm the changes.

Data subjects

The personal data processed relate to the following categories of data subjects:

- Data Controller's customers
- Customers of the Data Controller's customers
- Data Controller's employees
- Employees of the Data Controller's customers
- Contact persons at Data Controller's suppliers
- Contact persons at suppliers to the Data Controller's customers
- Data Controller's prospective customers
- Prospective customers of the Data Controller's customers

Categories of data

The following data categories are processed:

- Personnel master data (e.g. salutation, last name, first name, address, title, position)
- Communications data (phone number, email)
- Contract master data (e.g. contractual relationships, product and contractual interests)
- Customer history
- Contract billing and payment data
- Planning and control data
- Technical log data (e.g. login, IP address, time stamp)
- Data sent by users of their own accord in messages, free text fields or as content in files:
  Data that has been entered by the user by creating mind maps and tasks with title, descriptions, comments, files and images

Special data categories

No.

Scope, nature and purpose of the Data Processing, nature of the personal data and data subjects

The Data Processor provides an online mind mapping tool with which ideas can be visualized, developed and shared. The mind map editor is used for brainstorming, structuring information, taking notes, and planning projects at the client.

The Data Processor provides an online task management tool with which projects can be created at the Data Controller and tasks can be assigned to different team members. The Data Controller can also manage checklists and deadlines in the tasks, view the progress of the project and track the progress of the project.

The Data Processor provides an online documentation tool with which notes and documents can be created at the Data Controller and documents can be shared with team members. The documents are used for note-taking, checklists, presentations, and sharing information to collaborators.

Scope, nature and purpose of the Data Processing (services commissioned):

- in accordance with the definition in Art. 4 no. 2 of the GDPR

The Data Processor assumes the hosting, maintenance and support for the above online tools. Access to personal data of the affected persons is not excluded, as far as such data are entered into the online tools by the users. Furthermore, the Data Controller shall provide the Data Processor with personal data for the purpose of setting up the user accounts.

Annex 2 - Overview of technical and organizational measures

Privacy Policy / Security Concept

The Data Controller's and Processor's privacy policies (including any relevant security policies) address the security of personal data.

Organizational security measures

The internal organization is appropriately designed to meet the specific requirements of data protection.

- Policies and procedures are in place and are checked regularly.
- Risks are evaluated and documented
- Information is classified according to a policy.
- A security manager has been appointed.
- Appropriate measurements for the performance and effectiveness of security management are in place.

Security measures for changes in service

The change management process includes a data protection impact analysis and information security risk evaluation.

Personal data may only be utilized for process or system development activities and the testing associated therewith if they have been anonymised prior to their utilization or otherwise protected.

Security measures in user management

Measures prevent data processing systems from being used by unauthorized persons.

- Passwords are managed with a password manager.
- A password policy is in place and enforced through the password manager and a Unified Endpoint Management system.
- Two-factor authentication is enforced where required by our policy.

Security measures for logical access

Logical access to personal data is restricted.
Measures ensure that persons authorized to use the data processing systems may only access data for which they are authorized.

- Access is granted based upon the need-to-know principle (Principle of Least Privilege).

- Access is granted/revoked upon request. Revocation may also happen automatically after a set timeframe, or manually after a review was conducted.
- We have an authorization request process in place, with documentation of the user that needs access, the system, the requested permissions, the requester and the authorizer.
- As part of the HR on boarding process and HR off boarding process, access rights will be granted/revoked as well.
- We conduct regular reviews of logical access on all our systems, depending on the classification of information and document those reviews.

Separation of mandates

Customer data is logically separated and separated from each other by security mechanisms.
In addition, there are tests and staging systems that are completely separate from the productive system.

Deleting data

Data is deleted from the database or storage and backups are deleted after 95 days.

Security measures for physical access

Physical access to personal data in any format is restricted.

Personal data, in any format, is protected against accidental disclosure due to natural disasters and environmental hazards.

Personal data on portable media or devices is protected against unauthorized access. Storage media security measures prevent unauthorized reading, copying, modification, or removal of storage media.

Google data center (Frankfurt, Germany)

- see encryption measures and certificates of the data center:
  https://cloud.google.com/docs/security/encryption/default-encryption
  https://cloud.google.com/security/compliance/iso-27001/

MeisterLabs GmbH office (Munich, Germany)

- The MeisterLabs GmbH office in Munich, Zugspitzstraße 2, 85591 Vaterstetten.
- Access to the office building is secured via an external door with a lock.
- Access to the MeisterLabs GmbH office is additionally secured with a lock and only possible with the appropriate keys, which are only in the hands of MeisterLabs GmbH employees. The landlord does not have a key to these premises. The keys are handed out to employees of MeisterLabs GmbH when the contract is signed, the key is withdrawn when the employment relationship is terminated, and there is corresponding documentation on keys in circulation.
- Guests or visitors are not received in the office of MeisterLabs GmbH.
- The company network in the above-mentioned premises of MeisterLabs GmbH in Munich is protected by a state-of-the-art firewall.

Security measures for storage

There are measures in place to prevent unauthorized input and unauthorized evaluation, modification or deletion of stored personal data. These also include protection against malware.

- Cloud Storage
  - Data is encrypted at block-level, see “Security measures for physical access”.
  - Access to personal data is thoroughly managed, see “Security measures for logical access”.
  - Computer resources in the cloud are automatically checked for vulnerabilities.
  - A Host Intrusion Detection System (HIDS) is in place to detect unusual behavior on the machines.
  - Daily backups are kept for 14 days, after which they are deleted.
- Employee devices
  - All employee devices are full disk encrypted. A firewall and antivirus protection is present. Automatic screen locks are activated. Asset management processes are implemented. All devices are enrolled in a Unified Endpoint Management solution to automatically enforce policies.
  - Stolen or lost devices can be remotely locked or wiped.
  - Only authorized repair shops can be used to repair company owned devices. Computers are only bought at authorized resellers.
  - Storage of data on removable media is discouraged. Policies for disposal are in place.

Secure Development

A secure development policy is in place to make sure insecure code is not introduced, existing code and third party libraries are regularly checked for vulnerabilities.

- Measures are in place to detect insecure code (static code analysis)
- Development needs to adhere to our secure development policy.
- All application code is peer reviewed.
- Used libraries are automatically scanned for known vulnerabilities.

Security measures for data input

There are measures in place to ensure that it can be verified what personal data has been entered into data processing systems, by whom and when.

Control over processed information

The data subject has the possibility to obtain information on the processing of his/her personal data, to have such data corrected and deleted.

Data is deleted online directly in the database or in the online storage and then disappears from the back-ups after 2 weeks as soon as they are renewed.

Security measures during processing

There are measures in place to ensure that, in the case of commissioned processing of personal data, the data is processed strictly in compliance with the Data Controller’s instructions.

Security measures for transfer of data

There are measures in place to prevent unauthorized reading, copying, modification or deletion of personal data during the transmission or transport of storage media.

- All connections to our data centers are encrypted in transit with state of the art TLS. Supported ciphers are regularly checked
- for deprecation.
- Third parties that process personal data have appropriate security controls in place.
- Unencrypted email attachments do not include confidential or sensitive information.

Availability and Resilience

- Business continuity and disaster recovery plans are in place, tested, and updated regularly.
- See certificates of the data center: https://cloud.google.com/security/compliance/iso-27001/
- Cloudflare as a service provider for DDoS protection

Measures in the event of security incidents

- A documented procedure for the management of data protection incidents and violations has been implemented.
- Employees are regularly trained on preventing security incidents but also on how to react to such incidents, including the possible need to quickly report incidents to authorities and inform users.
- An internal hotline for security and data privacy incidents has been established and employees are encouraged to report incidents.

Assessment of security measures

Assessments and tests of the effectiveness of the key organizational, technical, and physical safeguards protecting personal data are conducted according to our policies, containing but not limited to:

- External vulnerability scans and penetration tests are conducted at least once a year
- External code audits are conducted when deemed necessary.
- Internal infrastructure audits are conducted at least once a year.
- Internal architecture and security audits are conducted at least once a year.

The results of the analyses are documented.

Annex 3 - Approved Sub-Processors

Upon conclusion of this DPA, the Data Controller approves of the engagement of the sub-processors listed below:

Subprocessors		Description of processing (*including a clear distinction of responsibilities in case more subprocessors have been approved*)	
Name	**Address**		**Processing location**
Provision of Meister-Products			
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Warranty of **product supply** by product hosting in the cloud region Europe. Providing AI-functionality.	Frankfurt a.M., Germany
MeisterLabs Software GmbH	Mariahilferstraße 97, 1060 Wien, Österreich	Warranty of **product functionality** especially by product maintenance and product development	Vienna, Austria
SmartBear (Ireland) Limited	Mayoralty House, Flood Street, Galway, Ireland	Warranty of **product functionality** inter alia by product troubleshooting with the help of protocols for the treatment of bugs in exceptional cases	USA
Iterable Ireland Limited	Iveagh Court, 8th Floor, Block E, Harcourt Rd, Dublin, Ireland	Warranty of **product functionality** by e-mail and notification sending.	EU
MongoDB Limited	Building 2, Number 1 Ballsbridge Shellbourne Road, Ballsbridge, D04 Y3X9, Dublin, Ireland	Warranty of **product functionality** by hosting certain application databases.	EU
Cloudflare	101 Townsend Street,	Warranty of **product safety**, especially	EU (multiple data

Inc.	San Francisco, California 94107, U.S.A.	through protection from DDoS attacks and provision of Content Delivery Network	centers)
Support Services			
Aircall SAS	11-15 rue Saint-Georges, 75009 Paris, Frankreich	Voice over IP in connection with support requests via phone	Frankfurt, Germany
Mailgun Technologies, Inc.	535 Mission St., 14th Floor, San Francisco, California 94105, USA	Email notification services	USA
Zendesk, Inc.	1019 Market Street, San Francisco, CA 94103, USA	Ticketing system for the organization and administration of support requests	EU (Germany, Belgium)
Crescendo, Inc.	201 Spear Street, Suite 1100, San Francisco, CA 94105, USA	Provision of AI-enabled support chatbot and general support services for basic plans	USA
Provision of AI-functionality within the Meister-Products. You can opt-out of using Meister AI functionality in your account settings any time.			
OpenAI Ireland Ltd	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 Yc43	Providing AI functionality within our products	USA