Data Processing Appendix

1. DEFINITIONS

1.1. The definitions used in the Agreement also apply to this Data Processing Appendix.

1.2. "**GDPR**" shall refer to Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.3. "**Member State**" shall refer to a member state of the European Union

1.4. "**Data Processor**" shall refer to MainFoundry.

1.5. "**Data Controller**" shall refer to the Customer.

2. ROLES & PROCESSING

2.1. This appendix sets forth the rights and obligations of the Parties with respect to the processing of personal data under the GDPR.

2.2. The Parties agree that during the Term of this Agreement, MainFoundry shall act as the data processor and the Customer shall act as the data controller.

2.3. During the Term of this Agreement, MainFoundry will process personal data on behalf of the Customer in accordance with this appendix.

2.4. The Data Processor shall process personal data only on documented instructions from the data controller, unless required to do so by EU or Member State law. The Data Processor shall immediately inform the Data Controller if the instruction, in the opinion of the Data Processor, contravene the GDPR or applicable EU or Member State data protection provisions.

2.5. The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis.

3. SECURITY OF PROCESSING

3.1. The Data Processor shall implement appropriate technical and organizational measures to ensure an appropriate level of security to mitigate the inherent risk in the processing of personal data.

3.2. The Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 GDPR along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under Article 32 GDPR.

3.3. The measures implemented by the Data Processor are:

(a) The Service processes the personal data that the Data Controller chooses to upload or synchronize, including email, calendar entries, documents and meeting recordings. Such content

may contain special categories of personal data within the meaning of GDPR article 9, and the Data Processor does not assume otherwise. The security measures taken by the Data Processor are risk-based and proportionate to the nature, scope, context and purposes of the processing, and to the risks to the rights and freedoms of natural persons, in accordance with GDPR article 32.

(b) Ensured two-factor authentication on all accounts with access to personal data.

(c) Ensured reasonable safeguards against IT-security threats on the database where the personal data is stored, including reasonable safeguards against the integrity, availability and resilience of the database system.

(d) Ensured organizational appropriate limitations on access to the personal data, as well as ensuring appropriate levels of confidentiality across the organization.

(e) Ensured any transmitted personal data only occurs by encrypted means of communication (e.g. HTTPS).

4. USE OF SUB-PROCESSORS & TRANSFER TO THIRD COUNTRIES

4.1. The Data Processor shall meet the requirements specified in Article 28(2) and (4) of the GDPR in order to engage another processor (a sub-processor)

4.2. The Data Controller grants the Data Processor the prior general written authorization to engage sub processors for the processing of personal data. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least one (1) month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

4.3. The Data Controller hereby grants authorization to the Data Processor for the following table of sub-processors already engaged by the Data Processor:

NAME	REGISTRATION NO.	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft Ireland Operations Limited	IE 8256796 U	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Hosting the cloud services where the database, document storage and user information of the Data Controller is located. This includes the AI services used to provide the AI features of the Service, optical character recognition used to read uploaded receipts and documents, speech services, and the transactional email service used to send

NAME	REGISTRATION NO.	ADDRESS	DESCRIPTION OF PROCESSING
			system emails such as password reset, onboarding and notification emails. Any personal data contained in emails sent between the Data Processor and the Data Controller will also be processed by this sub-processor (Outlook).
Hyperdoc Inc. (Recall.ai)	Delaware corporation; California Secretary of State entity no. 5973469 (registered 9 November 2023)	2261 Market Street #4339, San Francisco, CA 94114, United States	Recording, transcription and processing of meetings that the Data Controller chooses to have attended by the meeting-recording bot, including audio, video and transcripts containing personal data of the meeting participants.
Perplexity AI, Inc.	Delaware corporation; New York Dept. of State ID 6837808	115 Sansome Street, Suite 900, San Francisco, CA 94104, United States	Internet search performed on request, including searches run by AI agents and company and contact enrichment. Search queries may contain personal data such as names, company names and email domains.

4.4. The Data Processor is responsible for ensuring that the same data processing obligations imposed upon the Data Processor shall also be imposed upon any sub-processors engaged by the Data Processor. Where a sub-processor fails to fulfil its data protection obligations, the Data Processor remains fully liable to the Data Controller for the performance of that sub-processor's obligations.

4.5. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V of the GDPR.

4.6. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

4.7. The use of sub-processors in third countries entail that personal data may be transferred to the countries in which these are located. In these cases, the Data Processor will ensure that processing is done in accordance with GDPR through processing agreements based on a valid transfer mechanism under Chapter V of the GDPR — the EU Commission's standard contractual clauses or, where the sub-processor is covered by one, an adequacy decision such as the EU–US Data Privacy Framework — including appropriate organizational and technical measures to maintain the security in processing. The Data Processor has ensured a legal basis of transfer as well as any additional measures required to guarantee the safety of processing.

5. ASSISTANCE TO THE DATA CONTROLLER

5.1. The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is reasonably practicable, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

5.2. The Data Processor shall, taking into account the nature of the processing and the information available to it, assist the Data Controller in ensuring compliance with the obligations set out in GDPR articles 32 to 36, including security of processing, notification of a personal data breach to the supervisory authority and communication of a breach to data subjects, data protection impact assessments, and prior consultation of the supervisory authority. The Data Processor shall further assist the Data Controller, insofar as this is reasonably practicable, in ensuring compliance with the Data Controller's obligations towards any regulatory agency or data subjects with respect to personal data processed under this Agreement.

6. NOTIFICATION OF BREACH, ERASURE OF DATA & AUDITS

6.1. In case of any personal data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.

6.2. The Data Processor's notification to the Data Controller shall take place without undue delay and, where feasible, within 24 hours after the Data Processor has become aware of the personal data breach, followed by further information in phases as it becomes available. This is to leave the Data Controller sufficient time within its own 72-hour deadline to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the GDPR. The Data Processor shall assist in any practical capacity with the reporting obligation of the Data Controller towards the supervisory authority.

6.3. On termination of the provision of personal data processing services, the Data Processor shall, at the choice of the Data Controller, delete or return all personal data processed on behalf of the Data Controller, and shall certify to the Data Controller that it has done so, unless Union or Member State law requires storage of the personal data. The Data Controller may request an export of its data before deletion in accordance with the Master Services Agreement.

6.4. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and

contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

6.5. The following procedures shall be applicable to the Data Controller's audits, including inspections, of the Data Processor:

(a) The Data Controller can with two (2) months' notice and at most once every two (2) years request/perform an audit of the Data Processor to establish if processing of personal data is in compliance with this appendix and the GDPR. These limitations do not apply where the audit is prompted by a personal data breach affecting the Data Controller's personal data, by a substantiated concern regarding the Data Processor's compliance, or by a request or instruction from a competent supervisory authority, in which case the Data Controller may audit on reasonable notice.

(b) The audit is to be performed by an external third party capable of producing an inspection report.

(c) Any expenses incurred by the Parties during an audit are to be paid for by the Data Controller.

6.6. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

7. INFORMATION ABOUT THE PROCESSING

7.1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

(a) To register the Authorized Users of the Data Controller in the Data Processors database in order to grant access to the Service

(b) To process personal data in documents stored by the Data Controller in the Data Processor's System.

7.2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

(a) Collecting and storing e-mail-addresses, first and last names of users in a database.

(b) Collecting and storing information stored in emails or documents that the users of the Data Controller choose to upload to the Data Processor's system.

7.3. The processing includes the following types of personal data about data subjects:

(a) E-mail address of the Authorized Users of the Service.
(b) First and last names of the Authorized Users of the Service
(c) Personal data contained in emails or documents. These typically include email addresses, first and last names.

(d) The Service comprises features that process personal data in different ways and, in two cases, through sub-processors outside the EU/EEA. Those features are:

(e) AI assistant, agents and text generation. Prompts, and the CRM records, documents or messages the feature is invoked on, are sent to Microsoft's Azure OpenAI service within the Data

Processor's Azure tenant. Invoked by the Data Controller's users or by agents the Data Controller has configured. No separate retention beyond the resulting records stored in the Service.

(f) Receipt and document reading (optical character recognition). Uploaded receipts and documents are sent to Microsoft's Azure OCR service to extract their contents. Invoked when the Data Controller uploads a document.

(g) Speech-to-text transcription. Audio supplied to the Service is sent to Microsoft's Azure Speech service, including speaker separation. Invoked by the Data Controller.

(h) Meeting recording and transcription. Where the Data Controller sends the meeting-recording bot to a meeting, the audio, video and resulting transcript are processed by Hyperdoc Inc. (Recall.ai) in the United States. This feature is optional and is initiated per meeting by the Data Controller. Raw media should not be retained longer than the Data Controller's own policy requires.

(i) Internet search and enrichment. Where an agent performs a web search, or the Data Controller enriches a company or contact record, the search query is sent to Perplexity AI, Inc. in the United States. Queries may contain names, company names and email domains. Invoked by the Data Controller or by an agent it has configured.

(j) Email, calendar and transactional mail. Synchronized mail and calendar data is stored in the Data Processor's Azure tenant; system emails are sent through Microsoft's Azure Communication Services. On first connection the Service reads up to 30 days of existing mail and a calendar window of one year back and two years forward, then follows new items.

(k) Transfers to the United States under the two sub-processors named above are made on the basis set out in clause 4.7. All other processing described in this clause takes place within the Data Processor's Microsoft Azure tenant.

7.4. Processing includes the following categories of data subject:

(a) Employees of the Data Controller, and any other persons — such as contacts at the Data Controller’s suppliers, customers or other organizations — whose personal data the Data Controller tracks in the Service

7.5. The Data Processor’s processing of personal data on behalf of the Data Controller may be performed from the Effective Date. Processing will happen for the duration of this Agreement.

7.6. Processing of personal data cannot be performed at other locations than the Data Processor’s and sub-processors’ facilities.