Data Processing Agreement

This **Data Processing Agreement** (**DPA**) applies to the signed Pigion.AI B.V. (located at Vondellaan 4, 6881 MC Velp, the Netherlands) (**Company**) and the **Customer** (as defined in the Order Form). The Company and the Customer are the **Parties** and each a **Party**.

WHEREAS:

(A) The Company offers an AI-driven software tool that automates email management, meeting preparation, and workflow organization (the **Platform**). In addition to access to the Platform, Company may provide additional services, including any customization of functionalities or Platform offering (access to the Platform and any additional services offered to Customer, **Services**).

(B) Customer has retained the Services of Company under the agreement entered into prior to or on the date of this DPA (the **Agreement**).

(C) In doing so, Company will be Processing Personal Data on behalf of Customer, whereby Company will be acting as Data Processor (where Customer is the Data Controller) or Sub-processor (where Customer is a Data Processor acting on behalf of a Data Controller) and Customer will be acting as Data Controller or Data Processor (as applicable).

(D) The Parties seek to implement this DPA to comply with the requirements of the GDPR.

(E) This DPA will be supplemental to the Agreement between the Parties, and this DPA will follow the terms thereof and definitions therein.

THEREFORE IT IS HEREBY AGREED as follows:

1 DEFINITIONS

1.1 In addition to the definitions used in the Agreement, unless the context requires otherwise, capitalized terms and expressions have the meanings set out in this Clause:

(i) **Agreement:** means the agreement between Company and Customer relating to Company's Services, entered into on the Effective Date as defined in the Agreement.

(ii) **Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to transmitted, stored, or otherwise processed Personal Data.

(iii) **Data Controller:** a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or Member State law, the data controller or the specific criteria for its nomination may be provided for by Union or Member State law. For the purposes of this DPA, references to Data Controller shall, where Customer acts as a Data Processor, be deemed to include the ultimate Data Controller on whose behalf Customer is Processing Personal Data.

(iv) **Data Processing Agreement** or **DPA:** this agreement including its appendices.

(v) **Data Processor:** a natural or legal person, public authority, agency, or other body that Processes Personal Data on behalf of the Data Controller.

(vi) **Data Subject:** an identified or identifiable natural person to whom the processed Personal Data relates.

(vii) **GDPR:** Regulation (EU) 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).

(viii) **Personal Data:** any information relating to an identified or identifiable natural person (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.

(ix) **Process, Processes, Processed or Processing:** any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data.

(x) **Processing Purposes:** the purposes for which Personal Data are processed, as described in **Annex A**.

(xi) **Services:** has the meaning given to it in the Agreement.

(xii) **Sub-processors:** those who process (part of) the Personal Data on behalf of the Company.

(xiii) **Supervisory Authority:** an independent public authority responsible for monitoring compliance with the law in relation to the Processing of Personal Data. In the Netherlands, this is the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*).

2 SCOPE

During the term of the Agreement, Company will process Personal Data on behalf of Customer and in accordance with applicable laws and regulations. The relevant Personal Data Processed under this DPA are described in Annex A. Company Processes the Personal Data as Data Processor solely for the specified purpose or purposes of the Processing (the Processing Purposes), as described in Annex A, and for as long as necessary to provide the Services to Customer, unless further written instructions are provided by Customer. Where Customer acts as a Data Processor on behalf of a Data Controller, Customer warrants that all instructions provided to Company are consistent with the instructions received from the relevant Data Controller and that Customer has obtained all necessary authorizations to engage Company as a Sub-processor.

3 NATURE OF PROCESSING

3.1 Company Processes the Personal Data solely on behalf of Customer and based on Customer's documented instructions. Company Processes the Personal Data only to the extent necessary for the performance of the Agreement and for the Processing Purposes set out in Annex A and in accordance with the documented instructions of Customer. Customer may reasonably provide additional or different instructions in writing. Company will follow all instructions from Customer regarding the Processing of Personal Data. The nature of the Processing includes the collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, alignment, and erasure of Personal Data as necessary to provide the Services. Company will immediately notify Customer if, in its opinion, an instruction is in violation of applicable laws and regulations concerning the Processing of Personal Data. Where Customer acts as a Data Processor, Customer shall ensure that all instructions provided to Company derive from and comply with the documented instructions of the ultimate Data Controller.

3.2 Without prejudice to any other contractual confidentiality obligation binding on Company, Company guarantees that all Personal Data will be treated as strictly confidential. In this regard, Company will inform all its employees, representatives, and subcontractors (Sub-processors, see Clause 7) involved in this Processing of this confidentiality requirement and ensure that they will act accordingly.

4 SECURITY OF PERSONAL DATA

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk and severity for the rights and freedoms of natural persons, Company shall implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. An overview of the security measures at the Effective Date is included in **Annex B**. By signing this DPA, Customer agrees that these measures are appropriate. Notwithstanding the foregoing, Company does not warrant that security measures will be effective under all conditions. In the event of a threat of or an actual Data Breach, Company shall take all reasonable steps to mitigate the impact on Personal Data.

4.2 In assessing the appropriate level of security, Company shall take account of the risks that are presented by Processing, in particular from a Data Breach.

4.3 Company will monitor security breaches and maintain a record of any security incidents.

4.4 In the event of a Data Breach, whether actual or reasonably suspected, Company will notify Customer without undue delay and in any event within forty-eight (48) hours after Company becomes aware of the breach. The notification will include all relevant information available at that time regarding the nature of the incident, the affected Personal Data, and any measures taken or to be taken to mitigate the consequences. Company's obligation to report applies regardless of the impact of the breach. Where Customer acts as a Data Processor, Customer shall be responsible for notifying the relevant Data Controller in accordance with Customer's obligations to such Data Controller.

4.5 Company shall promptly investigate any Data Breach, determine an appropriate response, and take necessary measures, including potentially informing the Supervisory Authority and

the Data Subjects. Notwithstanding the foregoing, Customer will always remain responsible for the analysis of a Data Breach and notification to the Supervisory Authority, if necessary.

5 AUDIT

5.1 Customer has the right to have audits conducted by an independent expert third party bound by confidentiality to verify compliance with this DPA. Prior to initiating an on-site audit, Customer shall first request and review any available audit reports, certifications, or compliance documentation from Company (such as SOC 2 reports, penetration test summaries, or ISO certifications). If such documentation does not adequately address Customer's compliance concerns, Customer may conduct an audit subject to reasonable advance notice of at least two (2) weeks.

5.2 Such an audit is justified if Company's similar audit reports do not, or insufficiently, provide a definite answer to Company's compliance with this DPA. The audit initiated by Customer will take place at least two (2) weeks after prior announcement by Customer. Company will cooperate with the audit and will make all information reasonably relevant to the audit, including supporting data, such as system logs, and employees, available as soon as possible and within a reasonable period of time, whereby a period of a maximum of two (2) weeks is reasonably available. The findings of the audit carried out will be assessed by the Parties in mutual consultation and, as a result, whether or not they will be implemented by one of the Parties or by both Parties jointly. The costs of the audit will be borne by Customer. Where Customer acts as a Data Processor, audit rights under this Clause may be exercised by or on behalf of the ultimate Data Controller, subject to reasonable confidentiality undertakings and the prior written consent of Customer.

6 DATA TRANSFERS

Company may process the Personal Data in countries within and outside the European Economic Area, provided that the requirements of Chapter V of the GDPR are met. Customer hereby authorizes Company, where necessary, to enter into standard contractual clauses with a Sub-processor in a third country in accordance with applicable EU Commission decisions. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of Personal Data. Upon Customer's request, Company shall provide a copy of any such standard contractual clauses entered into with Sub-processors. Company will notify Customer prior to processing outside the EEA to which third country or countries the Personal Data will be transferred, unless prohibited by law.

7 SUB-PROCESSORS

7.1 Company engages Sub-processors to perform the Services. At the Effective Date, Company has engaged the Sub-processors listed in Annex A.

7.2 Customer consents to Company's use of its existing Sub-processors and grants Company a general written authorization to engage Sub-processors as necessary to perform the Services. Company will notify Customer in writing if Company intends to add one or more Sub-processors to that list at least fourteen (14) days before the changes take effect. Customer is entitled to object in writing on reasonable grounds to a specific new, or changing of, Sub-processor(s) within fourteen (14) days after Company has sent the notification. If Customer fails to object within this timeframe, Customer will have deemed to have agreed. If Customer makes an objection, Parties will consult to reach a solution. If, regardless of Customer's

objection, Company engages the intended Sub-processor, Customer has the right to terminate this DPA and the Agreement with a termination notice of fourteen (14) days.

7.3 Company confirms that each Sub-processor shall be held to the same conditions as outlined in this DPA.

8 DATA SUBJECT RIGHTS

In the event that a Data Subject wishes to exercise one of his or her legal rights under Chapter III of the GDPR and directs his or her request to Company, Company will forward this request to Customer. Customer will handle the request further. Company may inform the relevant Data Subject about this. In the event that a Data Subject makes a request to exercise any of his or her legal rights to Customer, Company will cooperate so that Customer can meet the request. Company may charge a reasonable fee to Customer for this. Where Customer acts as a Data Processor, Customer shall coordinate with the relevant Data Controller to handle such requests in accordance with the Data Controller's instructions and applicable law.

9 CONFIDENTIALITY

9.1 Company shall keep the Personal Data strictly confidential, whereby it shall exercise at least the same degree of care as that which it observes with respect to protecting its own confidential information.

9.2 Company may disclose, distribute, provide, or otherwise disclose the Personal Data to its employees who need to know the Personal Data in order to perform their work as Company's employee, provided such employees are only allowed access to the Personal Data after they have been informed of the confidential nature of the Personal Data. Company shall also impose the provisions of this DPA on its employees.

9.3 Company shall not share with or make Personal Data available to a third party except pursuant to an express written order of Customer or upon the order of a governmental authority, provided that in such case, provided Company is allowed to do so, Company shall notify Customer as soon as possible of receipt.

9.4 If Company is of the opinion that it must make Personal Data available to a competent governmental authority pursuant to a legal obligation, it will only do so after consultation with and obtaining the approval of the Customer, provided Company is allowed to do so. Company will notify Customer in writing of such legal obligation as soon as possible, providing all relevant information Customer reasonably needs to take the necessary measures to determine whether disclosure can take place and, if so, under what conditions.

10 LIABILITY

10.1 Where Customer acts as a Data Processor on behalf of a Data Controller, Customer shall remain liable to the Data Controller for Company's performance of its obligations under this DPA, and Company shall remain liable to Customer for its own acts and omissions in the performance of the Services.

The Parties explicitly agree that regarding liability, the provisions as laid down in the Agreement apply.

11 TERM AND RETENTION

11.1 The term of the DPA shall be the same as the duration of the Agreement and begins upon signing. This DPA cannot be terminated independently from the Agreement. This DPA shall terminate automatically upon the termination of the Agreement. Obligations from the DPA that, by their nature, are intended to continue after the termination of the DPA, shall continue to apply after the termination of the DPA.

11.2 Upon termination of the Agreement, or earlier upon Customer's written request, Company shall return all copies of Personal Data in its possession to Customer or, at the discretion of Customer, delete them. Upon request, Company shall provide Customer with a written confirmation of this.

11.3 Customer is responsible for determining and notifying Company of the appropriate retention periods for each category of Personal Data, and for ensuring that the retention periods comply with the principles of data minimization and data subject rights under the GDPR.

11.4 In the event that personal data must be retained for legal or regulatory reasons beyond the purpose of this Agreement, Customer shall provide the Company with written instructions, and Company shall continue to protect the Personal Data in accordance with the terms of this DPA during the retention period.

12 APPLICABLE LAW AND DISPUTE RESOLUTION

12.1 This DPA and any action in relation thereto shall be governed by the laws of the Netherlands. The competent court of Amsterdam, the Netherlands, shall have exclusive jurisdiction in relation to any actions regarding this DPA, and any other aspects of Customer’s relationship with Company.

13 MISCELLANEOUS

13.1 This DPA is an integral part of the Agreement. Accordingly, the terms and conditions of the Agreement shall apply to this DPA to the extent not inconsistent herewith.

13.2 Deviations from this DPA are only valid if agreed upon in writing by the Parties.

13.3 Customer acknowledges and agrees that the instruction to process Personal Data on behalf of Customer by Company when providing the Services, includes the anonymizing and/or aggregating Customer Personal Data in such a way that such data does not identify any natural person. Company may use such anonymized and aggregated data in accordance with the Agreement.

ANNEX A – PROCESSING OF PERSONAL DATA

Processing

The table below provides a comprehensive overview of the Personal Data that will be Processed. This facilitates the ability to demonstrate where, by whom, and for what purpose the Personal Data will be Processed.

Purposes of Processing	Personal Data shared with Company by the Customer in light of or through the Services. This Personal Data is Processed by Company (collected, organized, structured, analyzed, stored and used) for the following purposes: • to provide the Services, including email management, meeting preparation, and workflow organization; • for troubleshooting; • for analysis to enhance and improve the Services, monitor the usage of the Services, and gain insights into user behaviors, preferences, and trends; • to send communications; and • other purposes directly related to the provision of the Services.
Categories of Data Subjects	Platform users and authorized recipients.
Categories of Personal Data	• Name and e-mail address of users logging on to the Platform; email content and metadata processed through the Platform; calendar and meeting data; and workflow-related information. Usernames may be anonymized by the user.
Legal basis of Processing	Processing is necessary for the performance of a contract between Company and Customer.

Sub-processors

The Sub-processors engaged by the Company are:

Sub-processor engaged by the Processor for the Processing of Personal Data	Purpose	Categories of Personal data processed by Sub-processor	Type of Processing	Country of Processing	Country of establishment of the Sub-processor	Comments
Supabase, Inc.	Database and backend infrastructure services	User account data, email content and metadata, calendar and meeting data, workflow-related information	Storage, retrieval, organization, transmission	EU	United States	Servers located in the EU
Pinecone Systems, Inc.	Vector database services for AI functionality	Email content embeddings, workflow data embeddings	Storage, retrieval, analysis	EU	United States	Servers located in the EU
PostHog, Inc.	Product analytics and monitoring	Usage data, user identifiers, interaction data	Collection, analysis, storage	EU	United States	Servers located in the EU
Microsoft Corporation	Large Language Model (LLM) services	Email content, calendar data, workflow information processed for AI features	Processing, analysis, generation	EU	United States	Servers located in the EU

Vercel, Inc.	Hosting and deployment services	User identifiers, access logs	Storage, transmission	EU	United States	Servers located in the EU
Stripe, Inc.	Payment processing services	Payment details, billing information, user identifiers	Collection, storage, transmission	EU	United States	Servers located in the EU

Transfers outside the European Economic Area

Customer has given the Company specific permission for the following transfers to third countries or international organizations (to be completed by Customer).

Transfer Description	Entity transferring the Personal Data and the Country	Entity receiving the Personal Data and the Country	Transfer Mechanism	Additional safeguards implemented for transfers outside the EEA
Database and backend infrastructure services	Pigion.AI B.V.	Supabase, Inc.	Standard Contractual Clauses (Module Two and Module Three pursuant to Commission Implementing Decision (EU) 2021/914)	Encryption at rest (AES-256) and in transit (TLS 1.2), access controls based on Principle of Least Privilege, FIPS 140-2 compliant HSMs for key management
Vector database services for AI functionality	Pigion.AI B.V.	Pinecone Systems, Inc.	Standard Contractual Clauses (Module Two and Module Three pursuant to Commission Implementing Decision (EU) 2021/914)	Encryption (AES-256), PCI-DSS Level 1 compliance, SOC 1 and SOC 2 reports

			EU-US Data Privacy Framework	
Product analytics and monitoring	Pigion.AI B.V.	PostHog, Inc.	Standard Contractual Clauses (pursuant to Commission Implementing Decision (EU) 2021/914)	As set forth in PostHog DPA available at https://posthog.com/dpa
Large Language Model (LLM) services	Pigion.AI B.V.	Microsoft Corporation	Standard Contractual Clauses (Module Two and Module Three pursuant to Commission Implementing Decision (EU) 2021/914) EU-US Data Privacy Framework	Encryption at rest and in transit, ISO 27001/27002/27018 compliance, SOC audits, additional safeguards pursuant to Annex C of Microsoft DPA
Hosting and deployment services	Pigion.AI B.V.	Vercel, Inc.	Standard Contractual Clauses (pursuant to Commission Implementing Decision (EU) 2021/914)	As set forth in Vercel DPA available at https://vercel.com/legal/dpa
Payment processing services	Pigion.AI B.V.	Stripe, Inc.	Standard Contractual Clauses (EEA SCCs Module 1 and Module 2); UK International Data Transfer Addendum; EU-US Data Privacy Framework	| Encryption (AES-256, TLS 1.2), PCI-DSS Level 1 compliance, SOC 1 and SOC 2 reports

Contact information

General contact information	Name	Job title	E-mail address	Telephone number
Customer				
Company	J.H. Schram	CEO	security@pigion.ai	+31 6 28 30 69 46

Contact information in the event of a Personal Data Breach	Name	Job title	E-mail address	Telephone number
Customer				
Company	J.H. Schram	CEO	security@pigion.ai	+31 6 28 30 69 46

ANNEX B – SECURITY MEASURES

Version No 1.0, Date of latest amendment:

Details of the security measures taken by Company:

Measure	Description
Encryption	AES-256 encryption for data at rest (databases, backups, object storage). TLS 1.2+ for data in transit. Managed Key Management Service (KMS) with periodic key rotation.
Tenant Isolation	Row Level Security (RLS) in the database and a dedicated namespace per customer in the vector database. Automated tests verify cross-tenant data isolation at each deployment.
Access control and identity management	Multi-factor authentication (MFA) is mandatory for all internal and privileged accounts. Least privilege is enforced; access rights are periodically reviewed.
Confidentiality	All employees with access to systems or infrastructure have signed confidentiality agreements. Employees have no standard access to Customer Content (email content or attachments).
Secure development lifecycle	Mandatory code reviews, automated dependency scanning, secret scanning, and static application security testing (SAST). Periodic external penetration tests. Patch SLAs established per severity level (critical, high, medium, low).
Logging, monitoring and incident response	Centralized security monitoring with alerting on suspicious access and data exfiltration attempts. Formal incident response procedures with documented escalation paths. Audit logs retained for 2 years.
Backup and recovery	Backups encrypted with AES-256 and stored exclusively in EU data

Data retention and deletion	Operational data (embeddings, metadata, caches) retained for the duration of the Service. All Customer data deleted within 30 days of termination, including at Sub-processors. OAuth tokens revoked immediately upon termination. Written deletion confirmation provided to Customer. Invoice data retained for 7 years per Dutch fiscal requirements. System logs (containing no Customer Content) retained for a maximum of 2 years.
Internal Policies	Clean desk policy. Laptops and mobile devices secured and never left unattended.