SYNERGIST

DATA PROCESSING AGREEMENT

1. INFORMATION ABOUT THIS DPA

1.1 This data processing agreement ("**DPA**") forms part of the Agreement between the Supplier and the Customer and sets out the terms that apply to the processing of Personal Data in connection with the provision and receipt of the Services.

1.2 Capitalised terms used but not defined in this DPA shall have the meaning given to them in the Order Form, the General Terms and Conditions or the Service Specific Terms (as applicable).

2. DEFINITIONS AND INTERPRETATION

2.1 The following terms shall have the following meanings unless the context requires otherwise:

Term	Meaning
"Agreement"	has the meaning given to it in the Order Form.
"Controller"	has the meaning given to it by GDPR.
"Data Protection Laws"	means, in relation to any Personal Data which is Processed in the performance of this Agreement: (i) in respect of the United Kingdom, the Data Protection Act 2018, the UK GDPR and the Data (Use and Access) Act 2025; and (ii) in respect of the European Economic Area, the EU GDPR, the Directive on Privacy and Electronic Communications 2002/58 and other data protection or privacy legislation in force from time to time in the European Economic Area, in each case together with any national implementing laws, regulations, secondary legislation and any other applicable or equivalent data protection or privacy laws, as amended or updated from time to time, and any successor legislation to such laws.
"Data Subject"	has the meaning given to it by GDPR.
"GDPR"	means the UK GDPR and/or the EU GDPR, in each case as applicable, where: (a) "UK GDPR" means Regulation (EU) 2016/679 General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019; and (b) "EU GDPR" means Regulation (EU) 2016/679 General Data Protection Regulation as applicable in the European Economic Area, together with any applicable national data protection legislation of the relevant EEA member state.
"Personal Data"	has the meaning given to it by GDPR, and except for the caveat at Clause 4, relates only to personal data, or any part of such personal data, of which the Customer is the Controller and in relation to which the Supplier is the Processor in providing the Services under this Agreement.
"Personal Data Breach"	has the meaning given to it by GDPR.
"Process" and **"Processing"**	have the meaning given to them by GDPR.
"Processor"	has the meaning given to it by GDPR.
"Supervisory Authority"	means any regulatory authority responsible for the enforcement of Data Protection Laws, which shall at least include, in respect of the UK, the UK Information Commissioner's Office and, in respect of the EEA, the relevant competent supervisory authority of the applicable member state.

2.2 In this DPA, references to "**Clauses**" are to clauses of this DPA. The rules of interpretation set out in the General Terms and Conditions apply to this DPA.

3. ROLES OF THE PARTIES

3.1 The Parties acknowledge that, to the extent the Supplier is acting as a Controller in relation to Personal Data as set out in Clause 4, the Supplier acts as a separate and independent Controller from the Customer.

3.2 Except as in the limited circumstances provided for in Clause 4, the Parties acknowledge that:

3.2.1 for the purposes of Data Protection Laws, the Customer is the Controller and the Supplier is the Processor of any Personal Data; and

3.2.2 the Personal Data shall be in respect of data shared by necessity by the Customer with the Supplier for the provision and receipt of the Services only.

4. SUPPLIER ACTING AS CONTROLLER

4.1 To the extent the Supplier is acting as Controller, the Supplier shall:

4.1.1 comply with Data Protection Laws when Processing Personal Data;

4.1.2 only Process Personal Data:

4.1.2.1 in order to perform the Supplier's obligations under this Agreement; and

4.1.2.2 solely to the extent permitted by Applicable Laws to the extent necessary for the following purposes as Controller:

4.1.2.2.1 maintaining and developing the Supplier's relationship with the Customer;

4.1.2.2.2 billing and invoicing;

4.1.2.2.3 compliance with quality control and risk management procedures;

4.1.2.2.4 IT security-related processing (for example, automated scanning of incoming and outgoing emails for viruses);

4.1.2.2.5 complying with legal and regulatory obligations;

4.1.2.2.6 establishing, exercising and defending legal claims; and

4.1.2.2.7 creating Aggregated Data in accordance with Clause 10 of the General Terms and Conditions, to the extent the Supplier determines the purposes and means of such Processing;

4.1.3 notify the Customer as soon as reasonably practicable upon becoming aware of a Personal Data Breach affecting Personal Data; and

4.1.4 comply with Data Protection Laws in relation to any transfers of Personal Data under GDPR that would otherwise be prohibited but for the implementation of appropriate safeguards in accordance with Article 46 GDPR.

5. PROCESSING DETAILS AND INSTRUCTIONS

5.1 The scope, nature and purpose of the Processing, which constitutes the Customer's Processing instruction as Controller to the Supplier as Processor, is set out in Annex A.

5.2 The Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. The Supplier shall inform the Customer immediately if, in the Supplier's opinion, an instruction from the Customer violates Data Protection Laws.

5.3 Each Party confirms that, in the performance of this Agreement, it shall comply with Data Protection Laws.

6. SUPPLIER OBLIGATIONS AS PROCESSOR

The Supplier shall:

6.1 Process Personal Data only on documented instructions from the Customer, unless required to do so by Data Protection Laws or any other Applicable Law to which the Supplier is subject; in such a case, the Supplier shall inform the Customer of that legal requirement before Processing, unless that Applicable Law prohibits the Supplier from informing the Customer;

6.2 ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

6.3 ensure that the Supplier has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful

processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of the Supplier's systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by the Supplier);

6.4 be generally authorised to engage another Processor to Process Personal Data ("**Subprocessor**"), subject to the Supplier:

6.4.1 making available to the Customer a list of Subprocessors authorised to Process Personal Data ("**Subprocessor List**"), the initial Subprocessor List as at the date of this DPA being set out in Annex A;

6.4.2 notifying the Customer of any intended changes to its use of Subprocessors by providing the Customer with notice of any updates to the Subprocessor List, which the Supplier shall provide to the Customer at least 30 calendar days prior to authorising any new Subprocessor;

6.4.3 including terms in its contract with each Subprocessor which are no less protective than those set out in this Agreement;

6.4.4 remaining liable to the Customer for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of the Customer's Personal Data.

6.5 allow the Customer, in relation to any notice received under Clause 6.4.2, a period of 14 calendar days from the date of the notice to register any reasonable objection to the use of that Subprocessor. Where any objection is registered, the following shall apply:

6.5.1 the Parties shall meet as soon as possible to discuss the reasons for the objection, whereby the Customer shall provide the Supplier with all details of the concerns which led to the objection;

6.5.2 if the Customer does not withdraw the Customer's objection within 1 month from the date on which the Customer made the Customer's objection, the Supplier will use reasonable efforts to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening the Customer;

6.5.3 if the Supplier is unable to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor as per Clause 6.5.2 above, or if the Customer does not accept the proposed changes or recommendations, the Supplier shall be entitled to proceed with appointing that Subprocessor in accordance with Clause 6.5.4; and

6.5.4 the Supplier shall notify the Customer before appointing that Subprocessor, and the Customer may terminate the Agreement by providing written notice within 30 days from receipt of the Supplier's notice under this Clause 6.5.4. The Supplier shall not appoint that Subprocessor to Process the Customer's Personal Data until the expiry of that 30-day period or, if earlier, the date on which the Customer confirms that it does not wish to terminate, and shall refund any Fees paid in advance for any period after the date of termination.

6.6 taking into account the nature of the Supplier's Processing, assist the Customer by putting in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in Data Protection Laws, to the extent that such requests relate to Personal Data Processed in connection with this Agreement;

6.7 notwithstanding Clause 6.6 above, the Supplier shall direct:

6.7.1 all individual Data Subject requests, complaints or other communications (whether from the Data Subject or on their behalf); and

6.7.2 any requests, correspondence or communications from a Supervisory Authority,

in each case to the extent relating to Personal Data which the Supplier Processes on behalf of the Customer, to the Customer within 2 Business Days of receipt. The Supplier shall not engage with such Data Subject, requester or Supervisory Authority directly, except on the Customer's documented instructions or where required by Applicable Law;

6.8 assist the Customer, at the Customer's cost (save that the Supplier shall bear its own costs of any assistance with a Personal Data Breach to the extent the Personal Data Breach was caused by the

Supplier's or its Subprocessors' breach of this DPA), in responding to any request from a Data Subject and in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to Personal Data Breach notifications, data protection impact assessments and consultations with Supervisory Authorities;

6.9 in relation to the Customer's assessment of the Supplier's compliance with this DPA:

6.9.1 at the Customer's request, make available to the Customer all information necessary to demonstrate the Supplier's compliance with this DPA (which obligation may be satisfied by providing relevant certifications (such as ISO/IEC 27001 or equivalent), third party audit reports or other appropriate documentation);

6.9.2 to the extent that information obtained pursuant to Clause 6.9.1 is insufficient for the Customer to verify the Supplier's compliance with this DPA and Data Protection Laws, the Customer shall be entitled to carry out an inspection of the technical and organisational measures taken by the Supplier as relevant to the Supplier's compliance with this DPA upon giving at least 30 calendar days prior notice, unless a shorter period is required (in particular in cases where a Supervisory Authority requires an inspection to be performed at shorter notice), provided that any inspection takes place during normal Business Hours and with no unreasonable disruption to the Supplier's business, is proportionate to the Services the Supplier provided to the Customer and the criticality or importance of such Services, adheres to commonly accepted national and international audit standards, is conducted no more than once in any calendar year (unless a Supervisory Authority requires otherwise), does not include access to systems, data or information relating to any other customer of the Supplier, and employees or third party auditors being subject to appropriate confidentiality obligations in relation to any audit and / or inspection, and the costs of any such audit or inspection being borne by the Customer;

6.9.3 where the Customer requires additional assistance or information beyond what is reasonably necessary to demonstrate the Supplier's compliance with this DPA, the Supplier may charge reasonable fees for providing such additional assistance or information on a time and materials basis;

6.10 notify the Customer promptly and without undue delay if the Supplier becomes aware of a Personal Data Breach relating to the Supplier's obligations under this Agreement, which notification shall include, where available:

6.10.1 a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned;

6.10.2 the likely consequences of the Personal Data Breach; and

6.10.3 the measures taken or proposed to be taken to address and mitigate the Personal Data Breach;

6.11 in relation to any such notification under Clause 6.10, take all reasonable measures to prevent any further negative impact of the Personal Data Breach. The Supplier shall provide assistance, and provide the Customer with sufficient information so that the Customer is able to meet any obligations to assess and report a Personal Data Breach under the Data Protection Laws, which may be provided in stages as it becomes available to the Supplier, including obtaining any information that needs to be included in a notification to the Supervisory Authority or impacted Data Subjects; and

6.12 not transfer any Personal Data outside of the United Kingdom and the European Economic Area unless the Customer's prior written consent has been obtained (such consent not being required in respect of transfers of Personal Data to Subprocessors appointed in accordance with Clause 6.4) and either (a) the transfer is to a country, territory or sector covered by adequacy regulations or an adequacy decision under Data Protection Laws; or (b) appropriate safeguards have been implemented in accordance with Article 46 GDPR, which safeguards may include the Standard Contractual Clauses approved by the European Commission or any other lawful transfer mechanism recognised under Data Protection Laws (and the Customer authorises the Supplier to enter into such transfer mechanisms with Subprocessors on the Customer's behalf where required).

7. CUSTOMER-ENABLED THIRD-PARTY SERVICES

7.1 The Services may enable the Customer to connect the Services to Third-Party Services, including through the Supplier's application programming interfaces, Model Context Protocol server, connectors and integrations. Whether any Third-Party Service is connected, and on what terms, is solely a matter for the Customer.

7.2 Where the Customer (or any User acting on the Customer's behalf) connects, enables or authorises a Third-Party Service, this constitutes the Customer's documented instruction to the Supplier to Process Personal Data as necessary to give effect to that connection. This includes making Personal Data available

to the Third-Party Service and receiving, storing and acting on data, requests and instructions from it, in each case in accordance with the permissions and configuration selected by the Customer.

7.3 Any request, instruction or action submitted to the Services through a Third-Party Service using credentials, tokens or authorisations issued to the Customer or its Users shall be treated as an instruction of the Customer. This applies whether the request, instruction or action is initiated by an individual or generated automatically by the Third-Party Service (including by an artificial intelligence system or agent), and whether or not it has been reviewed by an individual before submission.

7.4 The Parties acknowledge that each Third-Party Provider is engaged by the Customer and not by the Supplier. A Third-Party Provider is not a Subprocessor of the Supplier. Clauses 6.4, 6.5 and 6.12 shall not apply to any Processing by, or transfer of Personal Data to, a Third-Party Provider. As between the Parties, any Processing of Personal Data by a Third-Party Provider is governed solely by the arrangements between the Customer and that Third-Party Provider and not by this DPA.

7.5 The Customer shall be solely responsible for:

7.5.1 selecting, assessing and monitoring each Third-Party Service and Third-Party Provider, including its security and compliance with Data Protection Laws;

7.5.2 ensuring that appropriate contractual terms (including, where applicable, terms meeting the requirements of Article 28 UK GDPR) and any transfer mechanism required under Data Protection Laws are in place with each Third-Party Provider;

7.5.3 ensuring that it has a lawful basis for, and has provided any information to Data Subjects required by Data Protection Laws in respect of, the disclosure of Personal Data to any Third-Party Service, and carrying out any data protection impact assessment required in connection with its use;

7.5.4 configuring and maintaining the permissions, access scopes and settings applicable to each connection, including which Users may use it and whether it may create, modify or delete data within the Services;

7.5.5 keeping secure, and promptly revoking where appropriate, all credentials, tokens and authorisations used to connect any Third-Party Service; and

7.5.6 the accuracy of, and any use made of, any output generated by a Third-Party Service.

7.6 Subject to Clause 7.9, the Supplier's obligations under this DPA in respect of Personal Data made available to a Third-Party Service shall cease once that Personal Data has been transmitted to the Third-Party Service in accordance with the Customer's instructions. The Supplier shall have no responsibility or liability for any subsequent Processing, security, retention or deletion of that Personal Data by or on behalf of the Third-Party Provider, except to the extent caused by the Supplier's breach of this DPA, the Agreement or Applicable Law. The Supplier's obligations under Clause 8 do not extend to copies of Personal Data held by any Third-Party Provider.

7.7 Any unauthorised or unlawful Processing of Personal Data occurring within, or caused by, a Third-Party Service shall not constitute a failure by the Supplier to comply with this DPA. The same applies to any such Processing resulting from the use of credentials, tokens or authorisations issued to the Customer or its Users, except to the extent caused by the Supplier's breach of this DPA, the Agreement or Applicable Law. Where the Supplier becomes aware of any such incident, it shall inform the Customer without undue delay and provide such reasonable assistance as the Customer may request, at the Customer's cost.

7.8 The Supplier may suspend, restrict or revoke any connection to a Third-Party Service, or apply rate or usage limits, where the Supplier reasonably considers this necessary:

7.8.1 to protect the security, integrity or availability of the Services or any Personal Data;

7.8.2 to prevent any risk to the Supplier's other customers or systems;

7.8.3 where the Supplier considers that the resulting Processing would infringe Data Protection Laws; or

7.8.4 to comply with Applicable Law.

Where reasonably practicable, the Supplier shall give the Customer prior notice of any such action and Clause 15.6 of the Service Specific Terms shall apply to any such action.

7.9 Nothing in this Clause 7 affects the Supplier's obligations under this DPA in respect of:

7.9.1 the Supplier's own interfaces, APIs, servers and connectors (including its Model Context Protocol server) and any Processing carried out within the Supplier's systems before Personal Data is transmitted to a Third-Party Service; or

7.9.2 any third party engaged by the Supplier to provide any part of the Services (including any artificial intelligence or machine learning service used by the Supplier to deliver features of the Services), which shall be a Subprocessor subject to Clauses 6.4 and 6.5.

8. DATA RETURN AND DESTRUCTION

8.1 Upon termination or expiry of the Agreement, the Customer may, within 30 days, request the return or export of Personal Data Processed by the Supplier on the Customer's behalf. Following the expiry of that period, the Supplier shall delete or irreversibly anonymise all Personal Data, unless Applicable Law requires retention of such Personal Data.

8.2 Notwithstanding Clause 8.1, Personal Data may be retained in backups, archives or disaster recovery systems until such data is deleted in accordance with the Supplier's standard retention cycles. During this period, such Personal Data shall remain protected in accordance with this DPA and shall not be actively Processed.

8.3 Upon written request, the Supplier shall confirm that deletion has been completed in accordance with this Clause 8, to the extent technically feasible.

8.4 The Customer is responsible for ensuring that it has securely exported or otherwise retained any Personal Data it requires prior to deletion. The Supplier shall not be liable for any loss of Personal Data following deletion carried out in accordance with this Clause 8.

9. INDEMNITY

The Customer agrees to indemnify the Supplier, and keep the Supplier indemnified, and defend the Supplier at the Customer's own expense, against all costs, claims, damages or expenses incurred by the Supplier or for which the Supplier may become liable, due to any failure by the Customer or the Customer's employees or agents to comply with this DPA.

10. LIABILITY

Nothing in this DPA shall increase or extend either Party's liability beyond that set out in the Agreement.

ANNEX A

Personal Data processing purposes and details

Subject matter of Processing	Processing of Personal Data as necessary for the Supplier to provide the Services under the Agreement.
Duration of Processing	For the duration of the Agreement and any applicable retention period in accordance with Clause 8.
Nature of Processing	Processing activities may include collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, transmission, restriction, deletion or destruction of Personal Data.
Purpose of Processing	Provision and operation of the Services, including: (a) hosting and storage of Personal Data; (b) processing of Customer Data; (c) implementation, configuration and data migration; (d) training and onboarding support; (e) support, maintenance and troubleshooting; (f) security monitoring and fraud prevention; (g) analytics and performance monitoring (in aggregated and anonymised form where possible); (h) creation of Aggregated Data (as defined in the General Terms and Conditions) as permitted by the Agreement (including anonymisation of Personal Data for that purpose, on the Customer's instruction under Clause 10 of the General Terms and Conditions); and (i) making Personal Data available to, and receiving data, requests and instructions from, Third-Party Services connected or enabled by the Customer.
Personal Data Categories	Depending on the Customer's use of the Services, Personal Data may include: (a) names, business contact details and job titles; (b) account, user permission and authentication information; (c) IP address, device and log data; (d) project, time-recording, resourcing and workflow information; (e) employee and contractor details used for configuration or migration; (f) charge-out rates, cost rates and related financial or remuneration-related information; and (g) any Personal Data contained in Customer Data, migration files, support tickets, screenshots or training materials.
Data Subject Types	(a) the Customer's employees, workers and contractors; (b) Users and customer contacts; (c) the Customer's clients, suppliers and other business contacts where their data is included in Customer Data; and (d) any other individuals whose Personal Data is included in Customer Data, migration files or support materials.

Approved Subprocessors

Name of Subprocessor	Processing activities	Location	Safeguard mechanism

Amazon Web Services EMEA SARL	Cloud hosting and infrastructure for the Subscription Services, including storage, AI functionality & email notifications.	UK / EEA	Data hosted in UK/EEA
Microsoft Ireland Operations Limited	Business communications and collaboration, including email, document storage and sharing.	UK / EEA	EU SCCs and UK international data transfer safeguards incorporated into the Microsoft DPA
Zendesk, Inc.	Customer support ticketing, chat, AI functionality and related support content	EEA / US	EU-US Data Privacy Framework and UK Extension; Binding Corporate Rules (EU and UK); SCCs and UK Addendum

Third-Party Providers of services connected by the Customer are not Subprocessors (as per Clause 7).