grath.

Data Protection Addendum

Grath Consultancy Group Limited

Processor terms issued under UK Data Protection Laws, including the UK GDPR, the Data Protection Act 2018.

This Data Protection Addendum ("DPA") is entered into between Grath Consultancy Group Limited, a company registered in England and Wales (company number 12072526), whose registered office is at 77 Coleman Street, London, EC2R 5BJ ("GCG"); and the entity identified as Customer in the applicable Master Services Agreement or Order Form ("Customer").

This DPA supplements and forms part of the Master Services Agreement ("Agreement") between GCG and Customer. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in respect of the processing of Personal Data. All capitalised terms not defined herein shall have the meaning given to them in the Agreement.

By executing an Order Form that references the Agreement, or by using the Services, Customer agrees to the terms of this DPA on behalf of itself and any Authorised Affiliates.

1. Definitions

In this DPA, the following terms shall have the meanings set out below:

"Authorised Affiliate" means any Affiliate of Customer that (a) is subject to Data Protection Laws, and (b) is permitted to use the Services pursuant to the Agreement, but has not signed its own Order Form with GCG.

"Controller" means has the meaning given under Data Protection Laws.

"Customer Personal Data" means any Personal Data that GCG processes as Processor on behalf of Customer in connection with the Services.

"Data Protection Laws" means all applicable legislation relating to data protection, privacy, and the processing of Personal Data in force from time to time, including the UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003, each as amended or re-enacted.

"Data Subject" means has the meaning given under Data Protection Laws.

"DPA" means this Data Protection Addendum, including all Schedules.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.

"Processor" means has the meaning given under Data Protection Laws.

"Processing" means has the meaning given under Data Protection Laws, and "Process" and "Processed" shall be construed accordingly.

"Restricted Transfer" means a transfer of Customer Personal Data from the United Kingdom to a country or territory not subject to an adequacy decision under UK Data Protection Laws.

"Services" means the services provided by GCG to Customer under the Agreement.

"Special Category Data" means has the meaning given under Data Protection Laws, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data, health data, and data concerning sexual life or sexual orientation.

"Sub-Processor" means any third party engaged by GCG to Process Customer Personal Data on GCG's behalf in connection with the Services.

"Supervisory Authority" means the Information Commissioner's Office ("ICO"), or any successor body exercising equivalent functions in the United Kingdom.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the ICO under section 119A of the Data Protection Act 2018, as updated from time to time.

"UK GDPR" means the retained EU law version of the General Data Protection Regulation (EU) 2016/679, 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.

2. Roles of the Parties

2.1 The parties acknowledge that, for the purposes of Data Protection Laws and in relation to the Customer Personal Data, Customer acts as the Controller and GCG acts as the Processor.

2.2 Customer is solely responsible for: (a) determining the lawful basis for the Processing of Customer Personal Data; (b) ensuring that Customer Personal Data provided to GCG is accurate and that its collection and transfer to GCG complies with Data Protection Laws; (c) responding to requests from Data Subjects exercising their rights, save where GCG is required to provide assistance under clause 8; and (d) maintaining all required records and notices in connection with Customer's use of the Services.

2.3 GCG shall Process Customer Personal Data only on the documented instructions of Customer as set out in this DPA, the Agreement, and any applicable Order Form, unless Processing is required by applicable law, in which case GCG shall (to the extent permitted by law) inform Customer of that legal requirement before Processing.

2.4 Nothing in this DPA shall prevent GCG from Processing Personal Data for its own purposes as a Controller where GCG is independently required or entitled to do so under applicable law (for example, for compliance, regulatory, or fraud prevention purposes). Any such Processing shall be carried out in accordance with GCG's own privacy notice.

3. Scope and Purpose of Processing

3.1 GCG shall Process Customer Personal Data only to the extent necessary for: (a) the delivery, maintenance, and support of the Services under the Agreement; and (b) compliance with applicable law.

3.2 The subject matter, duration, nature, and purpose of the Processing, the types of Customer Personal Data, and the categories of Data Subjects are set out in Schedule 1 (Processing Details).

3.3 Customer acknowledges that the reconciliation and financial data processing functionality of the Services may involve transactional records that contain limited identifying information (such as company or personal names appearing in transaction references). Customer shall ensure that any Customer Personal Data submitted to the Services is limited to what is necessary for the purpose of receiving the Services, and shall not submit Special Category Data to the Services unless expressly agreed in writing by GCG.

3.4 GCG does not require or intend to Process Personal Data relating to Customer's end-clients as part of standard service delivery unless explicitly agreed in writing by both parties. Customer shall not provide such Personal Data unless it is necessary for the Services and has been agreed between the parties in writing.

4. GCG's Obligations as Processor

4.1 GCG shall:

- Process Customer Personal Data only in accordance with Customer's documented instructions and this DPA;
- ensure that persons authorised to Process the Customer Personal Data are subject to appropriate obligations of confidentiality;
- implement and maintain the technical and organisational measures described in clause 5 (Security);
- assist Customer in complying with its obligations in respect of Data Subject rights as set out in clause 8;

- assist Customer, taking into account the nature of the Processing and the information available to GCG, in ensuring compliance with Customer's obligations under Data Protection Laws relating to security of Processing, notification of Personal Data Breaches, data protection impact assessments, and prior consultation with the Supervisory Authority;
- upon termination or expiry of the Agreement, return or delete Customer Personal Data in accordance with clause 12 (Retention and Deletion); and
- make available to Customer all information reasonably necessary to demonstrate compliance with this DPA, and cooperate with audits in accordance with clause 10.

4.2 GCG shall promptly inform Customer if, in GCG's reasonable opinion, any instruction from Customer infringes Data Protection Laws. GCG shall not be required to act on any instruction that GCG reasonably believes to be unlawful.

5. Security

5.1 GCG shall implement and maintain appropriate technical and organisational measures to protect Customer Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration, or disclosure, having regard to: (a) the state of the art; (b) the costs of implementation; (c) the nature, scope, context, and purposes of Processing; and (d) the risks to the rights and freedoms of Data Subjects.

5.2 GCG's technical and organisational measures include, at a minimum:

- logical access controls and role-based permissions applying the principle of least privilege;
- encryption of Customer Personal Data at rest and in transit using industry-standard protocols;
- multi-factor authentication for systems Processing Customer Personal Data;
- regular security monitoring, vulnerability scanning, and penetration testing;
- audit logging and anomaly detection;
- documented business continuity and disaster recovery procedures; and
- security awareness training for personnel with access to Customer Personal Data.

5.3 GCG currently holds ISO 27001 and SOC 2 certifications. GCG shall, upon written request, provide Customer with a copy of its then-current certification(s) or a summary of its audit report(s) as evidence of its security posture. GCG shall notify Customer without undue delay if any such certification is withdrawn or materially downgraded.

5.4 GCG shall ensure that only those personnel who need access to Customer Personal Data for the purpose of delivering the Services are granted such access, and that all such personnel are subject to appropriate confidentiality obligations.

5.5 Customer is responsible for implementing appropriate security measures in respect of its own systems, networks, and devices used to access the Services, including the management of User credentials and access controls on Customer's side.

6. Personal Data Breaches

6.1 GCG shall notify Customer without undue delay, and in any event within 72 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data.

6.2 Such notification shall include, to the extent then known:

- a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Personal Data records affected;
- the name and contact details of GCG's data protection contact point (dpo@grath.com);
- the likely consequences of the Personal Data Breach; and
- the measures taken or proposed to be taken by GCG to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

6.3 Where GCG cannot provide all information specified in clause 6.2 within the initial notification, GCG shall provide such information in phases as it becomes available, without undue further delay.

6.4 GCG shall provide reasonable assistance to Customer in complying with Customer's obligations to notify the Supervisory Authority and affected Data Subjects in accordance with Data Protection Laws.

6.5 GCG's notification of a Personal Data Breach under this clause shall not constitute an admission of fault or liability.

7. Sub-Processors

7.1 Customer provides general authorisation to GCG to engage Sub-Processors to Process Customer Personal Data in connection with the Services. GCG's current list of approved Sub-Processors is maintained as a separate document made available to Customer on request or via GCG's designated information portal ("Approved Sub-Processors List").

7.2 GCG shall give Customer no less than 30 days' prior written notice before adding or replacing any Sub-Processor that will Process Customer Personal Data. Such notice shall include the identity of the proposed Sub-Processor and the nature of the Processing.

7.3 Customer may object to any proposed addition or replacement of a Sub-Processor on reasonable data protection grounds by providing written notice to GCG within 14 days of receiving notification. Where Customer objects, the parties shall discuss the objection in good faith. If the parties are unable to resolve the objection within a further 14 days, either party may terminate the relevant Order Form(s) on 30 days' written notice, subject to the Agreement's termination provisions.

7.4 GCG shall ensure that each Sub-Processor is bound by data protection obligations no less protective than those set out in this DPA. Where a Sub-Processor fails to fulfil its obligations, GCG shall remain fully liable to Customer for the performance of the Sub-Processor's obligations under this DPA.

7.5 GCG's current Sub-Processors include, without limitation: Amazon Web Services (cloud infrastructure and data hosting); Okta (identity and access management); Auth0 (authentication services); and HelpScout (customer support platform). The Approved Sub-Processors List shall be updated to reflect any changes.

8. Data Subject Rights

8.1 As between the parties, Customer is responsible for responding to requests from Data Subjects exercising their rights under Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, and objection).

8.2 GCG shall promptly notify Customer (and in any event within 5 Business Days) upon receiving any request from a Data Subject purporting to exercise any right under Data Protection Laws in relation to Customer Personal Data. GCG shall not respond to any such request on Customer's behalf without Customer's prior written consent, save as required by applicable law.

8.3 GCG shall provide Customer with such reasonable technical and organisational assistance as Customer may reasonably require to fulfil its obligations to respond to Data Subject requests, taking into account the nature of the Processing. GCG may charge Customer for such assistance at its then-current standard professional services rates, where such assistance is disproportionate or involves significant operational effort.

9. Data Protection Impact Assessments and Prior Consultation

9.1 GCG shall provide reasonable assistance to Customer in carrying out any data protection impact assessment required by Data Protection Laws in connection with the Services, taking into account the nature of the Processing and the information available to GCG.

9.2 Where Customer is required under Data Protection Laws to consult with the Supervisory Authority prior to undertaking any Processing activity in connection with the Services, GCG shall provide reasonable cooperation and assistance to Customer in relation to such consultation.

10. Audit Rights and Records

10.1 GCG shall maintain complete and accurate records of all Processing activities carried out on behalf of Customer under this DPA and shall make such records available to Customer upon reasonable written request.

10.2 GCG shall, upon reasonable written request from Customer, provide information necessary to demonstrate its compliance with this DPA, which may be satisfied by providing:

- copies of applicable third-party audit reports or certifications (including ISO 27001 and SOC 2 reports);
- written responses to a data protection questionnaire submitted by Customer; or
- written assurances signed by GCG's data protection contact.

10.3 Where Customer (or its appointed representative) reasonably concludes, based on the information provided under clause 10.2, that an on-site or remote audit is necessary, GCG shall permit such an audit subject to the following conditions:

- Customer provides no less than 30 days' prior written notice of the proposed audit;
- audits are conducted no more than once per calendar year, except where required by a Supervisory Authority or following a confirmed Personal Data Breach;
- the scope of the audit is limited to GCG's Processing of Customer Personal Data under this DPA;
- the audit is conducted during GCG's normal business hours and in a manner that minimises disruption to GCG's operations; and

- the auditor is subject to appropriate confidentiality obligations and Customer shall bear all costs of the audit unless the audit reveals a material breach by GCG of this DPA.

10.4 Nothing in this clause shall limit GCG's obligation to cooperate with audits or inspections required by a Supervisory Authority to the extent required by applicable law.

11. International Data Transfers

11.1 GCG shall not make any Restricted Transfer of Customer Personal Data unless the transfer is made in compliance with Data Protection Laws, including by implementing one or more of the following safeguards:

- a UK adequacy decision confirming that the destination country provides an adequate level of protection;
- the UK Addendum to the EU Standard Contractual Clauses; or
- such other appropriate safeguard as is recognised under Data Protection Laws.

11.2 Where GCG relies on the UK Addendum for a Restricted Transfer, the terms of Schedule 2 (International Transfers) shall apply. The information required to complete the UK Addendum is set out in Schedule 2 and, where applicable, Schedule 1.

11.3 GCG shall maintain an up-to-date record of the countries to which Customer Personal Data may be transferred and shall inform Customer of any changes to the transfer arrangements upon request.

11.4 Customer acknowledges that GCG's use of Sub-Processors may involve transfers of Customer Personal Data to countries outside the United Kingdom and consents to such transfers provided GCG has implemented the appropriate safeguards referenced in clause 11.1 in relation to those Sub-Processors.

12. Retention and Deletion

12.1 GCG shall not retain Customer Personal Data for longer than is necessary for the purposes for which it is Processed.

12.2 Upon termination or expiry of the Agreement, or upon Customer's written request, GCG shall (at Customer's election): (a) return Customer Personal Data to Customer in a machine-readable format; or (b) securely delete or destroy Customer Personal Data and all copies thereof in GCG's possession or control.

12.3 GCG shall complete the return or deletion referred to in clause 12.2 within 45 days of the date of termination or expiry of the Agreement, or receipt of Customer's written request, whichever is earlier. Upon request, GCG shall provide written confirmation of such deletion or destruction.

12.4 Notwithstanding clauses 12.2 and 12.3, GCG may retain Customer Personal Data to the extent, and for the period, required by applicable law. Any such retained data shall remain subject to the obligations of this DPA.

12.5 GCG shall ensure that any Sub-Processors are subject to equivalent data retention and deletion obligations.

13. Liability

13.1 This DPA is subject to the liability provisions set out in the Agreement and does not expand the aggregate liability of either party beyond that set out therein, except where such limitation is not permitted under applicable law.

13.2 Nothing in this DPA shall: (a) expand the overall aggregate liability of either party beyond that set out in the Agreement; or (b) exclude or limit liability where such limitation is not permitted under applicable law, including in respect of wilful misconduct or deliberate breach of Data Protection Laws.

13.3 Each party's liability under this DPA forms part of, and is not in addition to, the aggregate liability cap set out in the Agreement. For the avoidance of doubt, liability arising from a breach of this DPA shall be subject to the same cap as liability under the Agreement generally.

13.4 Where both parties are responsible for damage caused by Processing in breach of Data Protection Laws, each party shall be liable only for that portion of the damage attributable to its own breach.

14. Term

14.1 This DPA shall come into force on the date the Agreement and shall continue in force for so long as GCG Processes Customer Personal Data under the Agreement.

14.2 Termination or expiry of this DPA shall not affect any accrued rights or obligations of the parties, nor shall it affect the obligations that by their nature survive termination, including clauses 12 (Retention and Deletion) and 13 (Liability).

15. General Provisions

15.1 **Governing Law.** This DPA and any non-contractual obligations arising in connection with it shall be governed by and construed in accordance with the laws of England and Wales. The parties submit to the exclusive jurisdiction of the courts of England and Wales.

15.2 **Order of Precedence.** In the event of any conflict between this DPA and the Agreement regarding the Processing of Customer Personal Data, this DPA shall prevail. In the event of any conflict between the main body of this DPA and any Schedule, the main body shall prevail unless the Schedule expressly provides otherwise.

15.3 **Entire Agreement.** This DPA, together with the Agreement and all Schedules, constitutes the entire agreement between the parties with respect to the Processing of Customer Personal Data and supersedes all prior agreements, understandings, and representations relating to that subject matter.

15.4 **Amendments.** No amendment to this DPA shall be effective unless made in writing and signed by authorised representatives of both parties. GCG reserves the right to update this DPA to reflect changes in Data Protection Laws or regulatory guidance, and shall provide Customer with no less than 30 days' written notice of any material amendment.

15.5 **Severability.** If any provision of this DPA is held to be invalid or unenforceable, that provision shall be modified to the minimum extent necessary to make it valid and enforceable. The remainder of the DPA shall continue in full force and effect.

15.6 **Notices.** Notices under this DPA shall be given in accordance with the notice provisions of the Agreement. Notices to GCG's data protection contact should be directed to dpo@grath.com.

15.7 Authorised Affiliates. Customer may extend the benefit of this DPA to its Authorised Affiliates. Customer shall remain responsible for ensuring that its Authorised Affiliates comply with the terms of this DPA and the Agreement, and shall be liable to GCG for any failure by an Authorised Affiliate to do so.

Schedule 1 – Processing Details

Parameter	Detail
Subject matter of processing	Provision of reconciliation, reporting, and data management services pursuant to the Agreement.
Duration of processing	For the term of the Agreement and any applicable retention period under clause 12.
Nature and purpose of processing	Collection, storage, retrieval, organisation, use, and deletion of Customer Personal Data as necessary to provide, support, and maintain the Services, including reconciliation of transactional financial records and associated reporting functionality.
Categories of Data Subjects	Customer personnel (employees, contractors, and authorised users); and, where applicable, individuals whose names or identifiers appear incidentally in transactional financial records submitted by Customer.
Categories of Personal Data	Identification data (name, email address, job title/role); business contact details; system access and usage data (login records, activity logs, access timestamps); and transactional financial records containing limited incidental identifying information (e.g., personal or company names appearing in transaction references). No Special Category Data is intended to be processed unless separately agreed in writing.
Special Category Data	Not processed unless required by applicable law or agreed in writing by both parties. Customer must not submit Special Category Data to the Services without prior written agreement from GCG.
Processing operations	Collection, recording, organisation, storage, retrieval, use, disclosure by transmission, and deletion.

Schedule 2 – International Transfers

This Schedule sets out the framework for Restricted Transfers of Customer Personal Data from the United Kingdom to third countries or territories not subject to a UK adequacy decision.

Part A – General

A.1 Where GCG makes any Restricted Transfer of Customer Personal Data, it shall implement the UK Addendum (incorporating the EU Standard Contractual Clauses (Module Two: Controller to Processor), as adjusted for UK law) as the primary transfer mechanism, unless an alternative adequate safeguard is in place.

A.2 For the purposes of the UK Addendum:

- the "Exporter" is Customer (as Controller);
- the "Importer" is GCG or the relevant Sub-Processor (as Processor);
- the subject matter, nature, purpose, and categories of data and Data Subjects are as set out in Schedule 1; and
- the technical and organisational measures are as described in clause 5 of this DPA.

A.3 The parties agree that Schedule 1 satisfies the requirements of Annex I and the technical and organisational measures described in clause 5 satisfy the requirements of Annex II of the EU Standard Contractual Clauses for the purposes of the UK Addendum.

Part B – Transfer Mechanisms by Sub-Processor

Where Customer Personal Data is transferred outside the United Kingdom by a Sub-Processor, GCG shall ensure that an appropriate transfer mechanism is in place. Current Sub-Processor transfer mechanisms are as follows:

Sub-Processor	Location of Processing	Transfer Mechanism
Amazon Web Services	UK / EU (primary); US (failover)	UK Addendum / EU SCCs
Okta	United States	UK Addendum
Auth0 (Okta)	United States	UK Addendum
HelpScout	United States	UK Addendum

GCG shall update this Schedule to reflect any changes to Sub-Processor transfer mechanisms and shall notify Customer in accordance with clause 7.2 of this DPA.

Part C – UK Addendum Table Completion

The following information completes the required table within the UK Addendum:

Field	Completion
Exporter	Customer, as identified in the Agreement.
Importer	GCG or the relevant Sub-Processor, as identified in Part B above.
Module	Module Two (Controller to Processor).
Clause 7 (Docking Clause)	Not applicable.

Field	Completion
Clause 9 (Sub-processors)	General authorisation (see clause 7 of the DPA). Notice period: 30 days.
Clause 11 (Redress)	Optional redress mechanism not included.
Clause 17 (Governing law of SCCs)	The law of a Member State that allows for third-party beneficiary rights. The parties select the law of Ireland.
Clause 18 (Jurisdiction)	Courts of Ireland (for the SCCs); courts of England and Wales (for the DPA and UK Addendum).
Annex I.A (Parties)	As set out above and in Schedule 1.
Annex I.B (Description of transfer)	As set out in Schedule 1.
Annex I.C (Competent supervisory authority)	Information Commissioner's Office (ICO).
Annex II (Technical and organisational measures)	As described in clause 5 of the DPA.