.جراث grath.

Data Protection Addendum

Grath Technologies Limited

Processor terms issued under the Data Protection Law, DIFC Law No. 5 of 2020 (as amended by Amendment Law No. 1 of 2025) and the DIFC Data Protection Regulations 2020

This Data Protection Addendum ("Addendum") is entered into between Grath Technologies Limited, a company registered in the Dubai International Financial Centre under Commercial Licence CL8894, whose registered office is at Unit Office 609, Level 6, Index Tower, Dubai International Financial Centre, Dubai, UAE ("Grath"); and the entity identified as Customer in the applicable Master Subscription Agreement or Order Form ("Customer").

This Addendum supplements and forms part of the Master Subscription Agreement ("Agreement") between Grath and Customer. In the event of any conflict between this Addendum and the Agreement, this Addendum 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 Addendum on behalf of itself and any Authorised Affiliates.

1. Definitions

In this Addendum, the following terms shall have the meanings set out below. Capitalised terms not defined here have the meaning given in the DP Law or the Agreement.

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

"Commissioner" means the Commissioner of Data Protection appointed under the DP Law, or any successor body exercising equivalent functions in the DIFC.

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

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

"DIFC Data Protection Laws" means the Data Protection Law, DIFC Law No. 5 of 2020 (as amended, including by Amendment Law No. 1 of 2025), the DIFC Data Protection Regulations 2020, and any directive, guidance or successor legislation issued by the Commissioner, each as amended or re-enacted from time to time.

"DIFC Standard Contractual Clauses" means the standard contractual clauses approved and published by the Commissioner under Article 27(2)(c) of the DP Law for transfers of Personal Data outside the DIFC to a jurisdiction that does not provide an adequate level of protection, as updated from time to time.

"DP Law" means the Data Protection Law, DIFC Law No. 5 of 2020, as amended.

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

"Addendum" 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" has the meaning given under DIFC Data Protection Laws.

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

"Restricted Transfer" means a transfer of Customer Personal Data from the DIFC to a Third Country (being any jurisdiction other than the DIFC, including onshore UAE) or an international organisation that has not been determined by the Commissioner under Article 26 of the DP Law to provide an adequate level of protection for Personal Data.

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

"Special Categories of Personal Data" has the meaning given under the DP Law, including Personal Data revealing or concerning racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify a person, and data concerning health, sex life, sexual orientation or criminal record.

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

2. Roles of the Parties

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

2.2 Customer is solely responsible for: (a) determining the lawful basis under Article 10 of the DP Law for the Processing of Customer Personal Data; (b) ensuring that Customer Personal Data provided to Grath is accurate and that its collection and transfer to Grath complies with DIFC Data Protection Laws; (c) responding to requests from Data Subjects exercising their rights, save where Grath is required to provide assistance under clause 8; and (d) maintaining all required records, notifications and notices in connection with Customer's use of the Services.

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

2.4 Nothing in this Addendum shall prevent Grath from Processing Personal Data for its own purposes as a Controller where Grath 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 Grath's own privacy notice.

3. Scope and Purpose of Processing

3.1 Grath 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 Categories of Personal Data to the Services unless expressly agreed in writing by Grath.

3.4 Grath 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. Grath's Obligations as Processor

4.1 Grath shall, in accordance with Article 24 of the DP Law:

- Process Customer Personal Data only in accordance with Customer's documented instructions and this Addendum;
- 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 Grath, in ensuring compliance with Customer's obligations under DIFC Data Protection Laws relating to security of Processing, notification of Personal Data Breaches, data protection impact assessments, and prior consultation with the Commissioner;
- 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 Addendum, and cooperate with audits in accordance with clause 10.

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

5. Security

5.1 Grath shall implement and maintain appropriate technical and organisational measures, in accordance with Article 14 of the DP Law, 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 of Data Subjects.

5.2 Grath'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 Grath currently holds ISO 27001 and SOC 2 certifications. Grath 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. Grath shall notify Customer without undue delay if any such certification is withdrawn or materially downgraded.

5.4 Grath 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 Grath shall notify Customer without undue delay after 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 Grath'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 Grath to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

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

6.4 Grath shall provide reasonable assistance to Customer in complying with Customer's obligations under Article 41 of the DP Law to notify the Commissioner and, where required, affected Data Subjects. Customer acknowledges that, as Controller, it is responsible for determining whether and when a Personal Data Breach must be notified to the Commissioner and to affected Data Subjects.

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

7.2 Grath 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 Grath 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 In accordance with Article 24(5) of the DP Law, Grath shall ensure that each Sub-Processor is bound by data protection obligations no less protective than those set out in this Addendum. Where a Sub-Processor fails to fulfil its obligations, Grath shall remain fully liable to Customer for the performance of the Sub-Processor's obligations under this Addendum.

7.5 Grath'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 Part 6 of the DP Law (including rights of access, rectification, erasure, restriction, portability, objection, in relation to automated decision-making, and non-discrimination).

8.2 Grath 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 DIFC Data Protection Laws in relation to Customer Personal Data. Grath 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 Grath 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. Grath 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 Grath shall provide reasonable assistance to Customer in carrying out any data protection impact assessment required under Article 20 of the DP Law in connection with the Services, taking into account the nature of the Processing and the information available to Grath.

9.2 Where Customer is required under the DP Law to consult with the Commissioner prior to undertaking any Processing activity in connection with the Services, Grath shall provide reasonable cooperation and assistance to Customer in relation to such consultation.

10. Audit Rights and Records

10.1 Grath shall maintain complete and accurate records of all categories of Processing activities carried out on behalf of Customer under this Addendum, in accordance with Article 15 of the DP Law, and shall make such records available to Customer upon reasonable written request.

10.2 Grath shall, upon reasonable written request from Customer, provide information necessary to demonstrate its compliance with this Addendum, 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 Grath'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, Grath 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 the Commissioner or following a confirmed Personal Data Breach;
- the scope of the audit is limited to Grath's Processing of Customer Personal Data under this Addendum;
- the audit is conducted during Grath's normal business hours and in a manner that minimises disruption to Grath'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 Grath of this Addendum.

10.4 Nothing in this clause shall limit Grath's obligation to cooperate with audits, investigations or inspections required by the Commissioner to the extent required by Applicable Law.

11. International Data Transfers

11.1 Grath shall not make any Restricted Transfer of Customer Personal Data unless the transfer is made in compliance with Part 4 of the DP Law, including by implementing one or more of the following safeguards:

- a determination by the Commissioner under Article 26 that the destination jurisdiction or international organisation provides an adequate level of protection;
- the DIFC Standard Contractual Clauses, or Binding Corporate Rules approved by the Commissioner; or
- such other appropriate safeguard or derogation as is recognised under Article 27 of the DP Law.

11.2 Where Grath relies on the DIFC Standard Contractual Clauses or other appropriate safeguard for a Restricted Transfer, the terms of Schedule 2 (International Transfers) shall apply. In accordance with the 2025 amendments to the DP Law, Grath shall carry out and document an assessment of whether Data Subjects will benefit from adequate legal protections and effective remedies in the recipient jurisdiction.

11.3 Grath shall maintain an up-to-date record of the jurisdictions 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 Grath's use of Sub-Processors may involve transfers of Customer Personal Data to jurisdictions outside the DIFC, including onshore UAE, and consents to such transfers provided Grath has implemented the appropriate safeguards referenced in clause 11.1 in relation to those Sub-Processors.

12. Retention and Deletion

12.1 Grath 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, Grath 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 Grath's possession or control.

12.3 Grath 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, Grath shall provide written confirmation of such deletion or destruction.

12.4 Notwithstanding clauses 12.2 and 12.3, Grath 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 Addendum.

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

13. Liability

13.1 This Addendum 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 Addendum 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 DIFC Data Protection Laws.

13.3 Each party's liability under this Addendum 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 Addendum shall be subject to the same cap as liability under the Agreement generally.

13.4 Where both Grath and Customer are responsible for damage caused by Processing in breach of the DP Law, their liability shall be apportioned in accordance with Article 64 of the DP Law. Customer acknowledges that, under the DP Law, a Processor is liable for damage caused by Processing only where it has not complied with obligations of the DP Law specifically directed to Processors, or where it has acted outside or contrary to the lawful instructions of the Controller.

14. Term

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

14.2 Termination or expiry of this Addendum 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 and Jurisdiction.** This Addendum and any non-contractual obligations arising in connection with it shall be governed by and construed in accordance with the laws of the DIFC. The parties submit to the exclusive jurisdiction of the DIFC Courts. Customer acknowledges that, following the 2025 amendments to the DP Law, a Data Subject has a private right of action and may bring proceedings directly before the DIFC Courts.

15.2 **Order of Precedence.** In the event of any conflict between this Addendum and the Agreement regarding the Processing of Customer Personal Data, this Addendum shall prevail. In the event of

any conflict between the main body of this Addendum and any Schedule, the main body shall prevail unless the Schedule expressly provides otherwise.

15.3 Entire Agreement. This Addendum, 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 Addendum shall be effective unless made in writing and signed by authorised representatives of both parties. Grath reserves the right to update this Addendum to reflect changes in DIFC Data Protection Laws or guidance issued by the Commissioner, and shall provide Customer with no less than 30 days' written notice of any material amendment.

15.5 Severability. If any provision of this Addendum 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 Addendum shall continue in full force and effect.

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

15.7 Authorised Affiliates. Customer may extend the benefit of this Addendum to its Authorised Affiliates. Customer shall remain responsible for ensuring that its Authorised Affiliates comply with the terms of this Addendum and the Agreement, and shall be liable to Grath 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 (for example, personal or company names appearing in transaction references). No Special Categories of Personal Data are intended to be Processed unless separately agreed in writing.
Special Categories of Personal Data	Not Processed unless required by Applicable Law or agreed in writing by both parties. Customer must not submit Special Categories of Personal Data to the Services without prior written agreement from Grath.
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 DIFC to Third Countries or international organisations that have not been determined by the Commissioner to provide an adequate level of protection.

Part A – General

A.1 Where Grath makes any Restricted Transfer of Customer Personal Data, it shall implement the DIFC Standard Contractual Clauses (in the Controller-to-Processor configuration) as the primary transfer mechanism, unless an adequacy determination under Article 26 of the DP Law or another appropriate safeguard or derogation under Article 27 applies.

A.2 For the purposes of the DIFC Standard Contractual Clauses:

- the "Data Exporter" is Customer (as Controller);
- the "Data Importer" is Grath 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 Addendum.

A.3 The parties agree that Schedule 1 satisfies the description-of-transfer requirements of the DIFC Standard Contractual Clauses, and that the technical and organisational measures described in clause 5 satisfy the security requirements of those clauses. Where required, Grath shall complete and document its assessment of the protections available to Data Subjects in the recipient jurisdiction.

Part B – Transfer Mechanisms by Sub-Processor

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

Sub-processor	Service	Location / transfer basis	Authorisation & DPA
Grath Consultancy Group Limited	Provision of SaaS	United Kingdom / DIFC SCCs	Article 24(5) agreement in place.

Grath 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 Addendum.

Part C – DIFC Standard Contractual Clauses: Completion

The following information completes the required details for the DIFC Standard Contractual Clauses:

Field	Completion
Data Exporter	Customer, as identified in the Agreement (acting as Controller).
Data Importer	Grath or the relevant Sub-Processor, as identified in Part B above (acting as Processor).

Field	Completion
Configuration	Controller to Processor.
Sub-processing	General authorisation (see clause 7 of this Addendum). Notice period: 30 days.
Description of transfer	As set out in Schedule 1.
Technical and organisational measures	As described in clause 5 of this Addendum.
Governing law of the Clauses	Law of the DIFC.
Jurisdiction	DIFC Courts.
Competent supervisory authority	DIFC Commissioner of Data Protection.
Recipient jurisdiction assessment	Documented by Grath where appropriate safeguards are relied upon, in accordance with clause 11.2 and the 2025 amendments to the DP Law.